На правах рукописи

ХО НГОК ЗУЙ

АЛГОРИТМЫ ОБРАБОТКИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Специальность 05.13.01 – Системный анализ, управление и обработка информации (технические системы)

АВТОРЕФЕРАТ

диссертация на соискание ученой степени

кандидата технических наук

Санкт-Петербург – 2012

Работа выполнена в Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» им. В.И.Ульянова (Ленина), на кафедре автоматизированных систем обработки информации и управления

Научный руководитель: доктор технических наук, профессор
Молдовян Николай Андреевич

Официальные оппоненты: доктор технических наук, профессор
Яшин Александр Иванович, заслуженный деятель науки РФ, директор научно-технического центра ОАО «Информационные телекоммуникационные технологии»
кандидат технических наук, доцент
Воронин Иван Викторович, доцент кафедры Систем обработки информации и управления Балтийского государственного технического университета «Военмех»

Ведущая организация: Петербургский государственный университет путей сообщения

Защита состоится «05» марта 2012 г. в 14ч. на заседании совета по защите докторских и кандидатских диссертаций Д 212.238.07 Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина) по адресу: 197376, Санкт-Петербург, ул. Проф. Попова, 5.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан «03» февраля 2012 г.

Ученый секретарь
совета по защите докторских и
кандидатских диссертаций Д 212.238.07 Цехановский В.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Система электронного документооборота (СЭД) — это электронная система, предназначенная для передачи информации по телекоммуникационным каналам связи между территориально удаленными информационными массивами. СЭД способствуют сбережению и рациональному использованию человеческих ресурсов и повышению эффективности управления потоками информации и корпоративных документов. В настоящее время, в связи с бурным развитием Интернет-технологий, системы электронного документооборота находят широчайшее применение во многих сферах человеческой деятельности. Высокие темпы роста объемов информации, хранимой и передаваемой по телекоммуникационным каналам связи, создают благоприятные условия для противоправных действий в отношении электронной информации. Наряду с организационными, правовыми и техническими методами для решения указанных задач, важнейшее значение приобретают программно-технические средства управления правами доступа к ресурсам информационно-вычислительных систем. Существенное повышение эффективности управления доступом к информационно-вычислительным ресурсам достигается широким применением алгоритмов обработки информации специального вида, позволяющих выполнять обратимые преобразования информации с использованием некоторой дополнительной информации, и обеспечивающие недоступность информации для лиц, не имеющих прав доступа. Достоинствами этого метода являются его гибкость, универсальность, высокая надежность и возможность достижения сравнительно невысоких экономических издержек.

Современные СЭД ориентированы на массовое использование, связаны с интенсивной передачей данных и характеризуются выполнением типовых процедур обработки информации в масштабе времени, близком к реальному. В связи с последним включение процедур маскирующей обработки информации требует согласования по производительности. Спецификой современных СЭД является их реализация на основе скоростных информационно-телекоммуникационных систем, включая в частности массово используемые мобильные терминальные устройства с ограниченными схемотехническими ресурсами, что требует реализации алгоритмов маскирующей обработки информации в условиях ограниченных схемотехнических ресурсов. С учетом ограниченных энергетических возможностей мобильных терминальных устройств возникает необходимость согласования типовых и маскирующих процедур обработки информации также и по энергопотреблению. На основе указанных моментов согласования типовых и маскирующих процессов обработки информации в СЭД сформулированы требования к процедурам маскирующей обработки информации, которые заключаются в ее выполнении в реальном масштабе времени и снижении аппаратной стоимости реализации и энергопотребления. Данные требования характеризуются противоречием между необходимостью повышения производительности алгоритмов маскирующей обработки информации и снижением схемотехнической

сложности их реализации. Для разрешения сложившегося противоречия ставится научная задача повышения интегральной эффективности аппаратной реализации алгоритмов маскирующей обработки информации на основе использования алгоритмов и базовых операций маскирующей обработки информации.

Актуальность темы диссертационного исследования связана с ее ориентацией на разрешение противоречия между необходимостью применения дополнительных ресурсов и ограничениями в наращивании схемотехнической сложности устройств, связанного с использованием скоростных алгоритмов маскирующей обработки информации в СЭД.

Целью диссертационной работы является уменьшение аппаратной сложности реализации скоростных алгоритмов маскирующей обработки информации в СЭД при одновременном повышении интегральной эффективности реализации, что обеспечивает сохранение высокой производительности современных СЭД.

Объектом исследования являются современные СЭД, базирующиеся на скоростных информационно-телекоммуникационных системах и мобильные терминальные устройства передачи, хранения и обработки информации.

Предметом исследования являются алгоритмы и базовые операции маскирующей обработки информации, ориентированные на согласованное использование совместно с типовыми алгоритмами обработки информации в СЭД.

В соответствии с поставленной целью работы определены основные задачи диссертации:

1. Разработка базовых операций алгоритмов маскирующей обработки информации на основе управляемых подстановочно-перестановочных сетей (УППС), отличающихся применением управляемых элементов, ориентированных на аппаратную реализацию с использованием 64-битовых ячеек памяти.
2. Синтез управляемых подстановочно-перестановочных сетей, обеспечивающих их эффективную аппаратную реализацию в программируемых логических интегральных схемах нового поколения.
3. Разработка критериев выбора типовых управляемых элементов (УЭ) для их реализации в виде векторной булевой функции от шести переменных.
4. Построение топологий управляемых подстановочно-перестановочных сетей, ориентированных на использование типовых управляемых элементов новых типов и обеспечивающих высокую интегральную эффективность алгоритмов обработки информации.
5. Синтез алгоритмов маскирующей обработки информации, обеспечивающих высокую интегральную эффективность их аппаратной реализации в программируемых логических интегральных схемах нового поколения.

6. Исследование статистических свойств алгоритмов маскирующей обработки информации.

7. Анализ обеспечиваемого уровня маскирования информации в условиях возможности перехвата передаваемых документов в СЭД.

Используемые методы:

В диссертационной работе используются методы дискретной математики, математической статистики, теории вероятностей, теории множеств.

Достоверность полученных результатов подтверждается математическими доказательствами, статистическими экспериментами, теоретическим анализом предложенных алгоритмов маскирующей обработки информации, практическими разработками, сопоставлением с известными результатами по синтезу и анализу алгоритмов маскирующей обработки информации, а также широкой апробацией в открытой печати и на научно-технических конференциях.

Научные положения, выносимые на защиту:

1. Управляемые подстановочно-перестановочные сети, построенные на основе управляемых элементов, для реализации базовых операций алгоритмов маскирующей обработки информации.
2. Переключаемые управляемые операции, реализуемые на основе управляемых подстановочно-перестановочных сетей.
3. Поточные алгоритмы маскирующей обработки информации.
4. Блочные алгоритмы маскирующей обработки информации на основе управляемых и переключаемых управляемых операций.

Научная новизна:

1. Управляемые подстановочно-перестановочные сети, построенные на основе управляемых элементов, для реализации базовых операций алгоритмов маскирующей обработки информации, отличающиеся использованием типовых управляемых элементов, описываемых векторной булевой функцией от шести переменных, что позволяет обеспечить высокую интегральную эффективность аппаратной реализации алгоритмов обработки информации в программируемых логических интегральных схемах (ПЛИС) нового поколения.
2. Переключаемые управляемые операции, реализуемые на основе управляемых подстановочно-перестановочных сетей, отличающиеся использованием новых топологий и управляемых элементов, что позволяет снизить аппаратную сложность реализации алгоритмов обработки информации в ПЛИС нового поколения.
3. Поточные алгоритмы маскирующей обработки информации, отличающиеся использованием латинских квадратов, реализованных с помощью управляемых подстановочно-перестановочных сетей, что позволяет повысить производительность.
4. Блочные алгоритмы маскирующей обработки информации на основе управляемых и переключаемых управляемых операций, отличающиеся

построением последних с использованием управляемых элементов, представляемых в виде векторной булевой функции от шести переменных, что позволяет повысить производительность при одновременном снижении аппаратной стоимости реализации.

Практическая ценность полученных результатов состоит в повышении интегральной эффективности аппаратной реализации скоростных алгоритмов маскирующей обработки информации и возможности ее осуществления в реальном масштабе времени с использованием мобильных терминальных устройств телекоммуникационных систем, на базе которых функционируют современные СЭД.

Реализация результатов. Результаты диссертационной работы внедрены в учебный процесс СПбГЭТУ при преподавании дисциплин «Инфокоммуникационные системы и сети», «Интеллектуальные информационные системы» и «Распределенные системы обработки данных» на кафедре Автоматизированных систем обработки информации и управления.

Апробация. Апробация полученных результатов и научных положений подтверждена их обсуждением на следующих конференциях: Санкт-Петербургская международная конференция Региональная информатика 2010; Инновационная деятельность в Вооруженных силах Российской Федерации: Всеармейская научно-практическая конференция (Санкт-Петербург, 2008, 2010); The 2011 International Conference on Advanced Technologies for Communications (ATC2011) (Da Nang, 2011).

Публикации. По материалам диссертации опубликовано 18 работ, из них по теме диссертации 8, в том числе 4 статьи в журналах из перечня ВАК. Доклады доложены и получили одобрение на 4 международных, всероссийских и межвузовских научно-практических конференциях.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав с выводами по каждой из них, заключения, приложения, содержит 161 страницу машинописного текста, включая 41 рисунок, 33 таблицы, список литературы из 99 наименований и 6 приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении дано обоснование актуальности темы диссертационного исследования, сформулированы цели и задачи работы, её научная новизна и практическая значимость, представлены положения, выносимые на защиту.

В первой главе дается общий обзор современных СЭД и требования обеспечения надежности, целостности и аутентификации информации в автоматизированных информационных системах, а также представлены известные результаты по использованию управляемых операций как элементарных операций алгоритмов маскирующей обработки информации.

Рассматриваются вопросы, связанные с надежностью, целостностью и аутентификацией информации в системах электронного документооборота, и роль алгоритмов маскирующей обработки информации для обеспечения

надежности, целостности и аутентификации информации. Надежность электронных документов должна достигаться применением взаимосвязанного комплекса мер, к числу которых относятся: электронная подпись документов; алгоритм маскирующей обработки сообщений при передаче по каналам связи; разграничение полномочий при работе с электронными документами; существование арбитра; организационные меры.

Отражена специфика современных СЭД, состоящая в их реализация на основе скоростных информационно-телекоммуникационных систем, включая в частности массово используемые мобильные терминальные устройства с ограниченными схемотехническими ресурсами и ограниченным энергопотреблением. Показана необходимость согласования типовых и маскирующих процедур обработки информации по скорости работы алгоритмов, аппаратной сложности реализации и энергопотреблению устройств, реализующих процедуры обработки информации. Для обеспечения указанного согласования сформулированы требования к процедурам маскирующей обработки информации, которые заключаются в ее выполнении в реальном масштабе времени и снижении аппаратной стоимости реализации и энергопотребления. На основе сформулированных требований поставлены задачи диссертационного исследования.

Далее в первой главе рассматриваются вопросы проектирования скоростных аппаратных алгоритмов маскирующей обработки информации с использованием операций преобразования, зависящих от преобразованных данных. В таких алгоритмах усиливается параллелизм вычислений и одновременно с преобразованием подблоков данных возможно преобразование раундовых подключей. Это создает предпосылки для применения простого расписания использования ключа (ПРИК) к построению блочных алгоритмов, обеспечивающих высокую скорость обработки информации в условиях частой смены ключа. Однако применение ПРИК приводит к тому, что для некоторых классов ключей процедура прямого преобразования будет совпадать с процедурой обратного преобразования информации. Кроме того, для некоторых подклассов ключей применение ПРИК приводит к тому, что все раундовые ключи оказываются одинаковыми, а, следовательно, все раунды алгоритма будут представлять собой одно и тоже преобразование. Это создает предпосылки для осуществления «слайд анализа». На основе анализа показано, что для устранения указанных проблем наибольший интерес представляет использование переключаемых УППС для синтеза алгоритмов маскирующей обработки информации с использованием ПРИК. В настоящее время в массовом масштабе выпускаются ПЛИС нового поколения (Virtex-5, Virtex-6, Virtex-7, Spartan-6 и т.д.), типовые логические блоки которых содержат ячейки с большим объемом памяти, которые позволяют существенно повысить производительность устройств преобразования информации.

На основе выполненного анализа существующих научно-технических задач в затронутой области и подходов к их решению формулируется цель и исследовательские задачи диссертационной работы.

Во второй главе предложено несколько подходов к синтезу блочных алгоритмов маскирующей обработки информации на основе переключаемых операций, а также несколько подходов к синтезу поточных алгоритмов маскирующей обработки информации на основе латинских квадратов. Разрабатываются способы построения перестановочных сетей с симметричной топологией для всех значений порядка и размера входа, равных натуральной степени числа 2, и разрабатывается способ вычисления значения управляющего вектора для выполнения заданных фиксированных перестановок с помощью сетей данного типа.

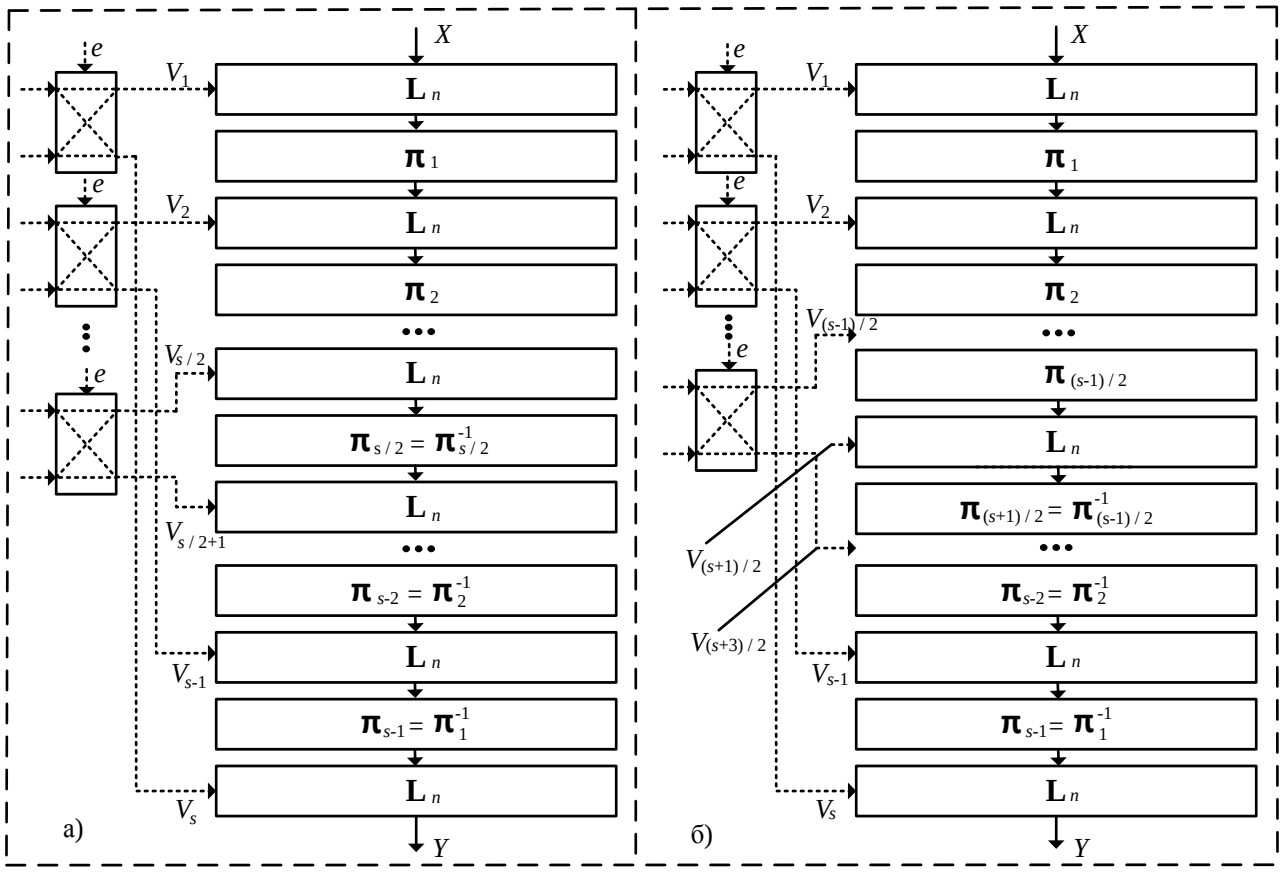

Рисунок 1. Построение ПУО $\mathbf{F}_{n/m}^{(V,e)}$ на основе УППС: а − с четным числом активных каскадов, б − с нечетным числом активных каскадов

Как уже отмечалось в первой главе, переключаемые управляемые операции (ПУО), реализуемые на основе УППС, обеспечивают решение задачи построения алгоритмов с простым расписанием использования ключа, свободного от слабых и полуслабых ключей, включая построение итеративных алгоритмов. На основе прямых УЭ легко построить УППС $\mathbf{F}_{n/m}$ и на основе обратных УЭ – обратные УППС $\mathbf{F}_{n/m}^{-1}$. Если типовой элемент представляет собой элементарную управляемую инволюцию, то активные каскады ($\mathbf{L}_n$) в блоках $\mathbf{F}_{n/m}$ и $\mathbf{F}_{n/m}^{-1}$ являются идентичными и представляют собой однослойные УППС. Поэтому, в зеркальной симметрии топологии блока $\mathbf{F}_{n/m}$ соответствующий ему обратный блок $\mathbf{F}_{n/m}^{-1}$ отличаются только тем, что компоненты управляющего вектора $V = (V_1, V_2, \ldots, V_s)$ распределены по активным каскадам в обратном порядке. Это означает, что в случае прямых

УППС ($e = 0$) они распределены сверху вниз, а в случае обратных УППС ($e = 1$) снизу вверх. Изменением порядка использования компонентов управляющего вектора можно задать переключение прямой УППС на обратную УППС. Очевидно, что такой способ построения ПУО пригоден для произвольной симметричной структуры УППС, т.е. проблема построения ПУО может быть решена предварительным построением УППС с симметричной топологией. Схемное представление ПУО $\mathbf{F}_{n/m}^{(V,e)}$ показано на рисунке 1.

На рисунке 2 представлен 64-битовый итеративный алгоритм **Hawk-64**, построенный на основе двух нелинейных операций: 1) блоки подстановок размера 4x4; 2) операция, зависящая от преобразуемых данных, а именно переключаемая операция $\mathbf{F}_{32/96}^{(L,e)}$ (см. рисунок 4). Итеративная структура алгоритма **Hawk-64** включает восемь типовых раундов преобразования блока данных. Этот алгоритм использует простое расписание использования ключа.

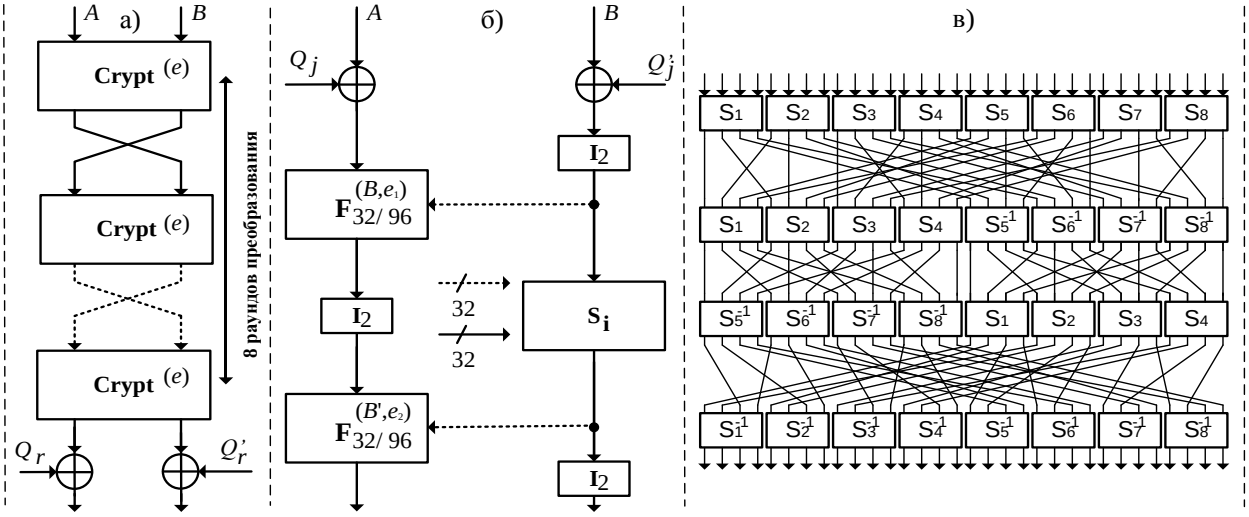

Рисунок 2. Алгоритм **Hawk-64**: а − итеративная структура, б − процедура **Crypt**$^{(e)}$, в − топология операции S_i

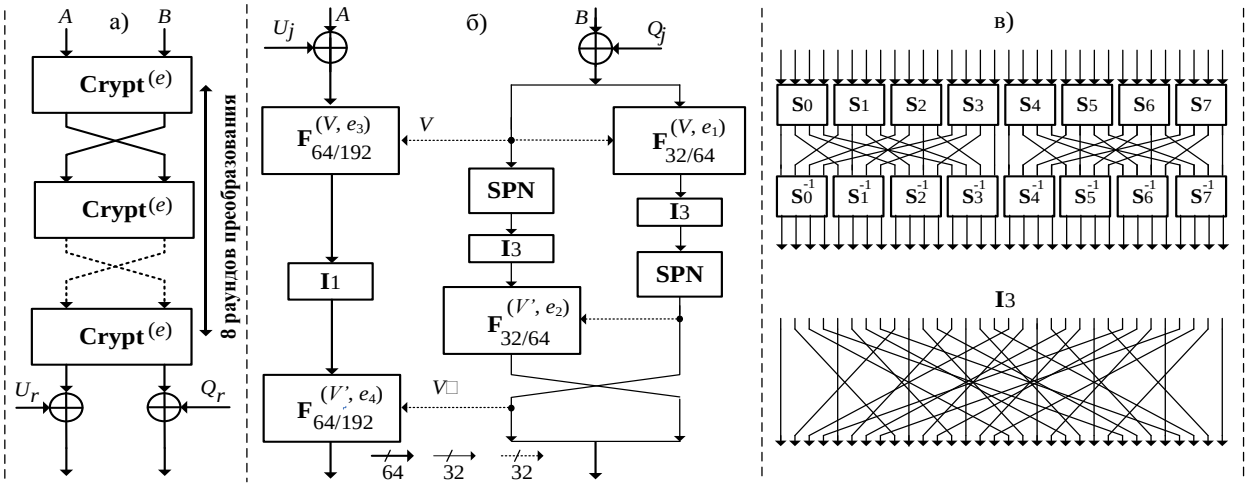

Рисунок 3. Алгоритм **Hawk-128**: а − итеративная структура, б − структура раунда преобразования, в − структура **SPN**

Строение 8-раундового итеративного блочного алгоритма **Hawk-128** аналогично строению алгоритма **Hawk-64**. Итеративная структура алгоритма

Hawk-128 включает восемь типовых раундов преобразования блока данных. На рисунке 3 представлена принципиальная схема процедуры раундового преобразования **Hawk-128**. В раундовом преобразовании используются переключаемые управляемые данными операции $\mathbf{F}_{64/192}^{(L,e)}$ и $\mathbf{F}_{32/64}^{(L,e)}$ (см. рисунок 4), а также подстановочно-перестановочная сеть SPN (см. рисунок 3). Этот алгоритм использует простое расписание использования ключа.

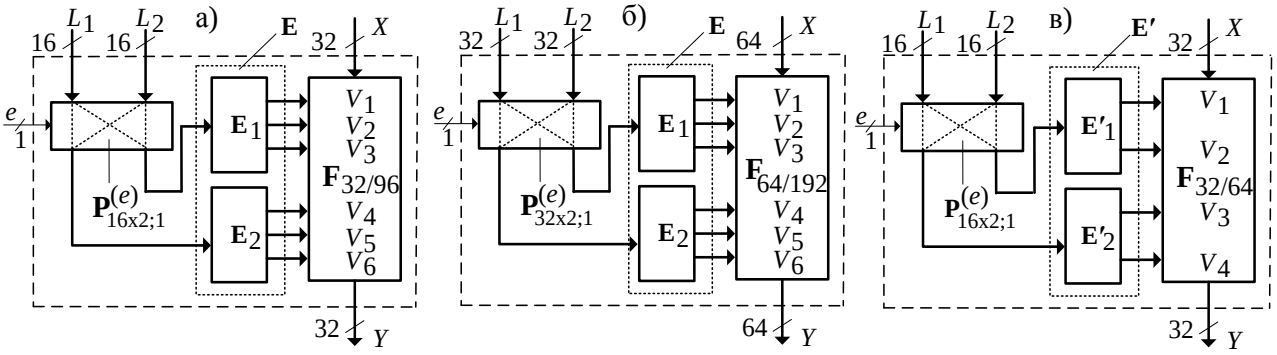

Рисунок 4. Переключаемые операции: а − переключаемая операция $\mathbf{F}_{32/96}^{(L,e)}$, б − переключаемая операция $\mathbf{F}_{64/192}^{(L,e)}$, в − переключаемая операция $\mathbf{F}_{32/64}^{(L,e)}$

Далее во второй главе рассматриваются методы построения поточных алгоритмов маскирующей обработки информации. Была показана эффективность использования УППС при синтезе блочных алгоритмов маскирующей обработки информации, ориентированных на аппаратную реализацию. Однако применение УППС в синтезе поточных алгоритмов до настоящего времени не рассматривалось, хотя они также представляют интерес для обеспечения маскирующей информации в информационных и телекоммуникационных системах. Блочные преобразования, реализуемые с помощью УППС, обладают выраженными свойствами рассеивания и перемешивания, а также достаточно высоким значением нелинейности. Это делает их интересными и для разработки поточных алгоритмов маскирующей обработки информации, однако проблема в этом направлении состоит в том, что требуется реализовать генератор ключевой гаммы с предсказуемой длиной периода.

Схемы генерации латинских квадратов размера $2^n \times 2^n$ на основе блочного алгоритма представляют собой расширение идеи реализации поточного алгоритма путем последовательного преобразования содержимого n-разрядного счетчика с помощью алгоритма, задающего некоторую функцию блочного преобразования $\boldsymbol{E}$ с n-битовым входом. Такой механизм создает элементы латинского квадрата, которые описываются следующим образом:

$$\gamma_{ji} = E_{K_1}\left(i \oplus E_{K_2}(j)\right).$$

Легко показать, что данная схема для всех различных значений j генерирует различные последовательности n-битовых блоков данных, причем n-битовые значения γ_{ij} будут представлять собой элементы латинский квадрат, если величины i и j интерпретировать как номера столбцов и строк, соответственно.

Механизм генерации латинских квадратов на основе УППС представлен на рисунке 5. Пусть $C = (C_l, C_h)$, $C' = (C'_l, C'_h)$ и $Y = (Y_l, Y_h)$, имеем следующие утверждения:

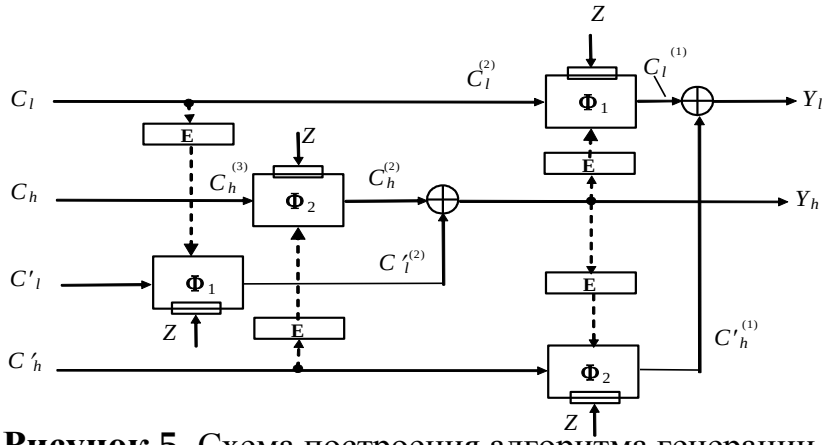

Рисунок 5. Схема построения алгоритма генерации псевдослучайных последовательностей – **Alg**

Утверждение 1. Для любых фиксированных значений C' и Z преобразование $Y = \boldsymbol{F}(C) = \mathbf{Alg}(C, C', Z)$ задает биективное отображение;

Утверждение 2. Для любых фиксированных значений C и Z преобразование $Y = \boldsymbol{F}(C') = \mathbf{Alg}(C, C', Z)$ задает биективное отображение.

Используя доказанные утверждения, можно легко доказать следующую теорему:

Теорема 1. Для произвольного фиксированного значения Z преобразование $Y = \mathbf{Alg}(C, C', Z)$ задает латинский квадрат $\|Y_{CC}\|$.

По сравнению с известными способами обеспечивается существенное увеличение длины гаммы. Предложенные схемы генерации латинских квадратов обобщены на случай генерации гаммы длиной $n2^{zn}$ бит, где $z \geq 2$. Предложенные схемы генерации латинских квадратов с использованием блочных алгоритмов могут быть использованы для синтеза на их основе скоростных поточных алгоритмов с нелинейной ключевой гаммой заданного периода.

<u>В третьей главе</u> разрабатываются критерии выбора управляемых элементов для эффективной реализации УППС на ПЛИС нового поколения. Разрабатываются методы построения и проектирования УППС различного порядка и размера входа на основе разработанных УЭ. На основе разработанных УППС разрабатываются новые блочные алгоритмы маскирующей обработки информации для аппаратной реализации с использованием ПЛИС нового поколения.

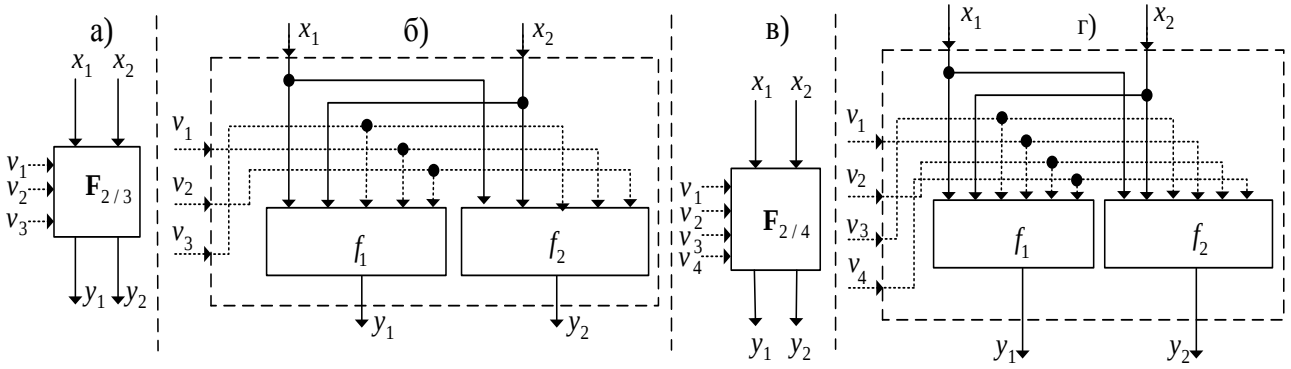

Рисунок 6. УЭ: а − УЭ $\mathbf{F}_{2/3}$, б − представление $\mathbf{F}_{2/3}$ в виде пары булевых функций, в − УЭ $\mathbf{F}_{2/4}$ и г − представление $\mathbf{F}_{2/4}$ в виде пары булевых функций

Как отмечалось в первой главе, каждый конфигурируемый логический блок ПЛИС нового поколения выполнит логическую функцию с большим количеством переменных. Это создает УЭ с расширением входной разрядности, например, УЭ $\mathbf{F}_{2/3}$, $\mathbf{F}_{2/4}$. Управляемые элементы $\mathbf{F}_{2/3}$ обладают двухбитовыми входом и выходом и трехбитовым управляющим входом (см. рисунки 6а и 6б). Управляемые элементы $\mathbf{F}_{2/4}$ обладают двухбитовыми входом и выходом и четырехбитовым управляющим входом (см. рисунки 6в и 6г).

Управляемые элементы с двухбитовым входом удобно представлять в виде пары двух булевых функций (БФ) или в виде упорядоченного набора подстановок размера 2×2. В соответствии с этим в общем случае УЭ $\mathbf{F}_{2/3}$ может быть представлен в виде:

1. двух булевых функций от пяти переменных;

2. восьми подстановок размера 2×2, каждая из которых выполняется над входным 2-битовым двоичным вектором (x_1, x_2) при одном из восьми возможных значений управляющего вектора $V = (v_1, v_2, v_3)$.

По аналогии с вариантами представления элементов $\mathbf{F}_{2/3}$ в общем случае УЭ $\mathbf{F}_{2/4}$ удобно представлять в следующих двух видах:

1. в виде пары булевых функций от шести переменных;

2. в виде упорядоченного набора из шестнадцати подстановок размером 2×2, каждая из которых выполняется над входным 2-битовым двоичным вектором (x_1, x_2) при одном из 16 возможных значений управляющего вектора $V = (v_1, v_2, v_3, v_4) = (0, 0, 0, 1); (0, 0, 1, 0); (0, 0, 1, 1); \ldots; (1, 1, 1, 1)$.

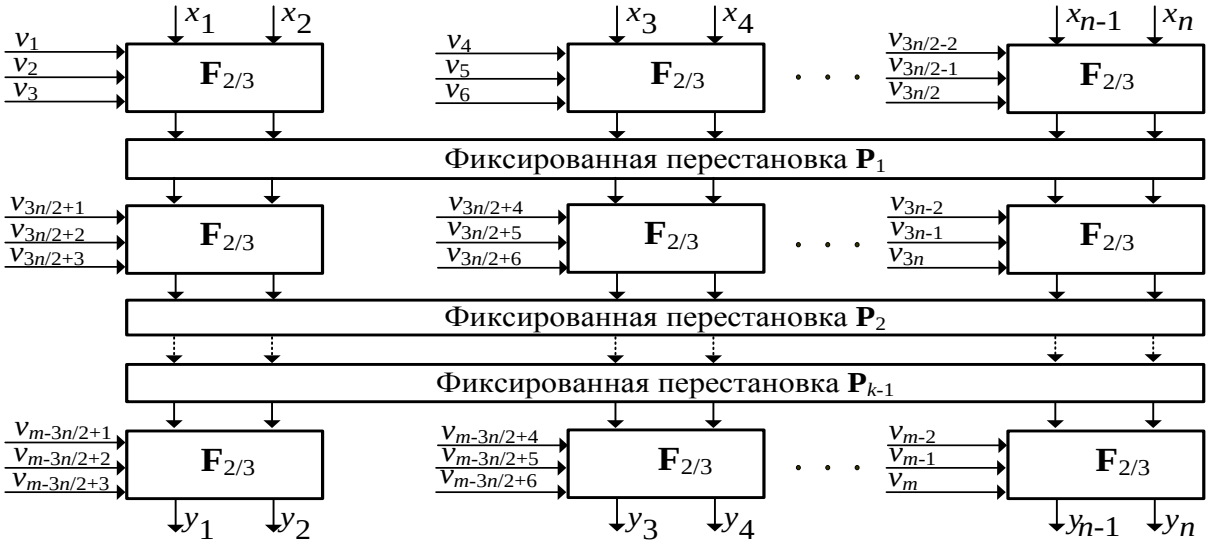

Рисунок 7. Слоистая структура УППС $\mathbf{F}_{n/m}$ на основе УЭ $\mathbf{F}_{2/3}$

Можно сформулировать следующие базовые критерии отбора и проектирования УЭ $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$:

1. Любой из двух выходов блока $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$ должен иметь значение нелинейности, близкое к максимально возможному для сбалансированных БФ от пяти (для $\mathbf{F}_{2/3}$) или шести (для $\mathbf{F}_{2/4}$) переменных;

2. Каждая из всех элементарных модификаций блока $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$, должна осуществлять биективное преобразование $(x_1, x_2) \to (y_1, y_2)$;

3. Каждая из всех элементарных модификаций блока $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$ должна быть инволюцией;

4. Линейная комбинация БФ $y_1 \oplus y_2$ должна иметь значение нелинейности, близкое к максимальному.

Найденные варианты УЭ $\mathbf{F}_{2/4}$, удовлетворяющие заданным критериям могут быть использованы для построения УППС, ориентированных на использование в скоростных блочных алгоритмах. Путем комбинирования базовых УЭ $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$ можно синтезировать УППС $\mathbf{F}_{n/m}$, где n – число входных (выходных) бит, m – число управляющих бит. Конкатенация всех управляющих битов образует управляющий вектор V. Общий вид УППС на основе УЭ $\mathbf{F}_{2/3}$ ($\mathbf{F}_{2/4}$) представлен на рисунке 7 (рисунке 8).

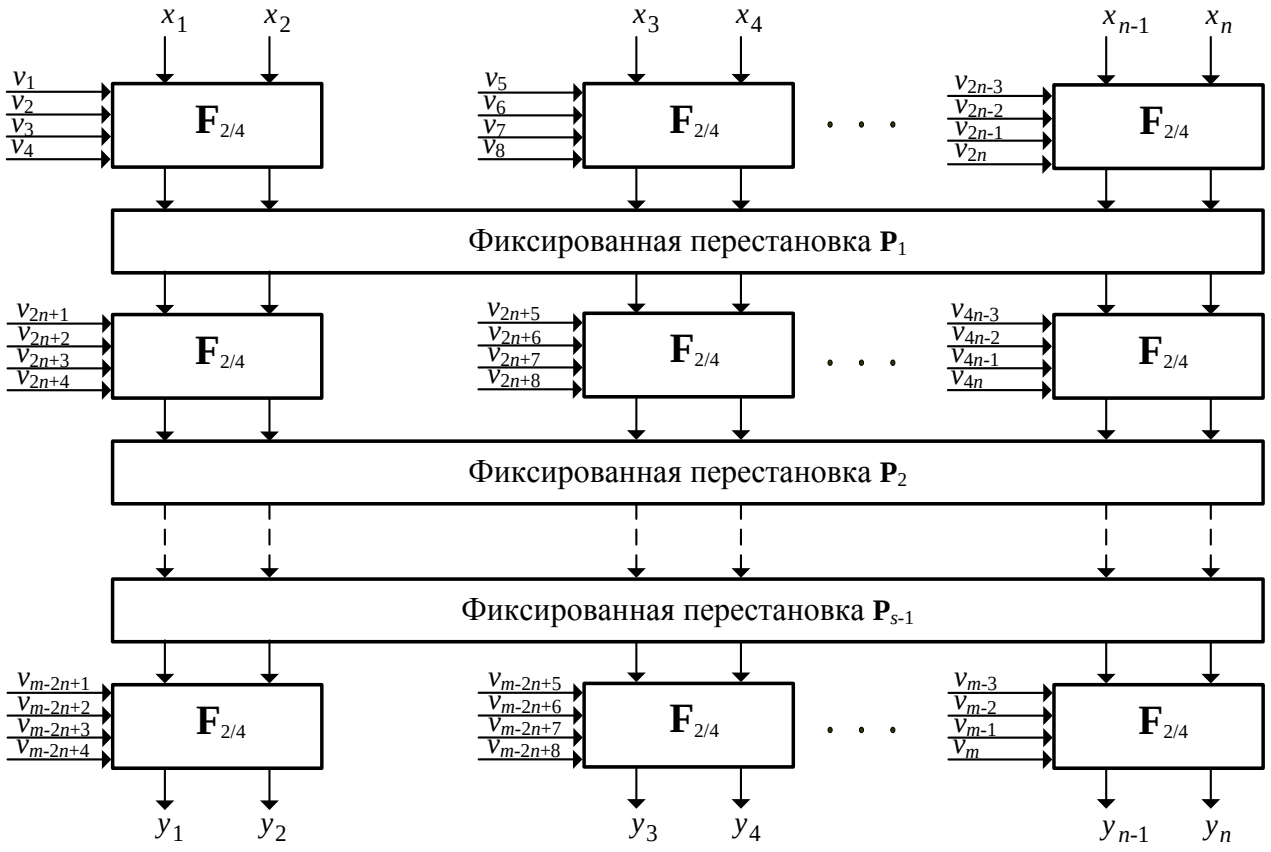

Рисунок 8. Слоистая структура УППС $\mathbf{F}_{n/m}$ на основе УЭ $\mathbf{F}_{2/4}$

Построение УППС различного порядка h = 1, 2, 4, …, n/4, n на основе УЭ $\mathbf{F}_{2/3}$, осуществляется с использованием трех следующих рекурсивных схем построения:

1. Модель *первого типа*, которая обеспечивает построение сети $\mathbf{F}_{2n/2m+3n}$ с использованием двух произвольных УППС $\mathbf{F}_{n/m}$ и n дополнительных элементарных блоков $\mathbf{F}_{2/3}$. Используя на первом шаге первой модели двух УЭ $\mathbf{F}_{2/3}$ в качестве объединяемых блоков $\mathbf{F}_{n/m}$, получим следующий ряд синтезируемых УППС первого порядка: $\mathbf{F}_{4/12}$, $\mathbf{F}_{8/36}$, $\mathbf{F}_{16/96}$ и т.д.;

2. Модель *второго типа*, которая обеспечивает построение сети $\mathbf{F}^{-1}_{2n/2m+3n}$, как объединение двух сетей $\mathbf{F}^{-1}_{n/m}$, с помощью дополнительного нижнего активного слоя, где $\mathbf{F}^{-1}_{n/m}$ обозначает УППС, являющуюся *обратной* по

отношению к сети $\mathbf{F}_{n/m}$. Начиная рекурсивное построение второго типа с использованием двух блоков $\mathbf{F}_{2/3}^{-1}$ в качестве объединяемых блоков $\mathbf{F}_{n/m}^{-1}$, получаем следующий ряд УППС первого порядка: $\mathbf{F}_{4/12}^{-1}$, $\mathbf{F}_{8/36}^{-1}$, $\mathbf{F}_{16/96}^{-1}$ и т.д.;

3. Синтез УППС, обладающих симметричной топологией, реализуется рекурсивной моделью *третьего типа*, которая характеризуется объединением двух исходных блоков $\mathbf{F}_{n/m}$ с помощью двух связующих активных слоев, коммутируемых двумя фиксированными перестановками с блоками $\mathbf{F}_{n/m}$.

По аналогии с методами построения УППС на основе УЭ $\mathbf{F}_{2/3}$ можно синтезировать УППС на основе УЭ $\mathbf{F}_{2/4}$, осуществляющие отображения вида $\mathrm{GF}(2)^{n(2\cdot k+1)} \to \mathrm{GF}(2)^n$.

В результате проведенных исследований определены следующие основные свойства однородных блоков УППС $\mathbf{F}_{n/m}$ слоистого типа, построенных на основе элементарных подстановочных УЭ $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$ и имеющих топологию, представленную на рисунке 7 и рисунке 8: 1) количество аргументов БФ f_i, реализующих конкретный вид УППС; 2) биективный УППС; 3) алгебраическая степень нелинейности БФ $\deg(f_i)$; 4) верхняя граница нелинейности УППС; 5) лавинные свойства УППС.

На рисунке 9 представлены итеративные алгоритмы **Video-64** и **Video-128**, ориентированные на эффективную аппаратную реализацию в ПЛИС нового поколения. Эти алгоритмы включают восемь типовых раундов преобразования блока данных. Они используют простое расписание использования ключа.

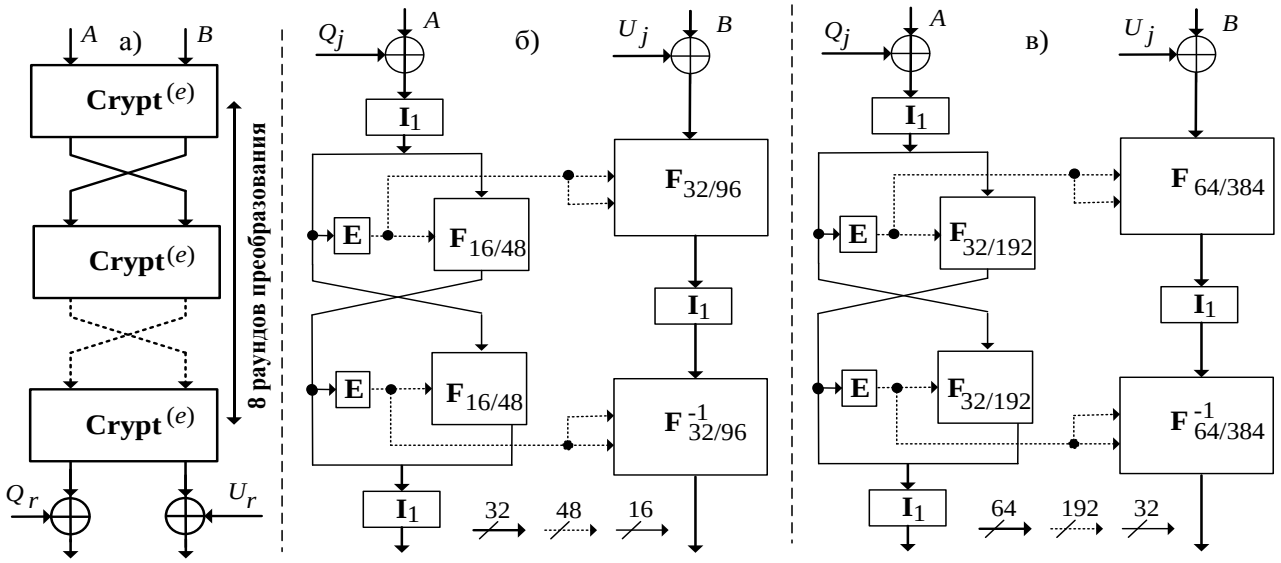

Рисунок 9. Алгоритмы маскирующей обработки информации:
а − итеративная структура, б − **Video-64**, в − **Video-128**

<u>В четвертой главе</u> представлены результаты комплексного статистического исследования разработанных алгоритмов, оценка обеспечиваемой стойкости к известным методам анализа и оценка сложности аппаратной реализации с использованием ПЛИС. Приводится сравнительный анализ аппаратной реализации разработанных алгоритмов.

При оценивании статистических свойств алгоритмов блочной обработки информации определялись следующие характеристики: 1) среднее число битов выхода, изменяющихся при изменении одного бита входного вектора d_1; 2)

степень полноты преобразования d_2; 3) степень лавинного эффекта d_3; 4) степень соответствия строгому лавинному критерию d_4.

Результаты статистического тестирования разработанного алгоритма **Hawk-64** (см. таблицу 1) показывают, что статистические характеристики удовлетворяются полностью как для влияния битов исходного текста, так и для влияния битов ключа на преобразованный текст. Аналогично получается для остальных алгоритмов: **Hawk-128**, **Video-64** и **Video-128**.

Таблица 1. Результаты статистической обработки алгоритма **Hawk-64**

Число раундов	Влияние битов входного текста				Влияние битов ключа			
	d_1	d_2	d_3	d_4	d_1	d_2	d_3	d_4
1	22.898	0.750	0.7155	0.7126	11.949	0.3828	0.3734	0.3563
2	**32.001**	**1.000**	**0.9996**	**0.9961**	27.531	0.8750	0.8601	0.8566
3	**32.000**	**1.000**	**0.9996**	**0.9961**	**32.000**	**1.0000**	**0.9996**	**0.9960**
4	**31.998**	**1.000**	**0.9995**	**0.9960**	**32.002**	**1.0000**	**0.9996**	**0.9960**
5	**32.000**	**1.000**	**0.9996**	**0.9961**	**32.001**	**1.0000**	**0.9995**	**0.9961**
6	**31.996**	**1.000**	**0.9995**	**0.9960**	**31.999**	**1.0000**	**0.9995**	**0.9959**
8	**31.999**	**1.000**	**0.9996**	**0.9961**	**32.000**	**1.0000**	**0.9995**	**0.9960**

Выполненный анализ разработанных алгоритмов показал, что из вариантов анализов на основе специально подобранных текстов наиболее низкой сложностью обладает дифференциальный анализ (ДА). В таблице 2 приведены результаты оценки стойкости разработанных алгоритмов к ДА. Полученные результаты показывают, что четыре раунда алгоритма **Hawk-64** и шесть раундов алгоритмов **Hawk-128**, **Video-64** и **Video-128** обеспечивают стойкость к ДА.

Таблица 2. Анализ стойкости разработанных алгоритмов к ДА

Наименование алгоритма	r	Характеристика		P(r)*	$r_{\min}$	Граница безопасности $(100\%(r-r_{\min})/r_{\min})$
		Разность	Вероятность			
Hawk-64	8	$(0, \Delta_1^R)$	$P(2) \approx 2^{-32}$	$\approx 2^{-59}$	4	100%
Video-64	8	$(0, \Delta_1^R)$	$P(2) \approx 2^{-20}$	$\approx 2^{-59}$	6	33%
Hawk-128	8	$(0, \Delta_2^R)$	$P(2) \approx 2^{-43}$	$\approx 2^{-117}$	6	33%
Video-128	8	$(0, \Delta_1^R)$	$P(2) \approx 2^{-44}$	$\approx 2^{-122}$	6	33%

*r и r_{min} – заданное и минимально безопасное число раундов, соответственно; * – вклад характеристики в вероятность прохождения разности через r раундов для случайного преобразования*

Интегральную эффективность аппаратной реализации алгоритма оцениваем по двум моделям:

1. **модель №1** – алгоритм реализуется в виде отдельной интегральной схемы, частота которой определяется глубиной комбинационной схемы, определяемой архитектурой реализации. Эффективность такой реализации можно посчитать по формуле: IE = S/R, где S – производительность, R – аппаратные ресурсы, необходимые для реализации;

2. **модель №2** – алгоритм реализуется в ПЛИС, отвечающей за другие функции, например, коммуникационные (задана частота). Формула эффективности в данном случае: IE = $S/(R*F)$, где F – частота.

Таблица 3. Сравнительный анализ реализации различных алгоритмов в ПЛИС Virtex Device v200pq240

Наим-ние алгоритма	Кол-во Раунд.	Кол-во #CLBs	Частот, MHz	Произв., Mbps	Интегральная оценка	
					Mbps/#CLBs	Mbps/(#CLBs*GHz)
Hawk-64	**8**	**560**	**85.0**	**680**	**1.211**	**14.3**
Hawk-128	**8**	**1,068**	**86.2**	**1379**	**1.273**	**14.7**
Cobra-128	12	2,364	86.0	917	0.392	4.5
CIKS-128	8	1,511	65.0	992	0.660	10.2
AES	10	2,358	22.0	259	0.114	5.0
RC6	20	2,638	13.8	88.5	0.034	2.4
Twofish	16	2,666	13.0	104	0.039	3.0

Таблица 4. Сравнительный анализ реализации различных алгоритмов в ПЛИС Virtex-5 Device XC5VLX50

Наим-ние алгоритма	Кол-во Раунд.	Кол-во #CLBs	Частот, MHz	Произв., Mbps	Интегральная оценка	
					Mbps/#CLBs	Mbps/(#CLBs*GHz)
Video-64	**8**	**56**	**380.63**	**3044**	**54.36**	**140.80**
Video-128	**8**	**95**	**420.20**	**6723**	**70.77**	**168.42**
AES	10	200	339.087	4350	21.75	64.14

CLB-конфигурируемый логический блок

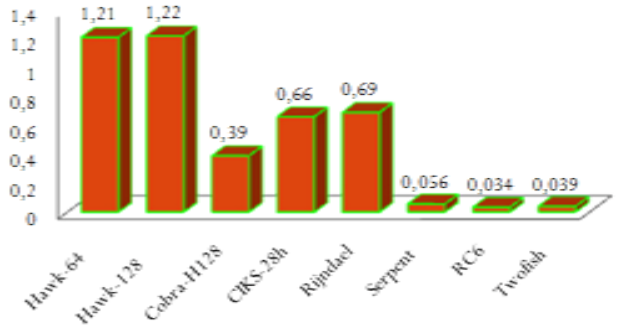

Рисунок 10. Сравнение эффективности аппаратной реализации с использованием модели оценки 1 в ПЛИС Семейства Virtex

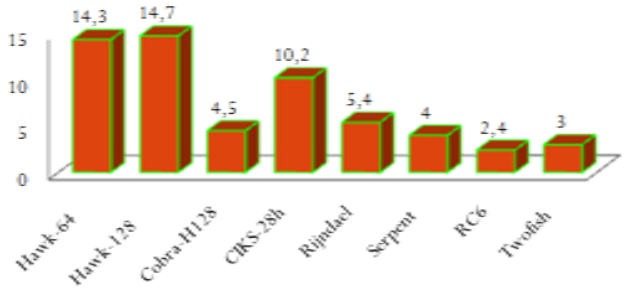

Рисунок 11. Сравнение эффективности аппаратной реализации с использованием модели оценки 2 в ПЛИС Семейства Virtex

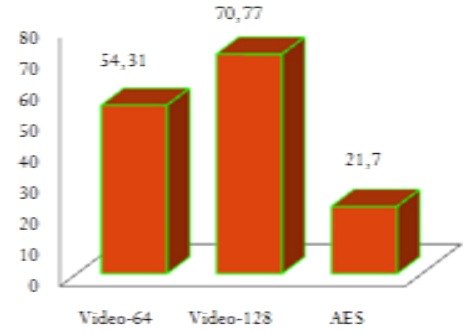

Рисунок 12. Сравнение эффективности аппаратной реализации с использованием модели оценки 1 в ПЛИС Семейства Virtex-5

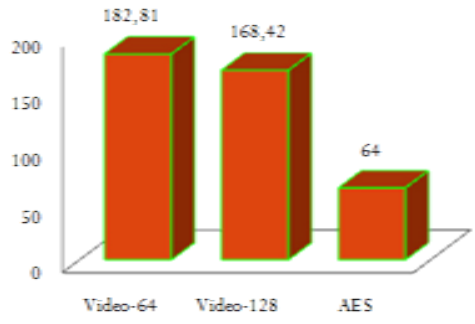

Рисунок 13. Сравнение эффективности аппаратной реализации с использованием модели оценки 2 в ПЛИС Семейства Virtex-5

В таблице 3 произведено сравнение эффективности аппаратной реализации алгоритмов **Hawk-64** и **Hawk-128** с большинством известных алгоритмов с использованием ПЛИС семейства Virtex по итеративной архитектуре. В таблице 4 произведено сравнение эффективности аппаратной реализации

алгоритмов **Video-64** и **Video-128** с алгоритмом AES с использованием ПЛИС семейства Virtex-5 по итеративной архитектуре. На рисунках 10, 11, 12 и 13 представлены диаграммы сравнения эффективности аппаратной реализации по двум моделям: “производительность / количество элементов” и “производительность / (количество элементов * частота)”. Из полученных результатов, видно, что разработанные алгоритмы являются существенно более эффективными для рассматриваемой реализации по сравнению с большинством известных блочных алгоритмов, основанных на управляемых перестановках и финалистов AES.

В заключение сформулированы основные результаты работы:

1. Предложены базовые операции алгоритмов маскирующей обработки информации – переключаемые управляемые операции, отличающиеся их реализацией на основе УППС, построенных использованием типовых управляемых элементов $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$.

2. Разработаны критерии отбора и проектирования управляемых элементов $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$ для синтеза УППС, ориентированных на реализацию в программируемых логических интегральных схемах нового поколения и также исследованы их основные свойства: нелинейность и дифференциальность.

3. Разработаны методы построения и проектирования УППС различного порядка и размера входа на основе разработанных управляемых элементов типов $\mathbf{F}_{2/3}$ и $\mathbf{F}_{2/4}$ и исследованы их основные алгебраические свойства. Полученные результаты показывают, что при использовании УППС со структурой в соответствии с УЭ с расширенным управляющим входом, могут повышаться значение нелинейности каждого выхода управляемых элементов, увеличиваться его алгебраическая степень нелинейности и усиливаться лавинный эффект при изменении одиночных битов управляющего подблока данных.

4. Разработан алгоритм вычисления значения управляющего вектора для выполнения заданных фиксированных перестановок в операционных блоках управляемых перестановок битов.

5. Разработаны новые блочные алгоритмы маскирующей обработки информации на основе операций преобразования, зависящих от преобразуемых данных: 64-битовые алгоритмы (**Hawk-64**, **Video-64**) и 128-битовые алгоритмы (**Hawk-128**, **Video-128**), ориентированные на реализацию в программируемых логических интегральных схемах.

6. Разработаны поточные алгоритмы маскирующей обработки информации с использованием латинских квадратов: 1) латинский квадрат на основе УППС; 2) латинский квадрат на основе блочных алгоритмов.

7. Выполнен комплекс статистических исследований по экспериментальному тестированию разработанных алгоритмов. Результаты эксперимента показали, что статистические критерии удовлетворяются полностью.

8. Выполнена оценка стойкости разработанных алгоритмов к известным методам анализа: дифференциальному, линейному. Результаты анализа

показали, что разработанные алгоритмы являются стойкими и к данным видам анализа. Проведено экспериментальное исследование, подтвердившее полученные теоретические оценки.

9. Выполнена оценка сложности аппаратной реализации разработанных алгоритмов. Полученные результаты показывают, что разработанные алгоритмы являются более эффективными за счет снижения сложности аппаратной реализации для рассматриваемой реализации по сравнению с известными алгоритмами.

Публикации в журналах, входящих в перечень ВАК

1. Хо Нгок Зуй. Варианты построения операционных блоков управляемых битовых перестановок / Хо Нгок Зуй, Д. Н. Молдовян, Н. А. Молдовян // Вопросы защиты информации. -2010. -№ 3(90). -С. 2-11.

2. Молдовян Д. Н. Конечные группы с четырехмерной цикличностью как примитивы цифровой подписи / Д. Н. Молдовян, П. А. Молдовяну, Хо Нгок Зуй // Информационно-управляющие системы. -2010. -№ 3(64). -С. 61-68.

3. Молдовян Н. А. Протокол слепой коллективной подписи на основе сложности задачи дискретного логарифмирования / Н. А. Молдовян, Хо Нгок Зуй, Д. К. Сухов // Известия СПбГЭТУ «ЛЭТИ». -03/2011. -№ 3. -С. 19-24.

4. Хо Нгок Зуй. Разработка управляемых подстановочно-перестановочных сетей на основе управляемых элементов $F_{2/3}$ для синтеза скоростных блочных шифров / Хо Нгок Зуй, А. А. Молдовян // Известия СПбГЭТУ «ЛЭТИ». -06/2011. -№ 6. -С. 25-30.

Прочие публикации

5. Морозова Е. В. Лавинный эффект в управляемых подстановочно-перестановочных сетях различных порядков / Е. В. Морозова, Хо Нгок Зуй, М. В. Шилков // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции,22-23 ноября 2008, г. Санкт-Петербург. СПб.: ВАС, 2008. -С. 417-421.

6. Молдовян Д. Н. Команда управляемой перестановки битов для процессоров универсального назначения / Д. Н. Молдовян, Хо Нгок Зуй // XI Санкт-Петербургская международная конференция Региональная информатика-2010 (РИ-2010) СПб, 22-24 октября 2010 г. Материалы конференции. -СПб, 2010. -С. 121.

7. Хо Нгок Зуй. Разработка и исследование нового класса управляемых элементов $F_{2/3}$ / Хо Нгок Зуй // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции, 25-26 ноября 2010, г. Санкт-Петербург. -СПб.: ВАС, 2010. -С. 419-424.

8. Nguyen M. H. On Functionality Extension of the Digital Signature Standards (Функциональное расширение стандартов электронной цифровой подписи) / M. H. Nguyen, D. N. Ho, D. H. Luu, A. A. Moldovyan, N. A. Moldovyan // The 2011 International Conference on Advanced Technologies for Communications (ATC/REV), Da Nang, 2011. -PP. 6-9.