На правах рукописи

ШНИПЕРОВ Алексей Николаевич

Компьютерные методы защиты информации на основе управляемых операций

05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

А В Т О Р Е Ф Е Р А Т

диссертации на соискание учёной степени

кандидата технических наук

Красноярск – 2008

Работа выполнена в Политехническом институте Сибирского федерального университета (СФУ)

Научный руководитель:	кандидат физико-математических наук, профессор ПИ СФУ **Виктор Иванович Томилин** (г. Красноярск).
Официальные оппоненты:	доктор физико-математических наук, доцент **Константин Владимирович Сафонов** (г. Красноярск).
	кандидат технических наук, доцент **Тамара Михайловна Пестунова** (г. Новосибирск).
Ведущая организация:	Кафедра безопасности информационных технологий Сибирского государственного аэрокосмического университета (г. Красноярск).

Защита состоится **29 мая 2008 г.** в $14^{\underline{00}}$ часов на заседании диссертационного совета ДМ 212.099.05 в Политехническом институте СФУ по адресу: 660074, г. Красноярск, ул. акад. Киренского, 26, ауд. Г418.

Ваш отзыв в двух экземплярах, заверенный гербовой печатью организации, просим направлять по адресу: 660074, г. Красноярск, ул. Киренского, 26, Политехнический институт Сибирского федерального университета, учёному секретарю диссертационного совета ДМ 212.099.05 Е. А. Вейсову.

С диссертацией можно ознакомиться в библиотеке Политехнического института СФУ.

Автореферат разослан "29" апреля 2008 г. и выставлен на сайте СФУ по адресу: http://sfu-kras.ru/science/dissertations.

Ученый секретарь диссертационного совета
кандидат технических наук, профессор Е. А. Вейсов

Актуальность. В настоящее время вопросы, связанные с информационной безопасностью, являются очень актуальными в силу стремительного развития информационных технологий практически во всех сферах деятельности человека. В связи с этим решение данных вопросов является очень важной научно-технической задачей.

Наиболее распространёнными методами решения задачи обеспечения конфиденциальности данных, циркулирующей в различных автоматизированных информационных системах, являются методы шифрования информации. При этом к этим методам (не зависимо от технологического исполнения) предъявляются чрезвычайно высокие требования, которые продиктованы как раз стремительным развитием радиотехнических средств (в том числе и вычислительных). Ужесточение требований по стойкости к вскрытию обусловлено тем, что разностороннее использование криптографии связано с более широкими возможностями для атакующего следовать особенностям конкретных условий, в которых функционирует шифр (например, имеются возможности: первая – осуществить внешнее воздействие на устройство шифрования с целью вызвать случайные аппаратные сбои, вторая – выполнить замер потребляемой мощности, третья – определить время вычислений и т. п.). Возросшие требования по скорости связаны с необходимостью сохранения высокой производительности автоматизированных систем после встраивания в них механизмов защиты. Простота программной (аппаратной) реализации обуславливает снижение стоимости средств шифрования, что, в свою очередь, способствует их массовому применению и расширению возможностей их встраивания в портативную аппаратуру.

Характерной особенностью современных шифров как с программной, так и аппаратной ориентацией является использование алгоритмов преобразования данных с предвычислениями, которые вносят существенные ограничения по быстродействию и зачастую требуют значительных вычислительных затрат, особенно при частой смене ключей. В связи с этим весьма важным становится существенное сокращение объёма предвычислений при сохранении высоких показателей нелинейности преобразований. Удачным решением данной задачи представляется полный отказ от предварительного преобразования секретного ключа путем замены этой процедуры операциями преобразования подключей в зависимости от преобразуемых данных, которые выполняются одновременно с операциями преобразования данных.

Таким образом, актуальной задачей в области компьютерных методов защиты информации является разработка скоростных шифров нового поколения, допускающих экономичную программную реализацию, сохраняющую как высокую скорость шифрования, так и нелинейность преобразований, даже при частой смене ключей. Одним из перспективных направлений построения скоростных шифров представляется использование гибких операций и/или процедур преобразования информации путём синтеза из них высокоэффективных методов шифрования.

Объект исследований. Теоретическая и практическая криптография в вычислительной технике.

Предмет исследований. Программные реализации высокоскоростных симметричных блочных шифров на основе бинарных управляемых операций.

Основная цель и задачи работы. Целью настоящей работы являются теоретическое и экспериментальное исследования управляемых бинарных операций, на основе которых можно программно реализовать высокоскоростные симметричные шифры (криптосистемы) с целью внедрения их в качестве программных модулей в различные автоматизированные системы обработки и передачи информации.

В ходе выполнения работы были поставлены и решены следующие основные задачи:

- проанализировать классические и современные симметричные криптосистемы, а также элементарные криптографические примитивы, на основе которых они построены;
- осуществить теоретический анализ управляемых бинарных операций, на базе которых можно программно синтезировать различные блоки преобразования информации (БПИ);
- разработать новые методы реализации программно-ориентированных симметричных шифров на основе БПИ, одновременно обеспечивающие высокую скорость и нелинейность преобразований;
- осуществить их обобщённый теоретический анализ на предмет стойкости к дифференциальному и линейному аналитическим исследованиям;
- разработать новый способ программной реализации блочного шифра, базирующегося на БПИ;
- исследовать на практике полученный блочный шифр на предмет скоростных характеристик и показателей нелинейности преобразований.

Методы исследований. При решении поставленных задач использовались: основные положения теории чисел (*конечные числовые поля*), классической и современной криптографии, элементы теории групп, методы математической статистики, теории вероятности, дискретной математики, а также современные методы построения программных комплексов и системного программирования.

Научная новизна. Новыми являются следующие результаты работы:

- предложены новые методы реализации программных шифров на основе блоков управляемых операций (в том числе оптимизированных с целью распараллеливания преобразований), позволяющие, в отличие от своих аналогов, осуществлять скоростное кодирование данных с высокими показателями нелинейности преобразований;
- впервые предложено оригинальное теоретическое обоснование стойкости программных симметричных шифров на базе управляемых подстановочных операций к линейному и дифференциальному аналитическим исследованиям;
- представлено новое программное обеспечение, реализующее симметричный блочный шифр на основе подстановочно-перестановочной сети преобразования двоичных данных (программный продукт *CryptoStar*), соче-

тающий в себе как высокую скорость работы, так и нелинейность преобразований;

- разработано и впервые представлено программное обеспечение для практической оценки скоростных и вероятностно-статистических характеристик симметричных шифров, в том числе и на основе управляемых операций (программный комплекс *CryptoT*), позволяющее осуществлять практическое исследование вероятностно-статистических свойств симметричных шифров.

На защиту выносятся:

- основные результаты теоретического анализа известных вариантов синтеза управляемых перестановочных и подстановочных операций;
- новые методы реализации программно-ориентированных симметричных шифров на основе управляемых операций, в том числе и их раундовые преобразования;
- программный симметричный блочный шифр (программный продукт *CryptoStar*) на базе управляемых операций, а также варианты его практического применения в задачах кодирования и защиты информации для вычислительных машин и комплексов;
- результаты практического исследования разработанного программного продукта на предмет скоростных характеристик и показателей нелинейности преобразований.

Практическая значимость исследований:

1. Предложены к использованию и апробированы новые методы программной реализации симметричных шифров, основанных на управляемых бинарных операциях и имеющие очень высокие показатели по быстродействию и нелинейности преобразований.

2. Разработано и апробировано программное решение нового блочного шифра (программный продукт *CryptoStar*), позволяющее организовать высокоскоростное шифрование информационных потоков данных в различных автоматизированных системах управления.

3. Созданное по результатам проведённых исследований программное обеспечение симметричного блочного шифрования *CryptoStar* позволит при незначительных трудозатратах обеспечить высокоэффективную (в показателях скорости и нелинейности преобразований) защиту информации, циркулирующей в высокоскоростных компьютерных сетях, в том числе и при частой смене ключей.

Достоверность научных положений работы обуславливается корректностью исходных посылок и преобразований, использованием апробированного математического аппарата, логической обоснованностью выводов. Достоверность результатов подтверждается практическими испытаниями созданного программного продукта на основе методики, предложенной членами Нового европейского проекта по созданию базовых криптографических примитивов (*NESSIE*).

Реализация и внедрение результатов работы. Основные результаты исследований использованы в качестве:

- разработанного программного обеспечения симметричного шифрования на основе управляемых операций *CryptoStar* (авторское св-во о государственной регистрации программы для ЭВМ «Роспатент» № 2006611273 от 14.04.2006 г.) в Сибирском федеральном университете, г. Красноярск;
- предложенных программно-ориентированных методов реализации высокоскоростных шифров на основе управляемых операций в Московском государственном институте электроники и математики (технический университет), г. Москва;
- программного обеспечения высокоскоростного шифрования (*CryptoStar*) в локальной компьютерной сети ФГУП ЦКБ «Геофизика», г. Красноярск.

Апробация результатов диссертации. Результаты работы докладывались и обсуждались на следующих научно-технических конференциях: Всероссийская конференция с международным участием «Современные проблемы радиоэлектроники», г. Красноярск (2004, 2005, 2006, 2007 гг.); Международная научно-практическая конференция «Информационная безопасность», г. Таганрог (2005, 2007 гг.); Международная научно-методическая конференция «Дистанционное образование – информационная среда XXI века», г. Минск (2004, 2005 гг.); Международная научная студенческая конференция «Студент и научно-технический прогресс», г. Новосибирск (2006, 2007 гг.); Всероссийская научно-практическая конференция с международным участием «Современные информационные технологии в науке, образовании и практике», г. Оренбург (2007 г.). Программные продукты, созданные в ходе исследования, демонстрировались на ряде выставок в Минске, Новосибирске и Оренбурге.

Публикации. По теме диссертации опубликовано 18 печатных работ, в том числе 1 в научно-практическом журнале «Информационные технологии» (перечень ВАК), получено 1 авторское свидетельство о государственной регистрации программы для ЭВМ. Основные печатные работы, отражающие полученные новые результаты исследования, опубликованы без соавторства.

Работа выполнялась в ходе реализации проекта «Развитие системы центров коллективного пользования (ЦКП) с удаленным доступом» (Государственный контракт на выполнение работ для государственных нужд № П 273 от 22.09.2006 г. в рамках Федеральной целевой программы развития образования на 2006–2010 годы). Автором было разработано и внедрено в эксплуатацию программное обеспечение высокоскоростного симметричного шифрования для обеспечения защиты информации, циркулирующей в интернет-портале ЦКП.

Структура и объём диссертации. Диссертационная работа состоит из введения, 3 глав, заключения, списка литературы (46 наименований) и 3 приложений. Основной текст содержит 136 страниц, иллюстрируется 57 рисунками.

СОДЕРЖАНИЕ РАБОТЫ

Во введении приведена общая характеристика работы, обоснована актуальность создания новых методов реализации программных шифров, одновре-

менно обладающих высокими показателями скорости шифрования и нелинейности преобразований, сформулированы цель и задачи диссертационной работы.

В первой главе рассмотрены общие вопросы реализации блочных и поточных симметричных шифров (криптосистем), а также приведён теоретический анализ управляемых операций.

Работа симметричных шифров включает в себя два преобразования:

$$C = E_k(m) \text{ и } m = D_k(C), \tag{1}$$

где m – открытый текст, E – шифрующая функция, D – функция дешифрования, k – секретный ключ, C – шифротекст. Заметим, что как шифрующая, так и расшифровывающая функции общеизвестны и тайна сообщения при известном шифротексте зависит только от длины и вероятностно-статистических характеристик ключа k. Также очевидно, что число возможных ключей в симметричного шифра должно быть очень велико. Это требование возникает в связи с тем, что при проектировании метода кодирования необходимо учитывать самый плохой сценарий развития событий, т. е. считать, что гипотетический противник:

- обладает полной информацией о шифрующем (расшифровывающем) алгоритме;
- имеет в своём распоряжении некоторое количество пар (открытый текст, шифротекст), ассоциированных с истинным ключом k.

Если количество возможных ключей мало, то атакующий имеет возможность взломать шифр простым перебором вариантов. Он может шифровать один из данных открытых текстов, последовательно используя разные ключи, до тех пор, пока не получит соответствующий известный шифротекст.

Далее в первой главе изложена общая концепция поточного и блочного шифрований, отмечены их основные достоинства и недостатки. Рассмотрены особенности проектирования регистров сдвига с линейной обратной связью для поточных шифров, а также базовая схема *SP*-сети Фейстеля в блочных шифрах. Рассмотрены наиболее популярные блочные и поточные шифры: поточные криптосистемы *A*5, *RC*4, *Lili*-128, блочные шифры *Blowfish*, ГОСТ 28147–89, *Rijndael.*

Также в первой главе утверждается, что главным недостатком практически всех программных симметричных шифров является то, что они либо не обеспечивают нужной скорости шифрования, либо не обладают достаточной нелинейностью преобразований. Отмечается, что значительное повышение скорости кодирования с сохранением высокой нелинейности преобразований является очень сложной научно-технической задачей.

Определяющим фактором быстродействия программных (аппаратных) шифров является наличие предвычислений, а также уровень их сложности. Практически все современные блочные симметричные шифры содержат в себе алгоритм разворачивания секретного ключа. Как показывает практика, именно этот алгоритм и вносит значительные задержки в скорости шифрования, особенно при частой смене ключа шифрования, отнимая до 70 % процессорного времени. Более того, эффективная аппаратная реализация алгоритма разворачивания ключа зачастую требует существенных схемотехнических ресурсов.

Таким образом, поворотным решением в проектировании высокоскоростных (1 Гбит/с и более при произвольной частоте смены секретных ключей), надёжных и гибких программных шифров представляется полный отказ от предварительного преобразования секретного ключа путём замены этой процедуры операциями преобразования подключей в зависимости от преобразуемых данных.

Далее в первой главе приводится детальный теоретический анализ двух основных типов управляемых операций: перестановочных и подстановочных. Отмечается, что в научных работах по данной теме уже были описаны попытки построения программных шифров на основе управляемых операций, зависящих от ключа, которые, однако, не могли конкурировать по быстродействию или степени нелинейности преобразований с другими симметричными шифрами. Основная причина этого заключается в том, что битовая перестановка, зависящая от ключа, остаётся строго линейной операцией, поскольку она является фиксированной после ввода ключа.

Для устранения этого недостатка в фиксированную перестановку включается дополнительный управляющий вектор. Тогда для k фиксированных перестановок $\pi^{(0)}, \pi^{(1)}, ..., \pi^{(k-1)}$ длины n, принадлежащих S_n (множеству всех перестановок), параметрическое преобразование $\pi(i, j)$, заключающееся в применении перестановки $\pi^{(j)}$ к аргументу i, где $i \in \{1,2,...,n\}$, можно рассматривать в качестве операционного блока управляемых перестановок.

Таким образом, для заданного множества перестановок $\pi^{(0)}, \pi^{(1)}, ..., \pi^{(k-1)}$ длины n блоком управляемых перестановок (БУП) является отображение $\pi(i, j)$, такое, что $\forall i \in \{1,2,...,n\}$ и для каждого фиксированного значения $j \in \{0,1,...,k-1\}$ имеет место равенство $\pi(i, j) = \pi^{(j)}(i)$.

В частности, для случая $k = 2^m$ параметр j может быть представлен двоичным вектором $V \in GF(2)^m$, а именно $j = \alpha(V)$, например:

$$j = \alpha(V) = /V/ = v_1 + v_2 2^1 + ... + v_m 2^{m-1} \text{ и } \sigma^{(j)} = \sigma^{(/V/)}. \quad (1)$$

Поскольку каждая перестановка $\pi^{(j)}$ задаёт биективное подстановочное преобразование $P_{\pi^{(j)}} : GF(2)^n \to GF(2)^n$, то блок управляемых перестановок $\pi(i, j)$ формирует блок управляемых подстановок $P(X, j) = P^{(j)}(X)$, где $X \in GF(2)^n$. Для случая $j = \alpha(V)$ обозначим операцию $P_{\pi^{(j)}} = P_{\pi^{(\alpha(V))}}$ через $P_V(X)$.

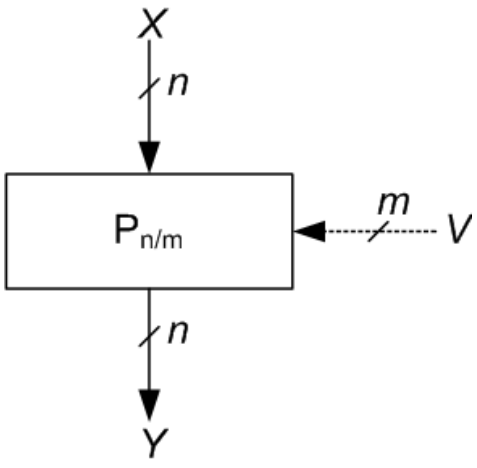


Рис. 1. Блок управляемых перестановок $P_{n/m}$

Тогда отображение вида $P_{n/m}(X, V)$ $\left[GF(2)^n \times GF(2)^m \to GF(2)^n \right]$, представляющее собой объединение 2^m подстановок $P_{\pi^{(j)}} \in S_{2^n}$, является $P_{n/m}$-блоком управляемых перестановок, если

для каждого фиксированного значения $V \in GF(2)^m$ задана некоторая перестановка $\pi_V = \pi^{(\alpha(V))} \in S_n$,
такая, что

$$P_{n/m}(X,V) = P_V(X) = P_{\pi^{(\alpha(V))}}(X) = P_{\pi_V}(X). \qquad (2)$$

Таким образом, отображение $P^{-1}_{n/m}(X,V)$ $(GF(2)^n \times GF(2)^m \to GF(2)^n)$, представляющее собой объединение 2^m подстановок $P_V^{-1} = P_{\pi_V^{-1}} \in S_{2^n}$, является обратным блоком управляемых перестановок по отношению к блоку $P_{n/m}(X,V)$ или просто обратным преобразованием, если блок $P_{n/m}(X,V)$ $(GF(2)^n \times GF(2)^m \to GF(2)^n)$ – объединение 2^m подстановок $P_V = P_{\pi_V} \in S_{2^n}$.

Далее рассматривается понятие управляемого подстановочного преобразования. В современных аппаратных блочных шифрах такие преобразования, как правило, связаны с применением криптографических примитивов двух типов:

- специальных нелинейных *S*-блоков, задаваемых в табличном виде;
- стандартных арифметических или алгебраических операций, реализующихся в командах исполняемого процессора.

Использование в блочных шифрах примитивов первого типа связано с разбиением преобразуемого блока данных из *n* битов на подблоки по *k* битов и с формированием для этих подблоков небольших подстановок (*S*-блоков). Таблицы, определяющие такие подстановки, имеют размер, пропорциональный величине 2^k. Недостатки табличного представления подстановочных преобразований заключаются в сложности их аппаратной реализации и быстром увеличении размеров таблиц с ростом значения *k*. Это обстоятельство делает проблематичным применение больших *S*-блоков как при аппаратной, так и при программной реализациях блочных шифров. В связи с этим размеры *S*-блоков ограничиваются в основном 4–8 битами. Это существенно ухудшает ряд вероятностно-статистических свойств преобразований, осуществляемых над всем блоком данных размера *n*, а также уменьшает общее многообразие (число модификаций) таких преобразований.

Подстановочные примитивы второго типа достаточно эффективно реализуются как стандартные операции в программном виде. Однако эти операции либо осуществляют линейные преобразования (операция XOR), либо имеют низкую нелинейность (операция сложения по модулю 2^n), либо связаны со сложностью вычислений (операции возведения в степень, умножения по модулю 2^n или простому модулю и др.).

Касаясь в общих чертах перечисленных свойств подстановочных примитивов, отмечаем в данной главе, что *S*-блоки предназначены для обеспечения заданных в пределах каждого *S*-блока степени нелинейности и степени распространения ошибок.

Таким образом, в заключение первой главы делаются выводы о недостатках современных программных симметричных шифров, которые прежде всего связаны со сравнительно низкими показателями скорости, и об очевидной необходи-

мости разработки новых методов программной реализации высокоскоростных симметричных шифров, обладающих высокими показателями нелинейности преобразований.

Во второй главе рассматриваются различные новые методы реализации программно-ориентированных симметричных шифров на основе управляемых перестановочных и подстановочных операций. Все рассмотренные в данной главе новые программные шифры представляют собой дальнейшее развитие известных аппаратных алгоритмов *SPECTR* и *COBRA* с точки зрения оптимизации под программную реализацию, скорости преобразований на универсальных процессорах архитектуры x86, распараллеливания преобразований, а также с точки зрения высокой степени нелинейности преобразований.

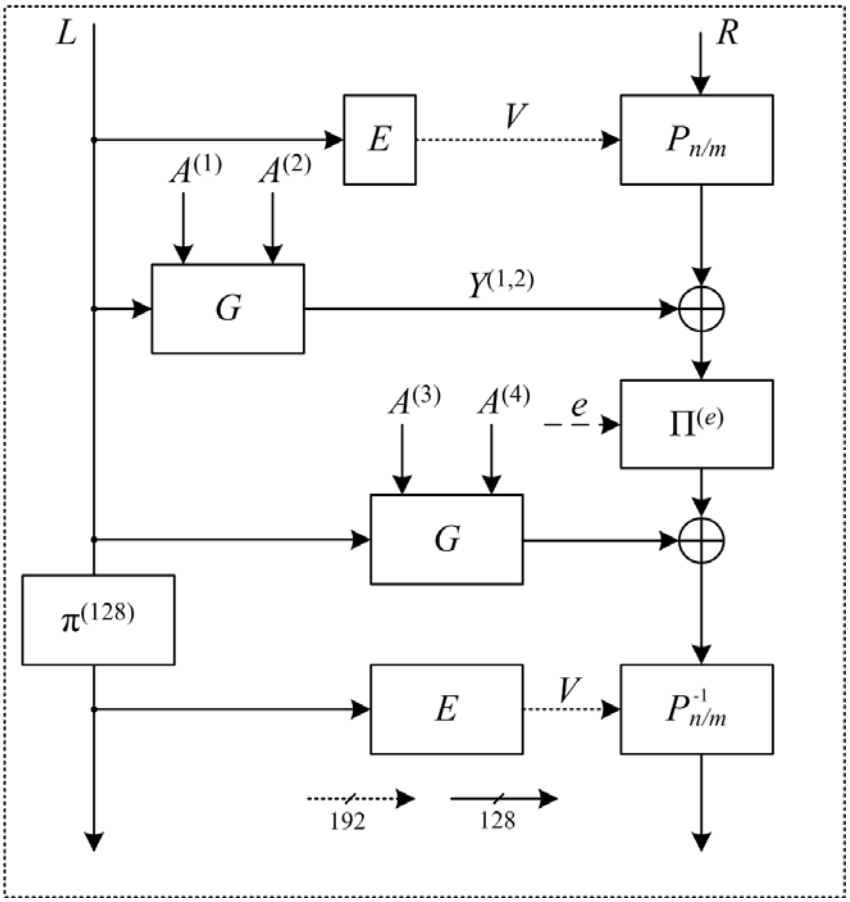


Рис. 2. Общий вид раундовой процедуры преобразования с переключаемой операцией

Как уже отмечалось в первой главе, достоинством управляемых перестановок является то, что влияние одного входного бита на все выходные обеспечивается за минимальное время задержки. Однако данное преобразование сохраняет значение веса Хэмминга. В связи с этим при реализации программно-ориентированных шифров представляется разумным дополнительно с перестановочными операциями использовать преобразования другого типа, которые изменяют вес и четность битов преобразуемых двоичных векторов. В качестве такой операции целесообразно использовать операции, подобные управляемой двухместной операции *G*, фиксированной перестановочной инволюции ***I***, а также параметрической переключаемой операцией $\Pi^{(e)}$.

На рис. 2 представлена принципиальная схема процедуры раундового преобразования, построенная на базе управляемых перестановочных и переключаемых операций. Приведённая схема и является основной процедурой кодирования данных нового программного шифра, рассмотренного в главе 2. Отмечается, что в данной схеме раундового преобразования используется оптимизированная одноцикловая перестановка $\Pi^{(e)}$, механизм оптимизации которой заключается в том, что бит из *j*-го разряда на входе блока $P_{n/m}$ попадает с примерно одинаковой веро-

ятностью во все выходные разряды блока $P_{n/m}^{-1}$, кроме j-го, в который он не попадает ни при каком значении управляющего вектора.

Далее во второй главе рассматривается новый программно-ориентированный симметричный шифр на основе управляемых операций и инволюций, приводится схема одного раунда преобразования. Чтобы избежать использования дополнительных активных элементов в качестве промежуточной фиксированной перестановки нами была применена перестановочная инволюция, содержащая только циклы длины 2. В этом случае, как и в случае использования одноцикловой перестановки, для всех значений j в одном раунде не обеспечивается влияние j-го входного бита на j-й выходной. Эта неравномерность в следующем раунде выравнивается, что позволяет отказаться от наложения различных раундовых подключей при формировании управляющих векторов, соответствующих прямому и обратному БУП.

Далее рассматриваются различные разработанные схемы раундовых преобразований, в которых были использованы несколько инволюций, фиксированные подстановочные операции, а также операции циклического сдвига.

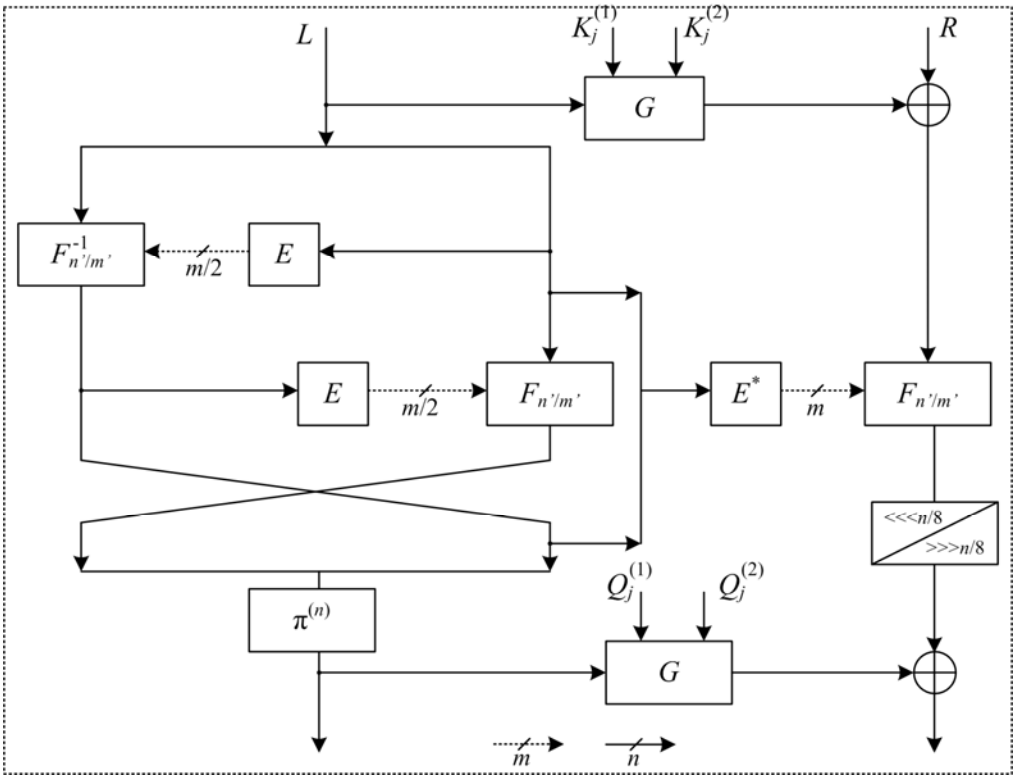


Рис. 3. Раунд шифрования с нелинейным преобразованием левого подблока и экономичной переключаемой операцией в правой ветви схемы шифрования

Для реализации преобразования всего блока данных в рамках одного раунда с сохранением достаточно высокого параллелизма вычислений во второй главе представлена новая многораундовая и программно-ориентированная процедура, которая базируется на принципах преобразования данных аппаратного шифра *COBRA*. Её основная процедура преобразования данных описана рядом новых принципиальных схем, оптимизированных по скорости многопоточного преобразования на универсальных многоядерных процессорах. Одна из таких схем раундового преобразования представлена на рис. 3.

Также во второй главе детально рассматривается новый программный блочный шифр (программный продукт *CryptoStar*). Отмечается, что данный шифр был разработан на основе уже известного аппаратно-ориентированного алгоритма

*COBRA-H*64 с учётом показателей стойкости к линейному и дифференциальному аналитическим анализам. Несмотря на то, что в общем этот аппаратный алгоритм является стойким к этим видам анализа, отмечается ряд его принципиальных недостатков, которые нами были решены путём существенной модернизации раундовых преобразований.

Отметим следующие отличия программного блочного шифра от его аппаратного прототипа *SPECTR-H*64:

- в раундовом преобразовании шифра *CryptoStar* используются два БУП второго порядка $P_{128/320}$ и $P^{-1}_{128/320}$, тогда как в *SPECTR-H*64 – три БУП первого порядка: два блока $P_{32/80}$ и один $P^{-1}_{32/80}$. Это позволяет в первом шифре существенно увеличить размерность обрабатываемых данных при достаточно равномерном распределении влияния управляющего подблока на выполнение битовых перестановок;
- в раунде *CryptoStar* используются две одинаковые нелинейные операции *G*, а в *SPECTR-H*64 – только одна;
- благодаря предыдущей особенности в принципиальной схеме раундового преобразования *CryptoStar* оказалось возможным задать над управляющим подблоком выполнение перестановочной инволюции, которая позволила отказаться от использования ключей при формировании управляющих векторов, соответствующих взаимно обратным БУП;
- в *CryptoStar* используется новый криптографический примитив – переключаемая операция, хотя и в наиболее простом варианте. Её использование позволило устранить наличие слабых и полуслабых ключей;
- в раунде шифра *CryptoStar* используется параметрическая операция циклического сдвига, зависимая от веса Хэмминга управляющего вектора, формализованного на основе преобразуемых данных.

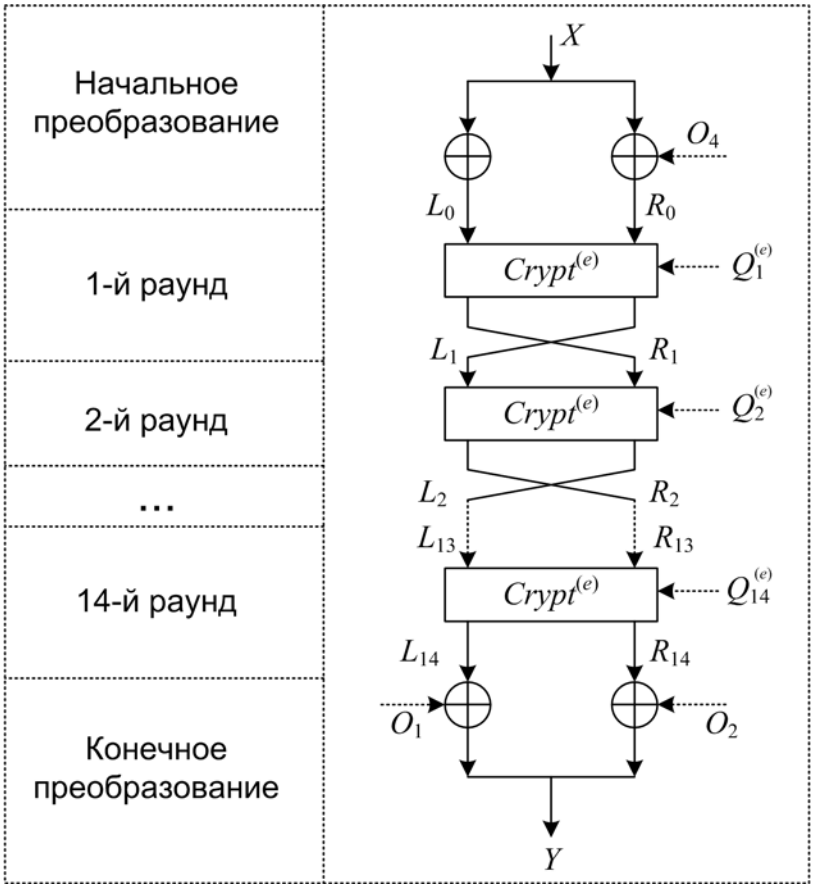


Рис. 4. Общая схема преобразования данных в программном шифре *CryptoStar* ($r = 14$)

Общая схема шифрования и расшифровывания в программном шифре *CryptoStar* определяется следующими преобразованиями: $Y = T^{(0)}(X, K)$

и $X = T^{(1)}(Y, K)$, где $X \in \{0,1\}^{256}$ – открытый текст (входной блок); $Y \in \{0,1\}^{256}$ – шифротекст (выходной блок); $K \in \{0,1\}^{512}$ – секретный ключ; $T^{(e)}$ – функция преобразования блока данных; $e \in \{0,1\}$ – параметр, определяющий режимы зашифровывания ($e = 0$) и расшифровывания ($e = 0$).

Секретный ключ рассматривается как объединение четырёх подключей $K = (K_1, K_2, K_3, K_4)$, где $K_i \in \{0,1\}^{128}$ для всех $i = 1,2,3,4$. Общая схема шифрования представляет собой четырнадцатираундовую итеративную структуру с очень простыми начальным и конечным преобразованиями (рис. 4). При выполнении каждого *j*-го раунда ($j = 1,2,...,14$) применяется раундовый ключ $Q_j^{(e)}$, формируемый на основе непосредственного использования всех четырёх подключей K_1, K_2, K_3, K_4 без выполнения каких-либо специальных процедур преобразования (расширения) секретного ключа, т. е. каждый ключ $Q_j^{(e)}$ формируется как простая последовательность секретных подключей K_i, применяемых в порядке, заданном достаточно простым расписанием ключей.

Процедура шифрования начинается с начального преобразования IT. Затем выполняется 14 раундов шифрования в соответствии с процедурой $Crypt^{(e)}$, за которыми следует конечное преобразование FT.

Далее во второй главе рассматриваются механизм формирования расписания использования ключа, механизмы генерации подключей, а также принципы рассеивания и перемешивания.

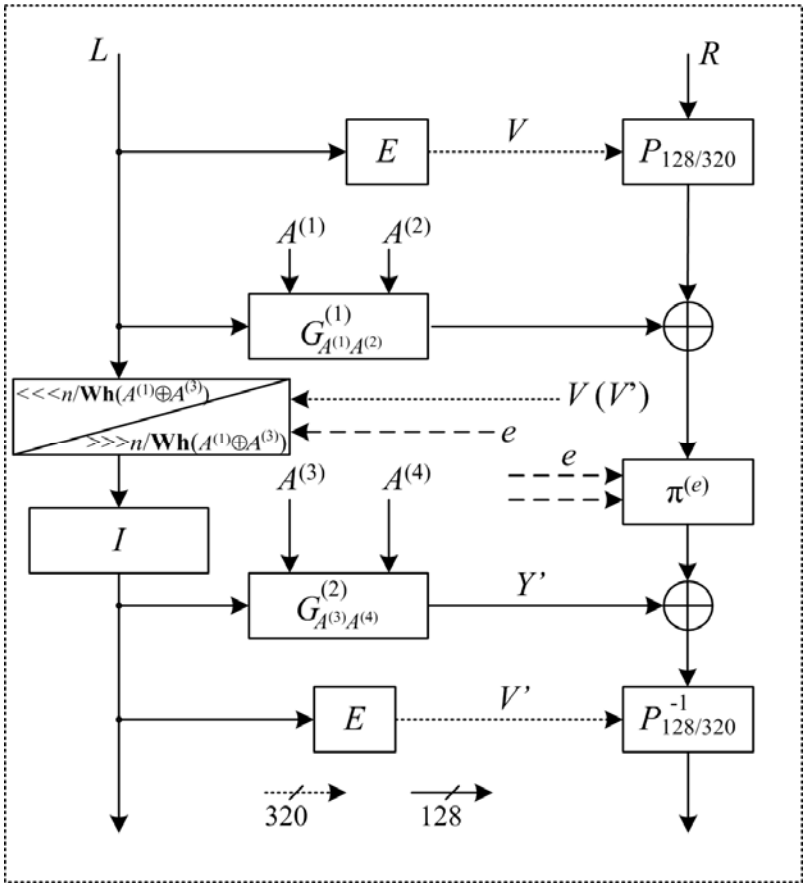


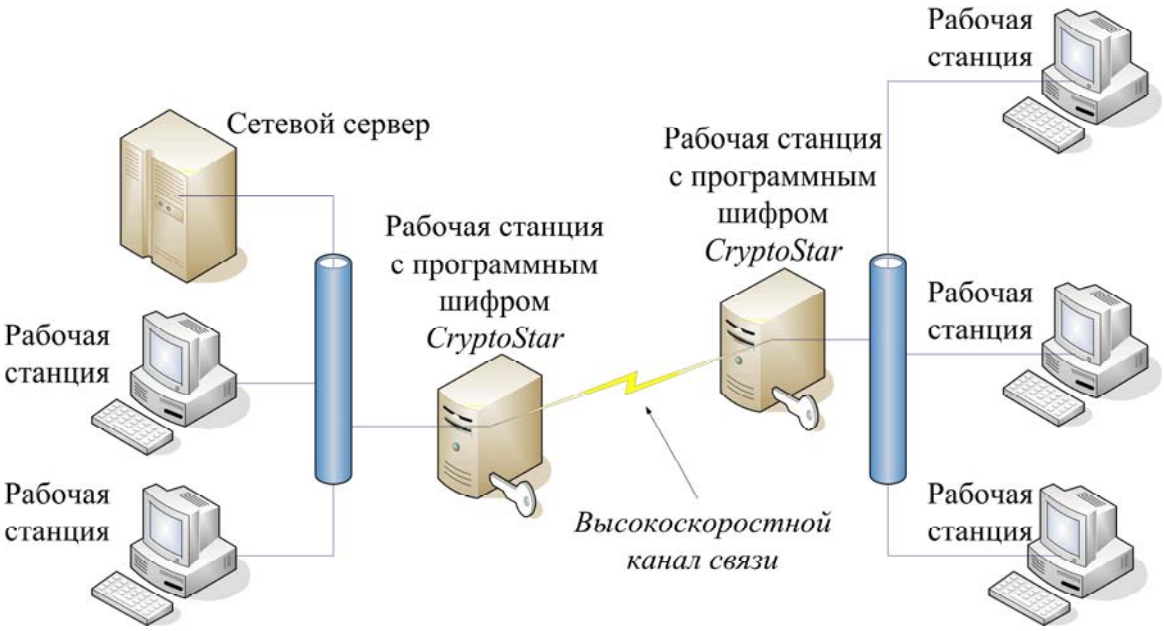
Рис. 5. Раунд яифрования программного шифра *CryptoStar*

Принципиальная схема одного раунда шифрования $Crypt^{(e)}$ блочного шифра *CryptoStar* представлена на рис. 5. Отмечается, что программно-ориентированный шифр *CryptoStar* представляет собой законченный программный продукт (св-во о государственной регистрации программы для ЭВМ «Роспатент» № 2006611273), реализованный с использованием объектно-ориентированных языков программирования *C++* и *C#*. Программный шифр адаптирован под современные универсальные

процессоры, чему способствовало наличие низкоуровневых макрокоманд, поддерживающих особенности наборов *SSE*, *SSE*2 и *SSE*3.

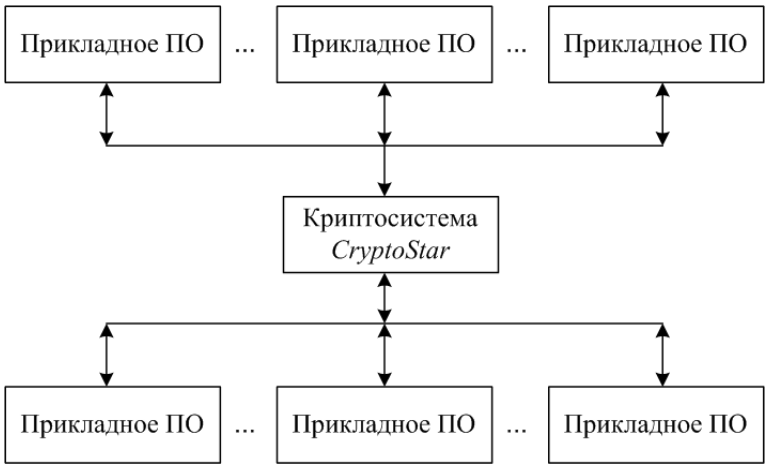
Также следует отметить, что программное решение *CryptoStar* оптимизировано под многоядерные процессоры, что обусловлено поддержкой многопоточных вычислений. Варианты практического применения программного продукта *CryptoStar* представлены функциональными схемами работы в межпрограммном и сетевом режимах (рис. 6).

Также во второй главе приведено авторское математическое описание механизмов влияния новых криптографических примитивов – управляемых подстановочных операций – на стойкость программно-ориентированных блочных шифров к дифференциальному и линейному аналитическим анализам.



а

Показана перспективность использования управляемых подстановочных и перестановочных операций в качестве криптографических примитивов при разработке новых программных методов реализации высокоскоростных программных шифров с высокими показателями нелинейности преобразований.



б

Рис. 6. Функциональная схема работы шифра *CryptoStar* в сетевом (*а*) и межпрограммном (*б*) режимах

Отмечено, что блочный шифр *CryptoStar* обладает рядом функциональных элементов, которые обеспечивают ему устойчивость к некоторым техническим видам атак, например к атаке по времени.

В третьей главе рассматриваются результаты проведённых исследований программной

реализации блочного шифра *CryptoStar*, а именно скоростных и вероятностно-статистических характеристик.

Для экспериментальной проверки скоростных характеристик программного шифра *CryptoStar* нами был разработан программно-аппаратный стенд на основе *IBM PC* – совместимого персонального компьютера (*Intel Core2Duo* 2·1,83 ГГц, 1024 Мб ОЗУ, жёсткий диск 250 Гб) и оригинального программного комплекса *CryptoT* (модуль замера производительности симметричных программных шифров, модуль статистического анализа частотного распределения байт в бинарных файлах).

Данный экспериментальный стенд позволяет осуществлять замер скорости шифрования блочного шифра *CryptoStar* с точностью 1 Кбайт, а также осуществлять вероятностно-статистический анализ выходных шифрограмм на предмет критериальных оценок степени нелинейности преобразований.

Суть эксперимента по замеру производительности блочного шифра сводится к следующему: испытательное программное обеспечение последовательно генерирует несколько блоков открытого текста различного размера (100 и 500 Кбайт, 1, 50, 100 и 300 Мбайт), далее, используя внутренние функции динамической библиотеки *CryptoStar*, зашифровывает их, замеряя время шифрования каждого из них. Затем с учётом полученных временных интервалов находятся скорости шифрования каждого из этих блоков. Далее скорости усредняются и выводятся на экран монитора в виде гистограммы. Для замера скоростей расшифровывания используются полученные блоки шифротекста.

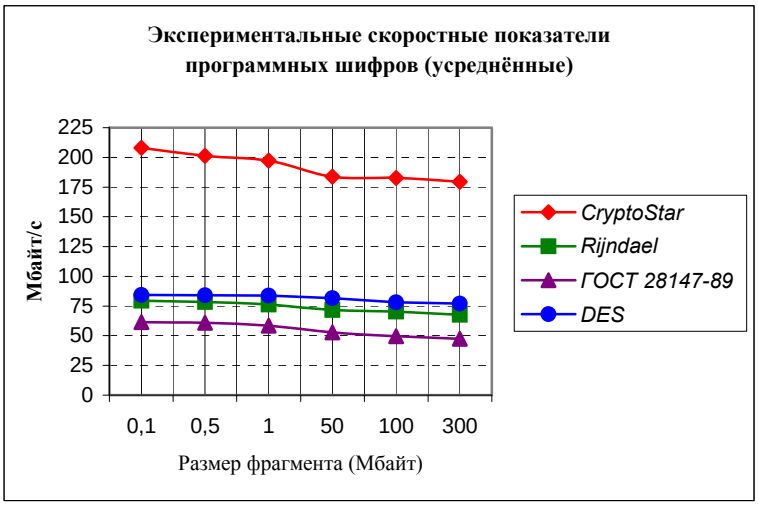


Рис. 7. Сравнительная характеристика скорости преобразований некоторых современных программных шифров

Следует отметить, что все скоростные испытания проводились с блоками данных, предварительно уже загруженными в оперативную память, т. е. все показатели не учитывают скоростные характеристики периферийных устройств (например, жёсткого диска). Сравнительная характеристика скорости преобразования некоторых современных программных шифров приведена на рис. 7.

Далее в третьей главе рассматриваются экспериментальные количественные оценки рассеивающих свойств симметричного шифра *CryptoStar*, для чего в программном комплексе *CryptoT* (с использованием которого делался анализ) была реализована применимая ко всем блочным шифрам методика, предложенная членами Нового европейского проекта по созданию базовых криптографических примитивов (*NESSIE*, *New European Schemes for Signature, Integrity and Encryption*). В частности были использованы следующие критерии рассеивающих свойств:

1. Среднее число битов выхода, изменяющееся при изменении одного бита входного вектора данных (d_1).
2. Степень полноты преобразования (d_c).
3. Степень лавинного эффекта (d_a).
4. Степень соответствия строгому лавинному критерию (d_{sa}).

Частотный анализ блочного шифра сводится к следующему: испытательное программное обеспечение последовательно генерирует несколько блоков открытого текста фиксированного размера (100 Кбайт). Каждый блок представляет собой либо упорядоченную последовательность, состоящую из 1, 10, 100 и 1000 символов, либо псевдослучайную последовательность с размерностью всего блока. Далее с помощью внутренних функций библиотеки *CryptoStar* осуществляется их зашифровывание. Полученные шифротексты обрабатываются процедурой частотного анализа, и, как результат, выводится гистограмма распределения байт в зашифрованном блоке, а также экспериментальные оценки критериев степени нелинейности преобразований. Далее в третьей главе приводятся графики частотного распределения байт в выходном шифротексте, который был получен путём зашифровывания двух блоков открытого текста, каждый из которых состоит из одного символа: 0x7F и 0x3D, с целью демонстрации лавинного эффекта.

На рис. 9 представлен один из таких графиков частотного распределения байт в выходном шифротексте, который был получен путём зашифровывания блока открытого текста, состоящего из одного символа.

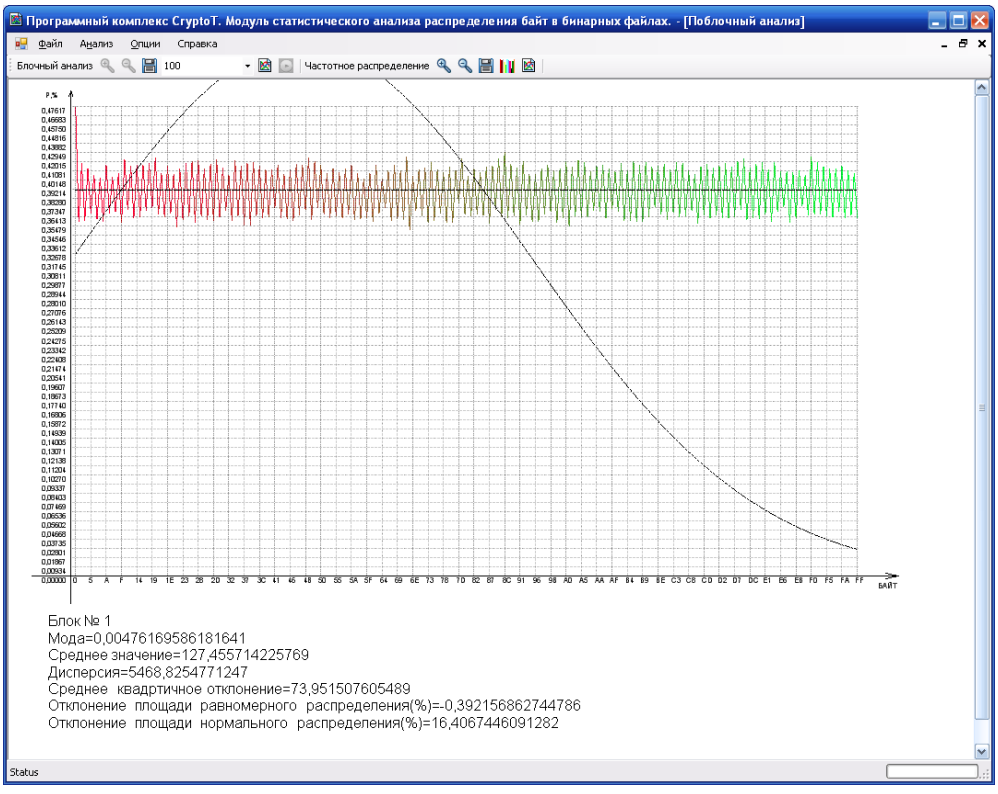


Рис. 8. Пример частотного распределения байт шифрограммы

Также приводятся усреднённые критериальные оценки: «Влияние битов открытого текста на шифротекст» (табл. 1) и «Влияние битов ключа на шифротекст» (табл. 2), которые были получены в ходе практических испытаний программного продукта *CryptoStar* с использованием множества тестовых примеров, подобранных в соответствии с рекомендациями *NESSIE*.

Далее в третьей главе приводятся экспериментальные данные оценки линейной зависимости частотного распределения блока байт «открытый текст – шифротекст». В табл. 3 представлена сравнительная характеристика некоторых современных программных шифров (на предмет линейной зависимости между блоком открытого текста и соответствующим блоком шифротекста при использовании одного ключа шифрования) в виде значений коэффициентов линейной корреляции.

Таблица 1

Значения критериев оценки влияния битов исходного текста на преобразованный текст

Число раундов	#K=1, #X=100				#K=100, #X=100			
	d_1 (1)	d_c (2)	d_a (3)	d_{sa} (4)	d_1 (1)	d_c (2)	d_a (3)	d_{sa} (4)
14	65,538	1,0000	0,9995	0,9937	65,531	1,0000	0,9993	0,9983
8	62,89	1,0000	0,9989	0,992	62,7926	1,0000	0,9991	0,9931
4	49,407	1,0000	0,9863	0,9821	49,501	1,0000	0,9835	0,9837
3	41,1056	0,9904	0,9745	0,9761	41,2893	1,0000	0,9776	0,9779
2	13,8349	0,8693	0,5326	0,5296	13,7634	1,0000	0,5344	0,5244
1	5,23468	0,3792	0,0871	0,0723	5,19702	0,4632	0,0796	0,0711

Таблица 2

Значения критериев оценки влияния битов ключа на преобразованный текст

Число раундов	#K=300, #X=25				#K=100, #X=100			
	d_1 (1)	d_c (2)	d_a (3)	d_{sa} (4)	d_1 (1)	d_c (2)	d_a (3)	d_{sa} (4)
14	65,4991	1,0000	0,9997	0,9971	65,6791	1,0000	0,9999	0,9979
8	62,9103	1,0000	0,9991	0,9934	62,8409	1,0000	0,9993	0,9964
4	49,5135	1,0000	0,9823	0,9833	50,0045	1,0000	0,9844	0,9849
3	41,2413	0,9908	0,9712	0,9772	41,304	1,0000	0,9799	0,9807
2	13,624	0,8704	0,5204	0,5304	13,6891	0,9931	0,5411	0,5504
1	5,0452	0,3689	0,0901	0,0712	5,1804	0,4705	0,0607	0,0612

Таблица 3

Сравнительная характеристика линейной зависимости «открытый текст – шифротекст»

Шифр	Размер блока открытого текста (Кбайт)	Значения коэффициентов корреляции (вход/выход шифра)				
		Блок открытого текста, состоящий из символа 0x7F	Блок открытого текста, состоящий из символа 0x3D	Блок произвольного открытого текста (№1)	Блок произвольного открытого текста (№2)	Блок произвольного открытого текста (№3)
1	2	3	4	5	6	7
CryptoStar	10	0,0079575	0,00612796	0,02898836	0,04586129	0,06870678
	200	0,0106834	0,02184563	0,03886559	0,05134023	0,06271680

Окончание табл. 3

1	2	3	4	5	6	7
DES	10	0,3749173	0,43165204	0,13045398	0,20798324	0,19468237
	200	0,4356289	0,48304230	0,29867012	0,28390861	0,17032568
Blowfish	10	0,1289012	0,11943265	0,09856269	0,09635600	0,07332569
	200	0,1632703	0,14872563	0,10586231	0,11238012	0,08723356
Rijndael	10	0,0630452	0,06789012	0,05042035	0,05789012	0,05222356
	200	0,0750124	0,08652341	0,06124503	0,04302368	0,04813125
ГОСТ 28147–89	10	0,2303526	0,22802365	0,10385623	0,09425360	0,13526771
	200	0,2432650	0,45327680	0,13256201	0,11237702	0,13985362

Таким образом, очевидно, что программный блочный шифр *CryptoStar* обладает хорошими рассеивающими свойствами даже при небольшом числе раундов. В частности, критерий полноты, согласно которому «каждый входной бит должен влиять на каждый выходной бит», выполняется уже после двух раундов преобразований. Для сравнения, в программных продуктах, реализующих алгоритмы *DES* и ГОСТ 28147–89, данный критерий выполняется не менее чем через четыре раунда шифрования данных, что обусловлено исключительно используемой схемой Фейстеля. Из данных, представленных в табл. 2, легко заметить, что даже без применения процедуры генерации расширенного секретного ключа обеспечивается достаточно сильное рассеивающее влияние каждого бита ключа на все биты преобразованного текста, что указывает на высокую стойкость к дифференциальному и линейному аналитическим методам анализа.

ОСНОВНЫЕ НАУЧНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

В данной работе решались задачи по теоретическому исследованию управляемых бинарных операций с целью программной реализации задачи защиты информации.

К числу основных результатов работы можно отнести следующие:

1. Предложены новые методы реализации программных шифров на основе блоков управляемых операций (в том числе оптимизированных с целью распараллеливания преобразований), позволяющие, в отличие от своих аналогов, осуществлять скоростное кодирование данных с высокими показателями нелинейности преобразований.

2. Впервые предложено оригинальное теоретическое обоснование стойкости программных симметричных шифров на базе управляемых подстановочных операций к линейному и дифференциальному аналитическим исследованиям.

3. Представлено новое программное обеспечение, реализующее симметричный блочный шифр на основе подстановочно-перестановочной сети преобразования двоичных данных (программный продукт *CryptoStar*), сочетающий в себе как высокую скорость работы, так и нелинейность преобразований.

4. Разработано и впервые представлено программное обеспечение для практической оценки скоростных и вероятностно-статистических характеристик симметричных шифров, в том числе и на основе управляемых операций (про-

граммный комплекс *CryptoT*), позволяющее осуществлять практическое исследование вероятностно-статистических свойств симметричных шифров.

5. Предложен новый метод программной реализации многораундового симметричного шифра на основе управляемых перестановочных и переключаемых операций.

6. Представлен новый метод программной реализации многораундового симметричного шифра, базирующегося на управляемых операциях и фиксированных инволюциях.

7. Показана перспективность использования управляемых подстановочных и перестановочных операций в качестве криптографических примитивов при проектировании программных методов высокоскоростного кодирования данных с высокими показателями стойкости к аналитическим видам анализа.

8. Предложена новая методика анализа скоростных и вероятностно-статистических качеств симметричных блочных шифров на основе управляемых операций.

9. Представлена положительная перспектива использования разработанного блочного шифра в различных радиотехнических системах обработки и передачи информации.

10. Показана теоретическая устойчивость программных шифров на основе управляемых операций к современным техническим видам атак.

При теоретическом исследовании были использованы положения теории чисел, методы дискретной математики, теории вероятности и теории программирования.

Теоретическое и экспериментальное исследования в основном обращены на подтверждение технической реализуемости программных симметричных шифров, обладающих высокими показателями скорости и нелинейности преобразований.

Научная новизна и основные положения работы, которые защищает автор, изложены во введении. Конкретные результаты и выводы даны в конце соответствующих глав.

Работа выполнена на кафедре конструирования и проектирования радиоэлектронных средств (КиПР) Политехнического института Сибирского федерального университета.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

1. **Шниперов, А. Н.** Синтез и анализ высокоскоростных симметричных криптосистем на основе управляемых операций / А. Н. Шниперов // Информационные технологии. – М.: изд-во «Новые технологии», 2008. – № 1. – С. 36–41.

2. **Шниперов, А. Н.** Методы информационной защиты и авторизации пользователей при проектировании учебно-методических комплексов / А. Н. Шниперов, В. И. Томилин // Современные проблемы радиоэлектроники: тезисы докладов Всероссийской научно-технической конференции с международным участием. – Красноярск, 2004. – С. 118–119.

3. **Шниперов, А. Н.** Защита информации в электронных учебно-методических комплексах для дистанционного обучения / А. Н. Шниперов, Б. М. Бидус, В. И. Томилин, С. И. Трегубов // Дистанционное обучение – образовательная среда XXI века: тезисы докладов Международной научно-практической конференции. – Минск, 2004. – С. 84–87.

4. **Шниперов, А. Н.** Некоторые аспекты информационной безопасности электронных учебно-методических комплексов / А. Н. Шниперов, Б. М. Бидус, С. И. Трегубов// Современные проблемы радиоэлектроники: тезисы докладов Всероссийской научно-технической конференции с международным участием. – Красноярск, 2005. – С. 679–681.

5. **Шниперов, А. Н.** Некоторые аспекты безопасности алгоритма аутентификации системы *GSM* / А. Н. Шниперов, В. И. Томилин // Современные проблемы радиоэлектроники: тезисы докладов Всероссийской научно-технической конференции с международным участием. – Красноярск, 2005. – С. 601–603.

6. **Шниперов, А. Н.** Использование управляемых битовых перестановок в криптографии / А. Н. Шниперов // Информационная безопасность: тезисы докладов Международной научно-практической конференции. – Таганрог, 2005. – С. 221–224.

7. **Шниперов, А. Н.** Элементы криптоанализа протоколов аутентификации сетей GSM / А. Н. Шниперов // Информационная безопасность: тезисы докладов Международной научно-практической конференции. – Таганрог, 2005. – С. – 170–172.

8. **Шниперов, А. Н.** Криптостойкость шифров на основе управляемых операций / А. Н. Шниперов // Информационная безопасность: тезисы докладов Международной научно-практической конференции. – Таганрог, 2005. – С. 224–226.

9. **Шниперов, А. Н.** Защита информации в системах дистанционного обучения / А. Н. Шниперов, В. И. Томилин // Дистанционное обучение – образовательная среда XXI века: тезисы докладов Международной научно-практической конференции. – Минск, 2005. – С. 76–77.

10. **Шниперов, А. Н.** Атака на сетевой сервер путём подмены одного из субъектов TCP-соединения / А. Н. Шниперов, С. И. Трегубов // Современные проблемы радиоэлектроники: тезисы докладов Всероссийской научно-технической конференции с международным участием. – Красноярск, 2006. – С. 538–541.

11. **Шниперов, А. Н.** Безопасность протокола *WEP* для беспроводных *Wi-Fi*-сетей / А. Н. Шниперов, В. И. Томилин // Современные проблемы радиоэлектроники: тезисы докладов Всероссийской научно-технической конференции с международным участием. – Красноярск, 2006. – С. 535–538.

12. **Шниперов, А. Н.** Криптосистемы на основе слоистых структур управляемых операций / А. Н. Шниперов // Студент и научно-технический прогресс: тезисы докладов Международной научно-технической конференции. – Новосибирск, 2006. – С. 95–96.

13. **Шниперов, А. Н.** Криптосистемы на основе управляемых операций / А. Н. Шниперов // Студент и научно-технический прогресс: тезисы докладов Международной научно-технической конференции. – Новосибирск, 2006. – С. 96–97.

14. **Шниперов, А. Н.** Проблемы построения блочных шифров с простым расписанием ключа // А. Н. Шниперов // Информационная безопасность: тезисы докладов Международной научно-практической конференции. – Таганрог, 2006. – С. 73–75.

15. **Шниперов, А. Н.** Некоторые аспекты криптоанализа протокола *WEP* для беспроводных сетей / А. Н. Шниперов // Информационная безопасность: тезисы докладов Международной научно-практической конференции. – Таганрог, 2006. – С. 45–48.

16. **Шниперов, А. Н.** Атака на *Bluetooth*-соединение путём подбора аутентификационного *PIN*-кода / А. Н. Шниперов // Современные проблемы радиоэлектроники: тезисы докладов Всероссийской научно-технической конференции с международным участием. – Красноярск, 2007. – С. 322–326.

17. **Шниперов, А. Н.** Алгоритм шифрования на основе тригонометрических функций / А. Н. Шниперов // Студент и научно-технический прогресс: тезисы докладов Международной научно-технической конференции. – Новосибирск, 2007. – С. 97.

18. **Шниперов, А. Н.** Высокоскоростная симметричная криптосистема на основе управляемых операций *CryptoStar* / А. Н. Шниперов // Современные информационные технологии в науке, образовании и практике: сб. науч. тр. – Оренбург: ИПК ГОУ ОГУ, 2007. – С. 154–156.

19. Программное обеспечение симметричного шифрования на основе управляемых операций (*CryptoStar*) / **А. Н. Шниперов.** – Заявка на регистрацию программы для ЭВМ № 2006610613 от 1.03.2006 г. Положительное решение от 14.04.2006 г. № 2006611273.

Соискатель: 

Подп. в печать _____. Формат 60×84/16. Бумага тип. № _____ печать.
Усл. печ. л. 1. Тираж 120 экз. Заказ _____

Сибирский федеральный университет;
660041, Красноярск, пр. Свободный, 79