ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ МОЛДОВЫ

На правах рукописи
У.Д.К.: 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

Автореферат диссертации на соискание ученой степени
доктор информатики

КИШИНЭУ, 2023

Диссертация разработана в рамках Департамента «Программная Инженерия и Автоматика» Технического Университета Молдовы.

Научный руководитель:
БЕШЛИУ Виктор, доктор технических наук, профессор.

Официальные оппоненты:
ПЕРЖУ Вячеслав, доктор хабилитат технических наук, доцент, Академик М.А.И.
ОХРИМЕНКО Сергей, доктор хабилитат экономических наук, профессор, Молдавская Экономическая Академия.

Состав Специализированного Ученого Совета:
БОСТАН Виорел, **председатель**, доктор хабилитат технических наук, профессор, Технический Университет Молдовы.
ФЕДОРОВ Ион, **секретарь**, доктор информатики, доцент, Технический Университет Молдовы.
ГАЙНДРИК Константин, доктор хабилитат информатики, профессор, Институт Математики и Информатики им. Владимира Андрунакиевича, член-корреспондент Академии Наук Молдовы.
БОЛУН Ион, доктор хабилитат информатики, профессор, Технический Университет Молдовы.
КОСТАШ Илие, доктор хабилитат информатики, профессор, Молдавская Экономическая Академия.
ЗГУРЯНУ Аурелиу, доктор физико-математических наук, доцент, Молдавская Экономическая Академия.
МОРАРУ Виктор, доктор технических наук, доцент, Технический Университет Молдовы.

Защита диссертации состоится **30 июня 2023**, в **15.00** на заседании Специализированного Ученого Совета D 232.02-23-4 при Техническом Университете Молдовы по адресу: MD-2045, Республика Молдова, г. Кишинев, ул. Студенческая 9/7, корпус № 3, каб. 3-208.

С текстом диссертации и автореферата можно ознакомиться в научно-технической библиотеке Технического Университета Молдовы и на веб-сайте Национального Агентства по Обеспечению Качества в Области Образования и Исследований (www.cnaa.md/anacec.md).

Автореферат был разослан “27” мая 2023.
Ученый секретарь
Специализированного Ученого Совета:
Доктор информатики, доцент **ФЕДОРОВ Ион**

Научный руководитель:
Доктор технических наук, профессор **БЕШЛИУ Виктор**

Автор: **КУНЕВ Вячеслав**

@Кунев Вячеслав, 2023

СОДЕРЖАНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность и значение темы диссертации. Все существующие финансовые и платежные системы (ПС) выросли из многообразия бумажных систем, при этом для каждой страны особенности учета финансовых операций различались. На данный момент, несмотря на значительные усилия по унификации все еще сохраняется значительная разница в построении и бизнес-логике таких систем. Платежные системы вынуждены взаимодействовать друг с другом для осуществления финансовых транзакций, однако соответствующие интерфейсы взаимодействия уникальны для каждой индивидуальной системы. Процесс интеграции сложен и трудоемок и, как следствие, в процессе последующей эксплуатации обязательно возникают вопросы, связанные с бесперебойной работой в частности, так и с безопасностью финансовых транзакций, в целом [1].

В работе под термином интероперабельность в контексте платежных систем понимается функциональная и информационная совместимость платежных систем, другими словами, способность большого количества платежных систем, интерфейсы которых полностью открыты, взаимодействовать без каких-либо ограничений доступа и реализации, включая обмен и использование информации о транзакциях, полученной в результате обмена. Иначе, платежные системы должны действовать по принципу «платежного интернета» - как набор независимых систем, которые используют стандартизированный набор правил, процедур, протоколов [3, 4, 6, 7].

Необходимость обеспечения информационной безопасности 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.

На данный момент криптография является неотъемлемой частью платежных систем, и для достижения интероперабельности платежных систем и необходимой безопасности требуется

использовать такие средства криптографии, которые совместимы, масштабируемы с точки зрения криптостойкости и обладают высокой скоростью работы [9, 10, 11, 12, 13]. Достижение квантового превосходства может обнулить все текущие платежные системы и, с другой стороны, замена текущей криптографии на что-то принципиально другое приведет к колоссальным издержкам. Таким образом необходимо принципиально усилить существующую криптографию, не меняя её принципов работы. Исходя из этого, одной из современных тенденций в криптографии является разработка новых методов, обеспечивающих информационную безопасность и криптостойкость, в том числе, с использованием методов сопоставительного анализа. Метод сопоставительного анализа является разделом теории чисел, который позволяет увеличить криптостойкость существующих систем, в том числе для криптосистемы RSA [14, 16]. Текущая высокая криптостойкость криптосистемы RSA 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.

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.

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 повышения 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.

Научные публикации. Основные результаты теоретических изысканий отражены в 6 публикациях, из которых 3 в научных журналах, в 2 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.

.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

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 интероперабельных систем, была представлена концептуальная модель и обобщённая архитектура интероперабельной системы. Были проанализированы стандарты обеспечения интероперабельности и безопасности информационных систем, был сделан обзор проблем интероперабельности современных платежных систем (ПС) и были предложены принципы построения интероперабельных платежных систем.

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.
- Каждый пользователь и администратор должен иметь свой уникальный цифровой идентификатор.
- 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 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.

Во второй главе – **Описание и моделирование крипто процессов** – отображены основные области применения криптографической защиты, принципы стойкости криптографических систем и основные методы шифрования - на базе работы с данными: блочное и поточное шифрование, и на базе работы с ключами: симметричное и асимметричное шифрование. Для каждого из проанализированных методов и алгоритмов шифрования/дешифрования были представлены их преимущества и недостатки.

Наиболее известной и распространённой в мире криптосистемой является асимметричная криптосистема RSA [14, 15, 16]. 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» [5] в котором приведен прогноз роста числа кубитов квантовых

компьютеров и, соответственно, для какой длины ключа классических криптоалгоритмов это представляет риски для компрометации. 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.

Исходя из этого, одной из современных тенденций в криптографии является разработка новых методов, обеспечивающих информационную безопасность и криптостойкость, с использованием методов сопоставительного анализа.

Таким образом, с учетом требований стандартов интероперабельности и безопасности платежных систем в электронной коммерции, предлагается технология базирующийся не на передаче самой информации по открытому каналу, а в передаче косвенных данных об этой информации, которые могут быть переданы в зашифрованном виде с необходимой степенью криптостойкости при помощи RSA, без задержек во времени [15, 17].

В третей главе – **Защита информации при помощи алгоритмов RSA-mAB на основе формантного анализа,** представлены разработанные модернизированные RSA-алгоритмы на основе формантной алгебры и строковой арифметики сопоставительного и формантного анализа.

Предложен способ контролируемого повышения вычислительной сложности криптоалгоритмов, 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.

Алгоритм AB1

Любое число в формантном анализе может быть представлено в виде двучленной конструкции [15]

$$N=pk+q, \qquad (1)$$

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

На Рисунке 1 показана блок-схема алгоритма АВ1 [4].

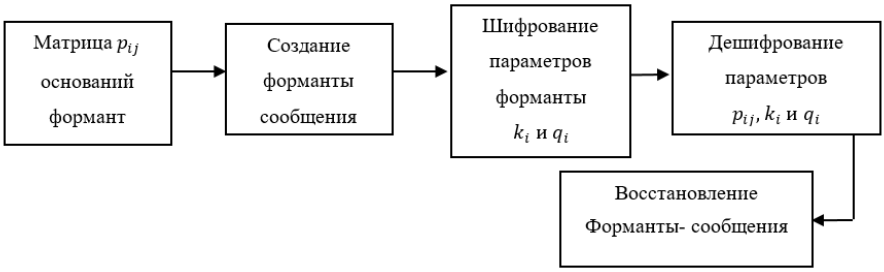

Рис. 1. Блок-схема алгоритма АВ1.

На основании (1) нужно шифровать не одно число N, а всего лишь три небольших числа. Различие в том, что N - большое целое число (порядка 10^{20} …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 (к примеру, число, соответствующее блочному шифру), для того чтобы остатки форманты находились в множестве достаточно больших чисел, что увеличивает итоговую криптостойкость. Для повышения скорости работы алгоритма, создаётся динамическая база данных, например, в виде матрицы, в ячейках которой хранятся заранее сгенерированные числа-основания формант. В зависимости от требований к степени 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 меняются индексы. Например, по правилу $p_{ij}=p_{ji}$, $i=j=0,1…n$, или менять процедуру индексирования по произвольному иному закону.

Описание алгоритма [15]:

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 $d_1d_2d_3$ о форманте открытого сообщения.
4. Зашифровывается сообщение $d_1d_2d_3$ 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:

$$F=p_{ij}\cdot k_i+q_i=p_i\cdot d_2+d_3. \quad (2)$$

Алгоритм АВ2.

В отличие от алгоритма АВ1 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 АВ1 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 099

01 От 100 … до 199

…….

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,… 99. Так, например, ячейка с номером 457 имеет адрес (индекс) P_{045}, а ячейка с номером 4057 – P_{4057}. Каждая ячейка матрицы $p_{ij}(e, d, n)$ содержит уже зашифрованное по системе RSA число-индекс, где e – открытый ключ, d – закрытый ключ, а $n=p \cdot q$. Для повышения степени крипто стойкости RSA-mAB рекомендуется в процессе создания шифрованного блока фиксированной длины случайным образом менять матрицы, соответствующие разным крипто замкам. Количество таких матриц и их объем зависят от долгосрочности секретности информации, а также от объёма оперативной и долговременной памяти микроконтроллера, на котором реализуется криптосистема RSA-mAB [15].

Алгоритм АВ3.

В отличие от алгоритма АВ2 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 АВ2 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 [15]:

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 $d_1d_2d_3$.
4. Генерируются крипто ключи для k_i и q_i.
5. Шифруется сообщение о форманте $d_1d_2d_3$.
6. Шифрованное сообщение передаётся в канал связи.
7. Принимается блок 64 бит.
8. Из принятого блока извлекается координата-адрес p_{ij}.
9. Восстанавливается значение основания форманты.
10. Из соответствующего блока извлекаются k_i и q_i.
11. Восстанавливается форманта по шифрованному сообщению на основании стандартной формулы.

На передающей стороне в программе есть таблица с уже сгенерированными 64-разрядными ключами (она содержит значения для $p, q, n, e, d, \varphi(n)$ где p и q имеют 64 разряда), где $n=p\cdot q$; e – открытый ключ; d – закрытый ключ; $\varphi(n) =(p-1)(q-1)$– значение функции Эйлера. Вводится текст, который переводится в цифры, каждая буква кодируется 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 (Рисунок 2) [15]. 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 выбираются ключи RSA, после чего, запускается процедура дешифрования очередного анализируемого блока данных. Далее это число конвертируется в букву, исходный символ или число (последовательность бит) (Рисунок 3) и продолжается снова поиск нулей в зашифрованном тексте.

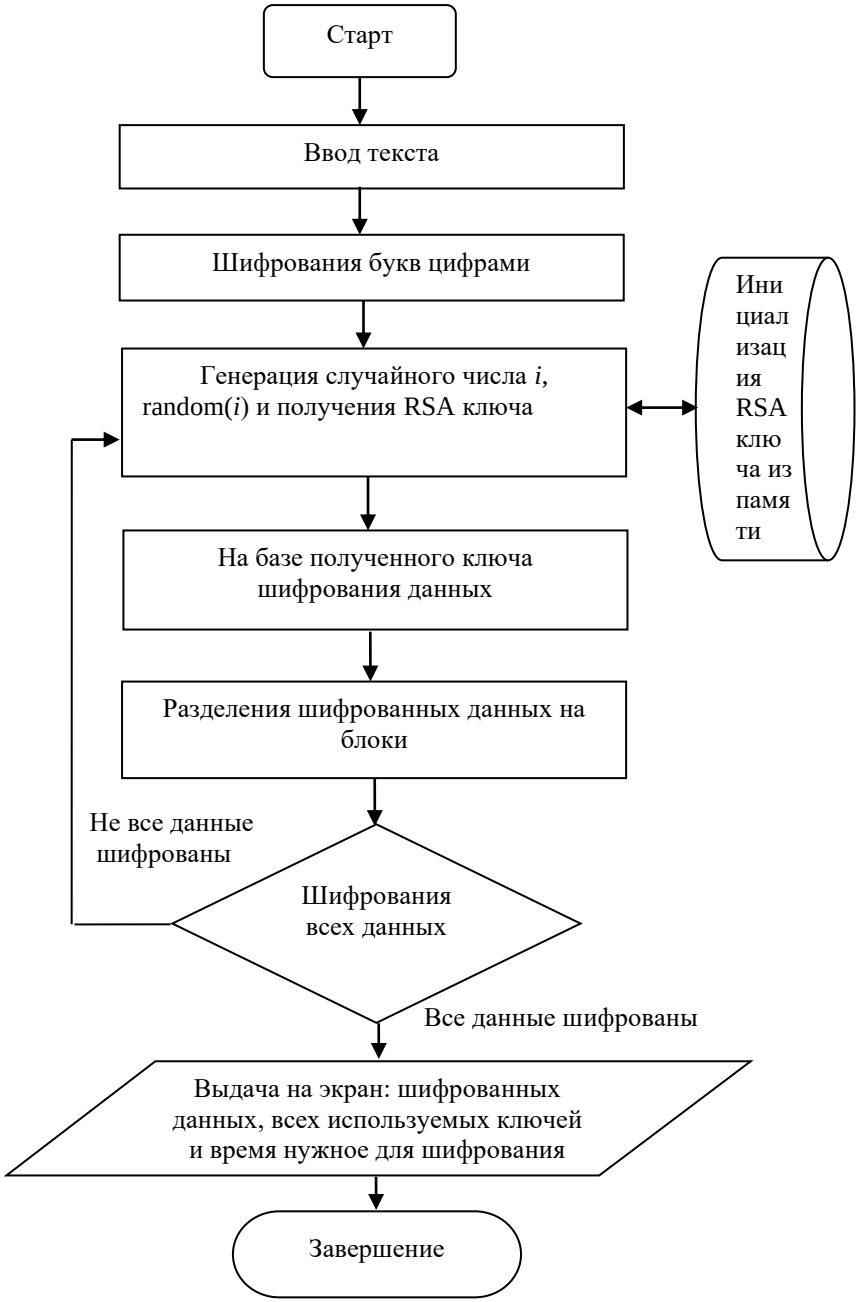

Рис. 2. Алгоритм шифрования на передающей стороне.

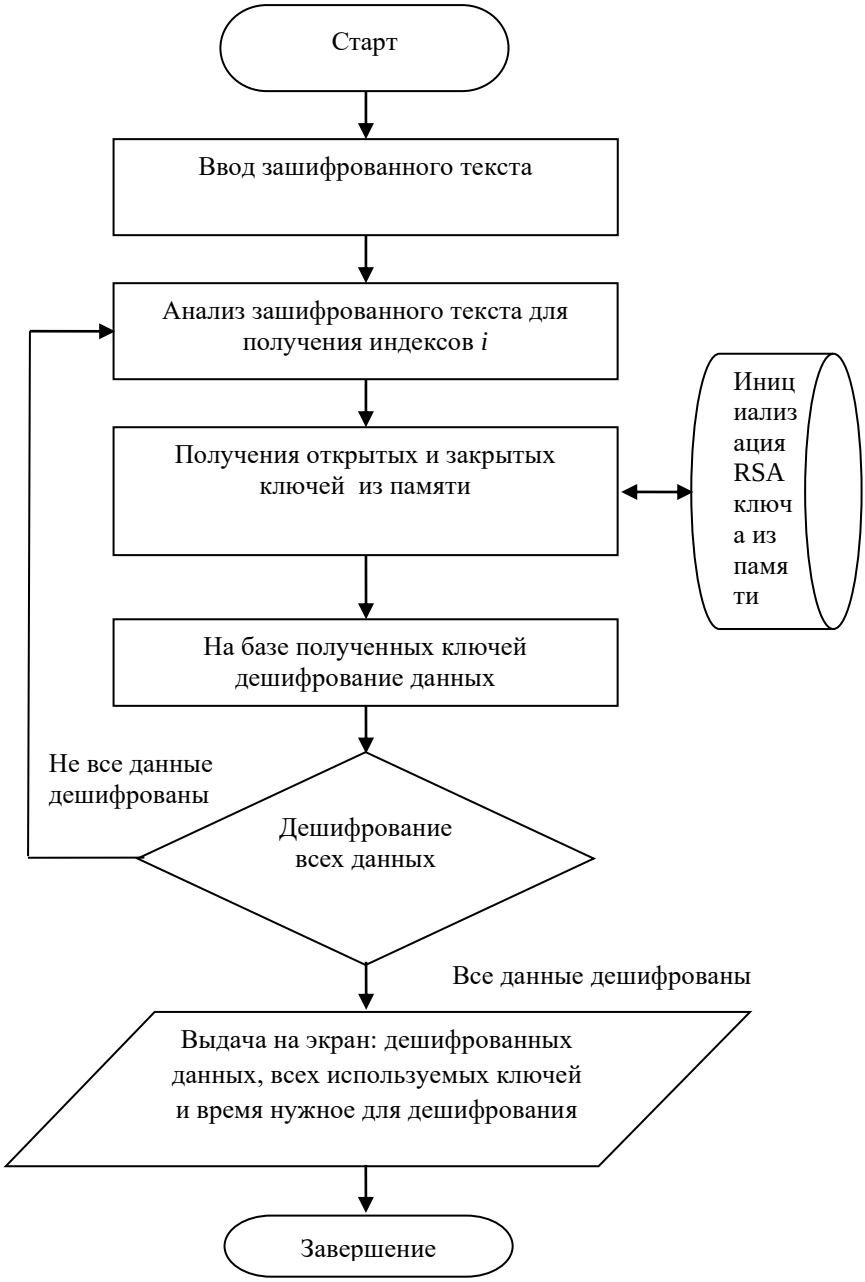

Рис. 3. Алгоритм дешифрования на приёмной стороне.

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

Формантный анализ позволяет вводить дополнительные неопределённости при шифрации/дешифровании если в уравнение крипто замка RSA (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=1[14-15].

$$e \cdot d = \varphi(n) \cdot k + 1. \qquad (3)$$

При a=1 выражение (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:

$$e \cdot d = k \cdot \varphi(n) + a = k \cdot \varphi(p) \cdot \varphi(q) + a = k \cdot (p-1) \cdot (q-1) + a,\ a \geq 1. \qquad (4)$$

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 [10].
- 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:

$$O(\exp\{(\alpha+1)[\ln n]^r \ln[\ln n]^{n-r}\}) + O(A^s),$$

или $$O\left(e^{1{,}9\lg[N]^{\frac{1}{3}}\lg([\log N])^{\frac{2}{3}}}\right) + O(A^S),$$

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), Рисунок 4.

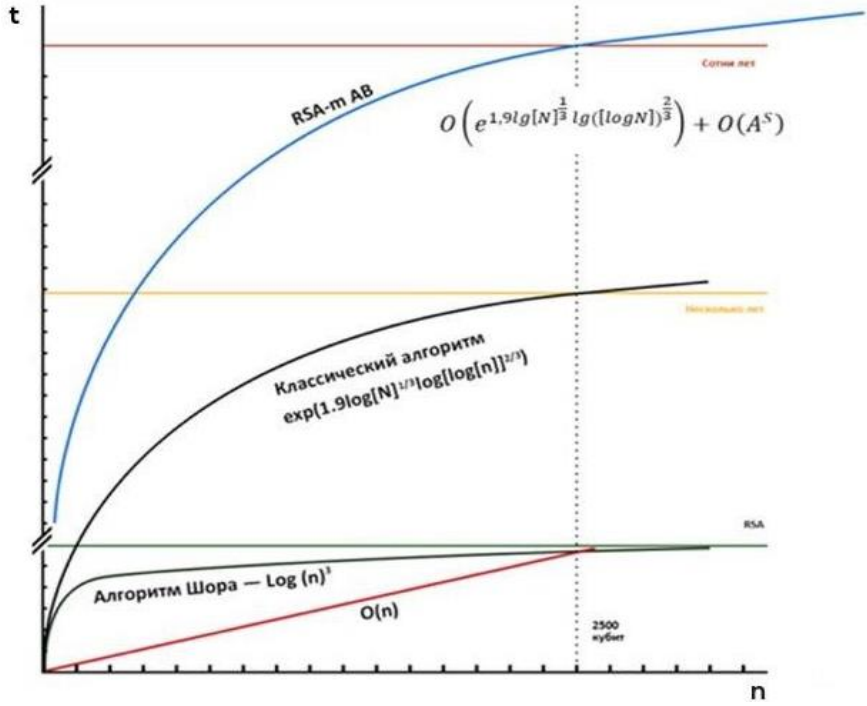

Рис. 4. Сравнительный график оценки крипто стойкости различных алгоритмов к атаке «грубой силой» в постквантовый период (r = 2048 бит).

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 подробно описана система асимметричного побитного шифрования форманты речевого сообщения, где были подробно проанализировано

шифрование 4096 возможных значений дискрет звука на базе предложенных алгоритмов.

Для реализации формантного подхода в подготовке исходного сообщения для шифрования 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 кодирования 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 $e_i d_i \pmod{N}=1$. 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 дешифрования [8].

Шифруются все дискреты тройкой параметров формант *p, q, k* и записываются в память в виде индексов матриц M_1. Таким образом

у одной и той же дискреты в ПЗУ будет существовать 10000 различных индексов-адресов в матрице типа M_1.

Такое же распределение ПЗУ формируется и на приёмной стороне [2].

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.

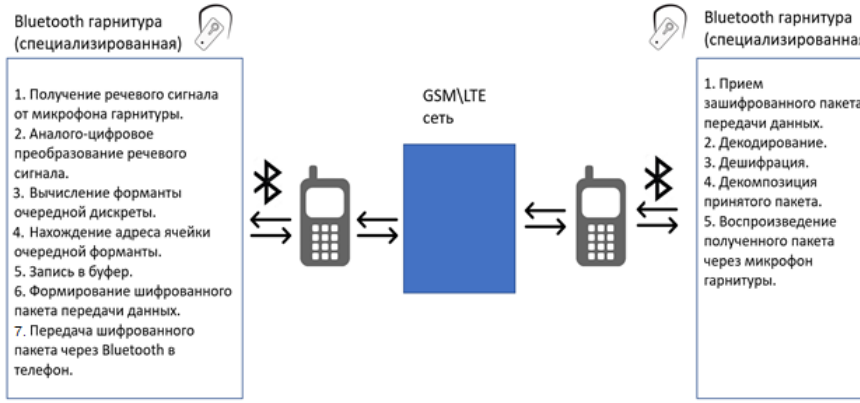

Рис. 5. Инфограмма устройства защищённой мобильной передачи данных.

На рисунке 5 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 [2].

III. 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.

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. 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).

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.

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.

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.

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 интероперабельные 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.

IV. БИБЛИОГРАФИЯ

1. 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.
2. 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.
3. 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.
4. 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.
5. *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 ediation, 2019, 42 p.
6. 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

7. MATSUI, M. The First Experimental Cryptanalyst of the Data Encryption Standard. *Proc. CRYPTO'94. Lecture Notes in Comp*, Sci. Springer-Verlag, 1996.
8. 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.
9. 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.
10. 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.
11. XIE, SC., NIU, XF. & ZHANG, JZ. An Improved Quantum E-Payment System. *Int J Theor Phys* 59, 2020, p. 445–453. https://doi.org/10.1007/s10773-019-04338-7.
12. YANG, JH., CHANG, CC. A Low Computational-Cost Electronic Payment Scheme for Mobile Commerce with Large-Scale Mobile Users. *Wireless Pers Commun* 63, 2012, p. 83–99. https://doi.org/10.1007/s11277-010-0109-2.
13. ZGUREANU, A. Information encryption systems based on Boolean functions. In: *Computer Science Journal of Moldova*, vol.18, no.3(54), 2010, pp. 319-335.
14. 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.
15. 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.

16. БАЛАБАНОВ, А. А., АГАФОНОВ, А. Ф. Методы сопоставительного анализа и формантных уравнений теории чисел в задачах криптографии. *Вестник Российской Академии Естественных Наук*,Том 14, № 4, 2014, кат. Б, с. 47-53. ISSN 1682-1696.
17. 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.

V. СПИСОК ОПУБЛИКОВАННЫХ НАУЧНЫХ РАБОТ АВТОРА

În reviste din străinătate recunoscute:

1. БАЛАБАНОВ, А., **КУНЕВ, В. В.** Современное применение алгоритмов формантного анализа для криптозащиты IT-систем. *Журнал: Вестник Российской Академии Естественных Наук РАЕН*, том 19, № 3, 2019, 25-35 с.

În reviste din Registrul Naţional al revistelor de profil, cu indicarea categoriei:
Categoria B +

2. 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, pp. 75 – 82. ISSN 2587-3474/ eISSN 2587-3482. https://doi.org/10.52326/jes.utm.2021.28(1).07. https://jes.utm.md/vol-xxviii-1-2021/
3. **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)

Articole în culegeri ştiinţifice:
În lucrările conferinţelor ştiinţifice internaţionale (peste hotare):

4. 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.

În lucrările conferinţelor ştiinţifice internaţionale (Republica Moldova)

5. CUNEV, V. Secure Voice Data Transmission Based on the Formant Analysis Algorithms. In: P*roceedings 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.

Brevete de invenţii şi alte obiecte de proprietate inteectuală, materiale la saloanele de invenţii

6. BALABANOV, A., AGAFONOV A., CUNEV, V. Dispozitiv și procedeu de protecţie crypto-grafică a informaţiei binare (variante). 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.

7. Cerere de înregistrare a brevetului din 15 aprilie 2021, titlu: Metoda de criptare a informațiilor binare în spațiul spectral și unui dispozitiv de transmisie în baza lui; autori: BALABANOV, A., KUNEV, V., CERNOMOREȚ, E.

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", Chișinău, 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 obținute sunt publicate în 5 - lucrări științifice, 1 – carte, 1- brevet de invenție, 1 – cerere de înregistrare a brevetului.

Cuvinte cheie: Interoperabilitate, securitate informațională, criptografie, stabilitate criptografică, algoritmi de analiză formantă.

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

Scopul și 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 și originalitatea științifică a rezultatelor obținute constă în propunerea algoritmilor RSA-modernizați pe baza algebrei formante și a aritmeticii de șiruri, a analizei comparative și formante, cu asigurarea stabilității criptografice temporale a sistemului în timp real și propunerea unei metode de creștere controlată a complexității de calcul a algoritmilor criptografici.

Semnificația 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 cifrare/decifrare, prin înlocuirea informației transmise cu anumite date protejate indirecte. Algoritmii criptografici propuși au permis de a spori stabilitatea criptografică și a asigura creșterea controlată a complexității algoritmilor criptografici, fără a fi nevoie de costuri semnificative de modernizare a sistemelor informatice existente.

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

Аннотация

Диссертации на соискание учёной степени доктор в информатике, с темой "Современные интероперабельные информационные технологии в защищенных 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 научных работах, 1-й – книге, 1-м - патенте, 1-й – заявке 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.

Annotation

Of the Ph.D. Thesis in Informatics with title "Modern interoperable information technologies in secure payment systems based on 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 algorithm 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 paper 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 paper 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 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.

UNIVERSITATEA TEHNICĂ A MOLDOVEI

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

Rezumatul tezei de doctor în informatică

CHIŞINĂU, 2023

КУНЕВ ВЯЧЕСЛАВ

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

232.02 – ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОДУКТЫ И СИСТЕМЫ

Автореферат диссертации на соискание ученой степени доктор информатики

Aprobat spre tipar: 25.05.2023
Hârtie ofset. Tipar digital.
Coli de tipar: 1.73

Formatul hârtiei 60×84 1/16
Tirajul 50 exemplare
Comanda Nr. 20

U.T.M. 2023. Chişinău, bd. Ştefan cel Mare şi Sfânt 168.
Secţia Redactare şi Editare a U.T.M.
2045, Chişinău, str. Studenţilor 9/9.