На правах рукописи

МОРОЗОВА Елена Владимировна

НОВЫЕ ПРИМИТИВЫ И СИНТЕЗ ШИФРОВ С ПРОСТЫМ РАСПИСАНИЕМ КЛЮЧА

Специальность 05.13.19. - Методы и системы защиты информации, информационная безопасность

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург

2004

Работа выполнена в Научном филиале Федерального государственного унитарного предприятия «НИИ «Вектор» - Специализированном центре программных систем «Спектр»

Научный руководитель: кандидат технических наук, доцент
Молдовян Александр Андреевич

Официальные оппоненты: доктор технических наук, профессор
Яковлев Виктор Алексеевич

кандидат технических наук, доцент
Зима Владимир Михайлович

Ведущая организация: Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Защита состоится 1 июля 2004 г. в 15 часов на заседании диссертационного совета Д 212.229.22 в ГОУ ВПО «Санкт-Петербургский государственный политехнический университет» по адресу: 194064, Россия, Санкт - Петербург, Тихорецкий пр., 21, к. 301.

С диссертацией можно ознакомиться в фундаментальной библиотеке ГОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан «____» мая 2004 г.

Ученый секретарь диссертационного совета
Д 212.229.22
доктор технических наук, _____ Шашихин В.Н.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность

В настоящее время основными задачами криптографии являются обеспечение конфиденциальности, подлинности и анонимности. Традиционная задача защиты информации от несанкционированного доступа решается с помощью зашифрования данных таким образом, что расшифрование возможно только при знании секретного ключа.

Для обеспечения скоростного шифрования в автоматизированных системах и последующего произвольного доступа к зашифрованной информации обычно применяются блочные шифры. Несмотря на появление большого числа новых шифров, требования к ним с момента создания и утверждения в качестве государственного стандарта шифрования США DES не изменились: это быстродействие (в том числе в режиме частой смены ключа), стойкость к известным видам криптоанализа, экономичность программной и аппаратной реализации.

Традиционно используемым способом увеличения быстродействия блочных шифров и экономичности их программной и аппаратной реализации является применение так называемого простого расписания ключа (ПРК). При таком подходе раундовые подключи получаются из секретного ключа с помощью некоторой выборки. Использование ПРК дает возможность избежать траты времени и ресурсов на предварительные преобразования ключа. Однако при этом весьма вероятно наличие так называемых «слабых» и «полуслабых» ключей. Под слабым ключом понимается такой ключ, при использовании которого шифр реализует инволюцию. Под полуслабыми ключами понимается такая пара ключей, что зашифрование некоторого текста сначала по одному из ключей, а затем по второму, даст в результате исходный текст. Кроме того, в последние годы были разработаны специализированные атаки на итеративные шифры с простым расписанием ключа, так называемые «слайд-атаки». Они основаны на периодичности повторов использования раундовых ключей, ведущей к повторению одних и тех же раундовых преобразований (однородность преобразований). Особенно такие атаки опасны для шифров с небольшим размером секретного ключа.

Все эти потенциальные уязвимости привели к тому, что в настоящее время в качестве универсального противодействия вместо ПРК используется так называемая стойкая процедура генерации расширенного ключа (СПГРК). Суть ее заключается в выполнении над секретным ключом некоторых сложных предварительных преобразований для получения раундовых подключей. Полученные таким образом раундовые подключи можно рассматривать как независимые равновероятно распределенные случайные величины.

В то же время, существенным плюсом ПРК по сравнению с СПГРК, является скорость формирования раундовых подключей, что особенно важно в условиях частой смены секретного ключа. Также ПРК намного экономичнее в плане аппаратной реализации по сравнению с СПГРК. Кроме того, известны метод противодействия слабым и полуслабым ключам и метод противодействия слайд-атакам. В первом случае для зашифрования и расшифрования используются различные алгоритмы, а во втором - избегают однородности раундовых преобразований. Все это дает возможность говорить о необходимости создания нового подхода, который позволил бы избавиться от указанных слабостей шифра с ПРК некоторым алгоритмическим способом, не ведущем к значительному удорожанию реализации криптоалгоритма и снижению его быстродействия.

Для решения проблем, связанных с синтезом блочных шифров с ПРК, в данной работе разрабатывается и исследуется новый криптографический примитив – переключаемые управляемые операции, зависящие от преобразуемых данных.

Целью настоящей работы является обеспечение стойкости блочных шифров с ПРК к слайд-атакам и устранение слабых и полуслабых ключей на основе разработки способа построения блочных шифров с ПРК.

Объектом диссертационного исследования являются системы защиты информации в компьютерных и телекоммуникационных системах от несанкционированного доступа на основе блочных алгоритмов преобразования данных.

Предметом исследования являются способы предотвращения появления слабых и полуслабых ключей, а также методы повышения стойкости к слайд-атакам блочных шифров с простым расписанием ключа.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Разработать способ построения нового криптографического примитива, обеспечивающего устранение слабых и полуслабых ключей.
2. Разработать способ построения нового криптографического примитива, обеспечивающего стойкость к слайд-атакам.
3. На основе разработанных криптографических примитивов синтезировать блочный шифр, свободный от таких уязвимостей шифров с простым расписанием ключа как слабые и полуслабые ключи и возможность проведения слайд-атак.
4. Разработать подход к автоматизированному исследованию блочных шифров, обеспечивающий проведение статистического тестирования синтезируемых блочных шифров на основе новых примитивов.

Используемые методы. В диссертационной работе используются методы дискретной математики, математической статистики, теории вероятностей, линейной алгебры, криптологии.

Достоверность полученных результатов опирается на статистические эксперименты, практические разработки, сопоставление с известными результатами по анализу управляемых операций и шифров с их использованием, а также на широкое обсуждение в открытой печати и на всероссийских конференциях.

Научная новизна

1. Предложен новый тип криптографических примитивов, обеспечивающий устранение слабых и полуслабых ключей при применении простого расписания ключа в блочных шифрах. Данный примитив, получивший название «переключаемые управляемые операции», реализует взаимно обратные преобразования в зависимости от дополнительного (переключающего) бита. В качестве модификации данного примитива разработаны расширенные переключаемые управляемые операции.
2. Предложены способы повышения стойкости блочного шифра с простым расписанием ключа к слайд-атакам за счет использования в одном раунде различных переключаемых управляемых операций или расширенных переключаемых управляемых операций.
3. На основе переключаемых управляемых операций разработаны новые блочные шифры с простым расписанием ключа, являющиеся стойкими к слайд-атакам и свободными от слабых и полуслабых ключей.
4. Разработан подход к автоматизации работ по синтезу и статистическому тестированию блочных шифров.

Практическая ценность полученных результатов состоит в разработке способа синтеза блочных шифров с ПРК, обладающих стойкостью к слайд-атакам и возникновению слабых и полуслабых ключей, и создании автоматизированной системы проектирования и исследования блочных шифров. Данная система позволяет вводить криптоалгоритм в виде графических схем и выполнять над ним различные тесты с целью получения статистических характеристик созданного блочного шифра. Тесты, реализованные в системе, соответствуют рекомендациям NESSIE по оцениванию статистических характеристик блочных шифров. Все статистические характеристики, приводимые в тексте диссертации, получены с помощью данной автоматизированной системы.

Помимо своего прямого назначения, данная система проектирования и исследования блочных шифров может быть использована в учебном процессе для лабораторного практикума по дисциплинам «Информационная безопасность и защита информации» и «Криптографические методы защиты информации».

Реализация результатов. Автоматизированная система оценки блочных шифров внедрена в НФ ФГУП НИИ «Вектор» – Специализированном центре программных систем «Спектр», где используется для разработки блочных шифров и новых примитивов, и в Санкт-Петербургском государственном университете водных коммуникаций (СПГУВК), где используется для организации учебного процесса.

Апробация работы. Научные положения обсуждались на следующих конференциях: VIII Санкт-Петербургская Международная Конференция «Региональная информатика – 2002», (Санкт-Петербург, 26-28 ноября 2002г), Всеармейская научно-практическая конференция «Инновационная деятельность в Вооруженных силах Российской Федерации» (Санкт-Петербург, 28-29 ноября 2002 г и 25-26 декабря 2003 г), V Международная научно-практическая конференция «Информационная безопасность» (Таганрог, 3-7 июня 2003 г) и были опубликованы в ряде статей в журналах «Вопросы защиты информации» и «Известия ВУЗов. Приборостроение»

Научные положения, выносимые на защиту:

1. Использование переключаемых управляемых операций позволяет предотвратить слабые ключи в блочных шифрах с простым расписанием ключа
2. Использование в одном раунде различных переключаемых управляемых операций или расширенных переключаемых управляемых операций повышает стойкость блочных шифров с простым расписанием ключа к слайд-атакам на основе выбранного ключа
3. Предложенный подход к проведению автоматизированных испытаний позволяет выполнять исследования блочного шифра непосредственно разработчику криптоалгоритма.

Публикации. Основной материал опубликован в 11 печатных работах, среди которых 4 статьи.

Структура работы. Диссертация состоит из введения, 4 глав с выводами по каждой из них, заключения, списка литературы и приложения. Она изложена на 127 страницах и включает 36 рисунков, 14 таблиц и список литературы из 87 наименований, 3 страницы приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении показана актуальность темы диссертации, определены цели и задачи проведенных исследований, отражена научная новизна и практическая значимость полученных результатов.

В первой главе рассматривается роль криптографии в области защиты информации и основные задачи, решаемые современной криптографией.

Также в первой главе рассматриваются некоторые существующие на сегодняшний день криптографические примитивы. Например, таким примитивом является так называемый «элементарный переключатель», обозначаемый как $\mathbf{P}_{2/1}$. Этот элемент выполняет управляемую перестановку двух входных битов x_1 и x_2 в зависимости от значения управляющего бита v. Выходными битами будут $y_1 = x_2$ и $y_2 = x_1$ при $v = 1$ или $y_1 = x_1$ и $y_2 = x_2$ при $v = 0$. В виде булевых функций это может быть записано так:

$$y_1=f_1(x_1,x_2,v)=x_1v\oplus x_2v\oplus x_1;\quad y_2=f_2(x_1,x_2,v)=x_1v\oplus x_2v\oplus x_2.$$

На основе элементарных переключателей можно создавать блоки управляемых перестановок (БУП) $\mathbf{P}_{n/m}$. Такие блоки используются при синтезе блочных аппаратно-ориентированных шифров с ПРК, как, например, Spectr-H64 и его модификации. Показана структура симметричных БУП, в которых для получения обратного преобразования достаточно подать управляющий вектор в обратном порядке.

Кроме того, в первой главе рассматриваются достоинства и недостатки ПРК и СПГРК, а также проводится анализ существующих способов избавления от слабых и полуслабых ключей при использовании ПРК, среди которых можно выделить следующие:

1. Увеличение размерности раундового ключа, причем желательно, чтобы в каждом раундовом ключе использовались все биты секретного ключа. Недостатком данного подхода является сложность разработки расписания ключей, учитывающего возможные уязвимости.
2. Использование вместо ПРК СПГРК. Недостатком данного подхода является уменьшение скорости шифрования и увеличение стоимости аппаратной реализации.
3. Использование псевдослучайных констант для изменения раундовых ключей. Недостатком данного подхода является необходимость наличия генератора псевдослучайных последовательностей.
4. Использование различных алгоритмов зашифрования и расшифрования. Недостатком данного подхода этого способа является увеличение стоимости аппаратной реализации криптоалгоритма.

Также рассматривается уязвимость итеративных шифров с ПРК к разработанным в 2000 году слайд-атакам (Slide attacks), основанным на периодичности повторов использования раундовых ключей, что ведет к повторению одних и тех же раундовых преобразований. Наиболее известными способами противостояния слайд-атакам, основанным на слабостях ключевой системы, являются:

1. Неоднородность раундовых преобразований. Недостатком данного подхода является увеличение стоимости аппаратной реализации.
2. Использование СПГРК вместо ПРК (для некоторых разновидностей слайд-атак).

Делается вывод о том, что, учитывая экономические и скоростные преимущества ПРК над СПГРК, необходимо разработать способы преодоления указанных уязвимостей без существенного ухудшения данных характеристик.

Во второй главе описываются различные топологии разработанного нового примитива - переключаемых управляемых операций. Переключаемой управляемой операцией (ПУО) будем называть операцию $F^{(V,e)}(X) = F^{(e)}(X,V) = F(X,V,e)$, удовлетворяющую условию: при $e = 0$ $F^{(V,e)}(X) = F^{(V)}(X)$ и при $e = 1$ $F^{(V,e)}(X) = (F^{(V)}(X))^{-1}$, где $e \in \{0,1\}$. Таким образом, переключаемая управляемая операция состоит из двух взаимно обратных управляемых операций, причем выбор между этими операциями производится в зависимости от значения некоторого дополнительного (переключающего) бита.

Переключаемые управляемые операции могут строиться как на основе уже известных топологий, так и на основе новых разработок. Так, на основе БУП с симметричной топологией были построены переключаемые управляемые операционные блоки (УОБ), один из которых показан на рис.1. В этом случае УОБ $\mathbf{F}_{32/96}$ является блоком с симметричной топологией, т.е. для получения обратного блока $\mathbf{F}^{-1}_{32/96}$ достаточно подать на вход $\mathbf{F}_{32/96}$ управляющий вектор в обратном порядке. Показанный на рис. 1 БУП $\mathbf{P}_{96/1}$ выполняет зависимую от бита переключения e перестановку управляющих векторов, и при e=0 результирующий управляющий вектор будет V=(V_1,V_2,V_3,V_4,V_5,V_6), а при e=1 V=(V_6,V_5,V_4,V_3,V_2,V_1), что создает переключение между прямым и обратным блоком $\mathbf{F}_{32/96}$.

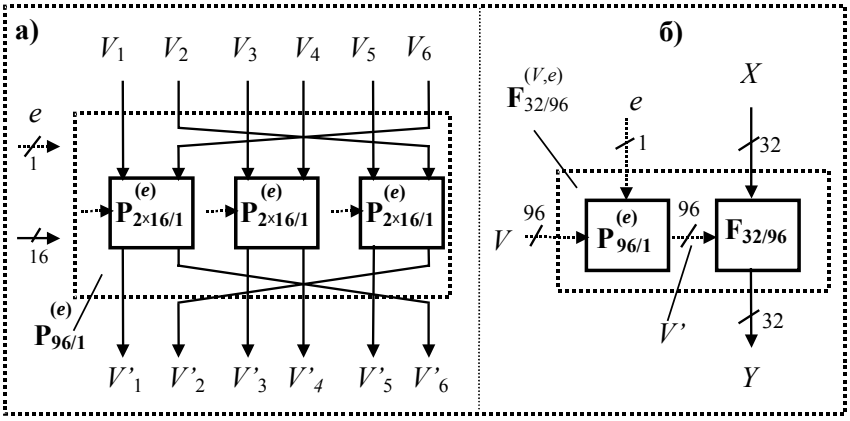

Рис. 1 Структура переключаемого УОБ $\mathbf{F}^{(V,e)}_{32/96}$ (б) и БУП $\mathbf{P}_{96/1}$ (а)

Однако в общем случае УОБ не является блоком с симметричной топологией. Для этого случая была разработана показанная на рис. 2 схема построения переключаемых УОБ.

Данная схема включает в себя некоторые обратимые управляемые блоки $\mathbf{F}_1$ и $\mathbf{F}_2$. Управляющие вектора блоков $\mathbf{F}_1$ и $\mathbf{F}_2$ и обратных им блоков $\mathbf{F}^{-1}_1$ и $\mathbf{F}^{-1}_2$ формируются с помощью блоков управляемых перестановок в зависимости от значений переключающих битов e_1 и e_2.

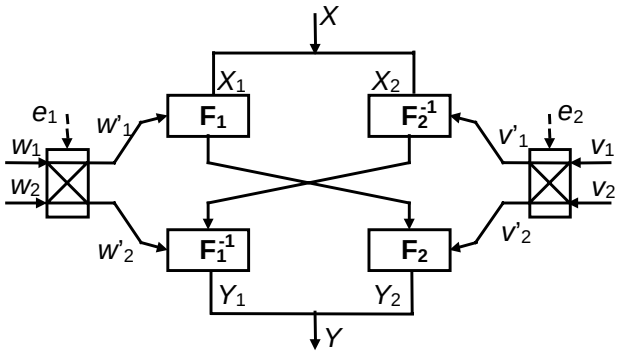

Рис. 2 Схема построения произвольного переключаемого УОБ

В качестве доказательства правильной работы разработанной схемы в режиме зашифрования и в режиме расшифрования можно привести следующие рассуждения: при зашифровании результат преобразований Y можно представить как

$$Y=(Y_1,Y_2)=((X_2)\mathbf{F}_2{}^{-1}{}_{v'_1}\bullet\mathbf{F}_1{}^{-1}{}_{w'_2},\ (X_1)\mathbf{F}_{1\,w'_1}\bullet\mathbf{F}_{2\,v'_2}),$$

где X_1, X_2 – это левая и правая части входного вектора X, Y_1,Y_2 – левая и правая части выходного вектора Y, v'_1, v'_2, w'_1, w'_2 – управляющие вектора соответствующих УОБ, получившиеся из исходных управляющих векторов v_1, v_2, w_1, w_2 путем применения к ним блоков управляемых перестановок с управляющими битами e_1 и e_2. Обозначим теперь за Y', результат расшифрования данной схемой полученного зашифрованного вектора Y, и посмотрим, получится ли при подаче в качестве входного вектора шифртекста Y исходный текст X.

Тогда при расшифровании имеем:

$$Y' = (Y'_1,\ Y'_2)=((Y_2)\ \mathbf{F}_2{}^{-1}{}_{v'_1}\bullet\mathbf{F}_1{}^{-1}{}_{w'_2},\ (Y_1)\mathbf{F}_{1\,w'_1}\bullet\mathbf{F}_{2\,v'_2}) =$$

$$= ((X_1)\mathbf{F}_{1\,w'_1}\bullet\mathbf{F}_{2\,v'_2}\bullet\mathbf{F}_2{}^{-1}{}_{v'_1}\bullet\mathbf{F}_1{}^{-1}{}_{w'_2},\ (X_2)\mathbf{F}_2{}^{-1}{}_{v'_1}\bullet\mathbf{F}_1{}^{-1}{}_{w'_2}\bullet\mathbf{F}_{1\,w'_1}\bullet\mathbf{F}_{2\,v'_2}) =$$

$$=((X_1)\mathbf{F}_{1\,w'_1}\bullet\mathbf{F}_1{}^{-1}{}_{w'_2},\ (X_2)\mathbf{F}_2{}^{-1}{}_{v'_1}\bullet\mathbf{F}_{2\,v'_2}) =$$

$$= (X_1,\ X_2)= X$$

Также предлагается способ построения произвольной переключаемой фиксированной операцию $\boldsymbol{\pi}^{(e)}$. Данный способ показан на рис. 3, где $\boldsymbol{\pi}$ и $\boldsymbol{\pi}^{-1}$ – соответственно, прямая и обратная фиксированные операции с n-битовым входным вектором. В качестве фиксированной операции может выступать, например, фиксированная перестановка. Возможность изменить прямую фиксированную операцию на обратную обеспечена использованием однослойного БУП $\mathbf{P}^{(e)}{}_{2n/1}$. Правый (левый) входной n-битовый вектор блока $\mathbf{P}^{(e)}{}_{2n/1}$ соединяется с выходным вектором прямой (обратной) фиксированной операции $\boldsymbol{\pi}$ ($\boldsymbol{\pi}^{-1}$). Левый выходной вектор блока $\mathbf{P}^{(e)}{}_{2n/1}$ является выходом фиксированной операции $\boldsymbol{\pi}^{(e)}$. Таким образом, получаем $\boldsymbol{\pi}^{(0)} = \boldsymbol{\pi}$ и $\boldsymbol{\pi}^{(1)} = \boldsymbol{\pi}^{-1}$.

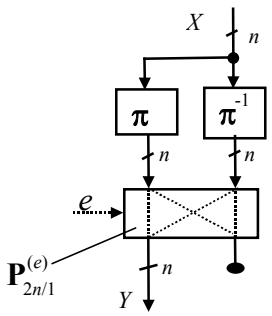

Рис. 3 Переключаемое фиксированное преобразование

Для решения задачи создания криптографического примитива, обеспечивающего стойкость блочного шифра с ПРК к слайд-атакам, была разработана модификация переключаемых управляемых операций, содержащая в себе несколько взаимно обратных управляемых операций различного типа, получившая название расширенной переключаемой управляемой операции. Расширенными переключаемыми управляемыми операциями называются некоторые зависимые от параметра E операции $\mathbf{F}^{(V,E)}$, где E – k-битовый вектор ($k \geq 2$), зависящий от e (бита переключения) и от номера раунда шифрования, причем для всех V модификации $\mathbf{F}^{(V,E)}$ и $\mathbf{F}^{(V,E')}$ являются взаимно обратными при $E \oplus E' = \{1\}^k$. Таким образом, $\mathbf{F}^{(V,E)}$ содержит 2^{k-1} пар взаимно обратных модификаций управляемой операции $\mathbf{F}^{(V)}$, что позволяет легко построить 2^k уникальных раундовых преобразований для каждого раундового ключа.

Расширенные переключаемые управляемые операции можно сконструировать путем некоторой доработки схемы построения показанных выше переключаемых управляемых операций. Пример построения расширенной переключаемой управляемой операции для случая, когда $k = 4$, показан на рис. 4, где **I** – инволюция.

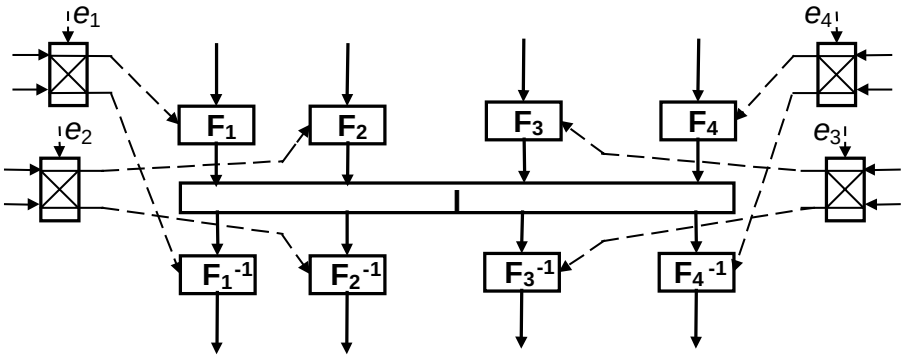

Рис. 4 Расширенная переключаемая операция $\mathrm{F}^{(V,E)}$, где E=(e_1, e_2, e_3, e_4)

В данном случае каждый блок управляемых операций $\mathbf{F}_i$ и соответствующий ему обратный блок $\mathbf{F}_i^{-1}$ (i = 1,..,4) в качестве управляющих векторов имеют векторы, полученные с помощью одного из четырех БУП, в зависимости от значения соответствующего переключающего бита e_i. В общем случае все $\mathbf{F}_i$ могут быть различны. При $k = 4$ можно построить $2^4 = 16$ раундовых преобразований для каждого раундового ключа.

Делается вывод о том, что использование разработанных переключаемых управляемых операций обеспечивает существенное различие алгоритмов зашифрования и расшифрования, что устраняет слабые и полуслабые ключи при использовании ПРК. При применении нескольких различных переключаемых управляемых операций в одном раунде или использовании расширенных переключаемых управляемых операций устраняется однородность раундовых преобразований, что обеспечивает стойкость итеративных блочных шифров с ПРК к слайд-атакам. Преимущество применения расширенных переключаемых управляемых операций заключается том, что они позволяют решить проблему стойкости к слайд-атакам с минимальными дополнительными затратами схемотехнических ресурсов.

Кроме того, во второй главе предлагается использовать в переключаемых УОБ элементарные блоки так называемого **S**-типа, выделенные в ходе проведения классификации элементарных управляемых блоков с двухбитовыми входом и выходом и с однобитовым управляющим входом. Проведенные исследования показали, что управляемые элементы (УЭ) **S**-типа являются более предпочтительными по сравнению с УЭ $\mathbf{P}_{2/1}$, как по дифференциальным характеристикам, так и по свойствам нелинейности. Все полученные в диссертации результаты, касающиеся переключаемых управляемых блоков и разработанных на их основе шифров, получены в результате исследования переключаемых управляемых блоков, построенных на УЭ **S**-типа. Пример общего вида и возможной реализации при $v = 0$ и $v = 1$ УЭ **S**-типа показан на рис. 5.

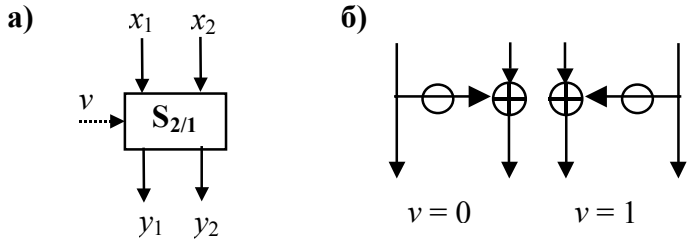

Рис. 5 Общий вид (а) и конкретная реализация (б) УЭ **S**-типа

В **третьей главе** в качестве иллюстрации эффективности применения переключаемых управляемых операций описываются разработанные шифры, построенные на следующих принципах:

1. Криптосистема должна быть итеративным 64-битовым шифром с 128-битовым секретным ключом.
2. Процедуры зашифрования и расшифрования должны выполняться с помощью одного и того же алгоритма путем смены расписания ключей.
3. Шифр должен обеспечивать высокую производительность в случае частой смены ключей, поэтому предварительное преобразование ключа не должно производиться.

4. Шифр должен использовать переключаемые управляемые операции в качестве основного криптографического примитива.

Было разработано два шифра, удовлетворяющих этим требованиям, которые получили названия PUO-1 и PUO-2 («переключаемые управляемые операции»). Кроме того, для подтверждения предположения о преимуществе переключаемых управляемых операций, построенных на основе УЭ **S**-типа, над переключаемыми управляемыми операциями, построенными на основе УЭ $\mathbf{P}_{2/1}$, был создан шифр под названием PVP-64, основанный на переключаемых управляемых перестановках. Проведенные исследования показали, что наилучшие статистические характеристики имеет шифр PUO-2, в котором в наибольшей степени используются переключаемые управляемые операционный блоки (УОБ) на основе УЭ **S**-типа.

На рис. 6 представлен общий вид схемы шифрования PUO-2 и схема процедуры Crypt(e), в которой используются преобразования, основанные на переключаемых управляемых операциях.

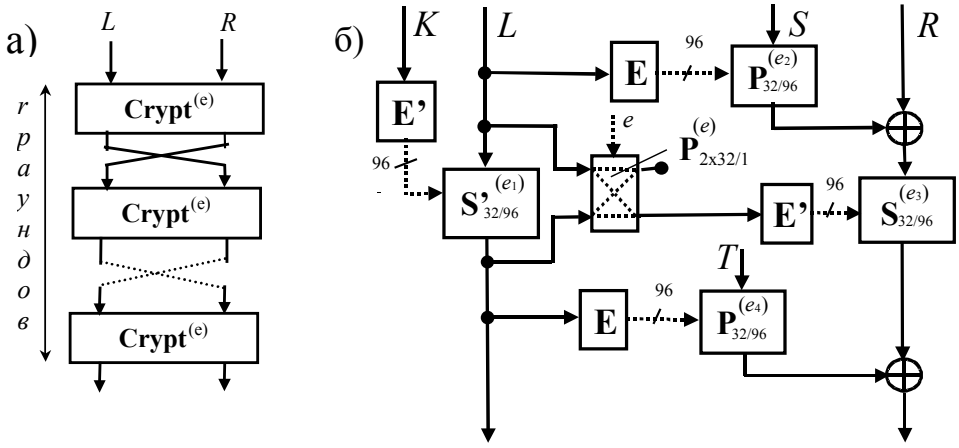

Рис. 6 Общая схема шифрования (а) и один раунд шифра PUO-2 (б)

Пунктирными стрелками обозначены управляющие данные. Значения переключающих бит e_1, e_2, e_3, e_4, служащие для модификации соответствующих переключаемых управляемых блоков $\mathbf{S}^{(e)}$ и $\mathbf{P}^{(e)}$, являются фиксированными для каждого раунда для режимов зашифрования и расшифрования, а смена этих режимов происходит с помощью переключающего бита e. Переключаемые БУП $\mathbf{P}_{32/96}{}^{(e_i)}$ ($i = 2, 4$) построены на основе УЭ $\mathbf{P}_{2/1}$, а переключаемые УОБ $\mathbf{S}_{32/96}{}^{(e_i)}$ ($i = 1, 3$) – на основе УЭ **S**-типа. **E** и **E**’ – процедуры расширения управляющего вектора.

Подобный способ построения шифра с ПРК устраняет возможность возникновения слабых и полуслабых ключей, т.к. использование переключаемых управляемых операций делает алгоритмы зашифрования и расшифрования различными. Стойкость к слайд-атаке

обеспечивается с помощью неоднородности раундовых преобразований, получающейся за счет использования различных переключаемых управляемых операций в одном раунде.

Для проведения исследований построенных криптоалгоритмов была разработана автоматизированная система проектирования и исследования блочных шифров, позволяющая вводить криптоалгоритмы в виде графических схем и выполнять над ними различные статистические тесты. Данная система описывается в четвертой главе.

Полученные с помощью этой системы результаты статистических испытаний шифра PUO-2 показаны в табл. 1 (исследовались среднее количество выходных бит, изменяющихся при изменении одного входного бита d_1, степень полноты преобразования d_c, степень лавинного эффекта d_a, степень соответствия строгому лавинному эффекту d_{sa}), и эти результаты свидетельствуют, что построенный шифр не уступает финалистам AES по статистическим характеристикам и приобретает хорошие рассеивающие свойства уже после четырех раундов.

Таблица 1

Результаты статистического тестирования шифра PUO-2

Кол-во раундов	d_1	d_c	d_a	d_{sa}	Кол-во исп.
1	11,1287703	0,3984375	0,3477741	0,2827340	10000
2	26,3817437	0,8674316	0,8243386	0,8172683	10000
3	31,8613859	1	0,9952156	0,9886782	10000
4	32,002225	1	0,9990066	0,9922031	10000
5	32,003209	1	0.9989076	0,9920704	10000
6	31,998534	1	0,9989453	0,9923051	10000
7	31,995075	1	0,9988811	0,9918571	10000
8	32,007470	1	0,9989309	0,9919306	10000

Для анализа стойкости шифра PUO-2 к дифференциальному криптоанализу рассматривается формирование двухраундовой дифференциальной характеристики (Δ^L_0, Δ^R_1, $p(2)$), показанное на рис. 7. Здесь Δ^L_0 – результат сложения по модулю 2 (разность) двух входных левых подблоков данных, с весом Хэмминга равным 0, Δ^R_1 – разность двух входных правых подблоков данных с весом Хэмминга равным 1, $p(2)$ – вероятность двухраундовой характеристики.

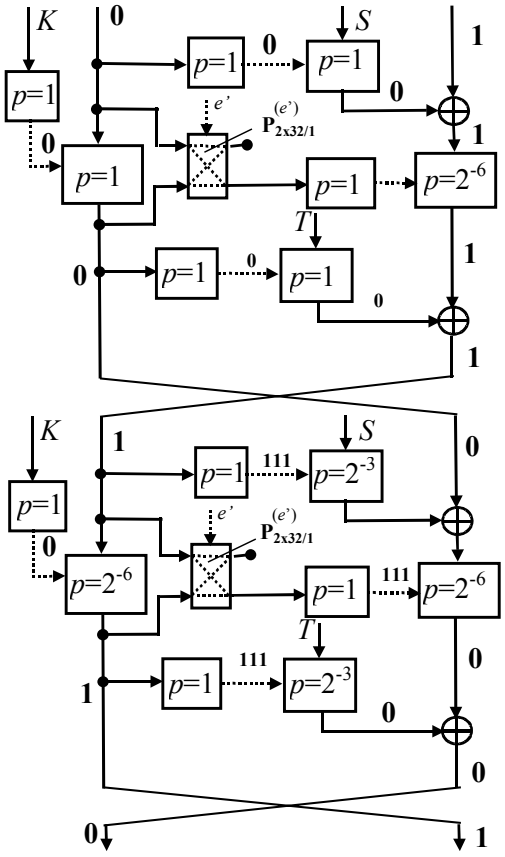

Рис. 7 Формирование двухраундовой характеристики (Δ^L_0, Δ^R_1, $p(2)$) в PUO-2

В данной криптосхеме формирование дифференциальной характеристики включает следующие события. В первом раунде активный бит правого подблока данных проходит операцию $\mathbf{S}^{(e)}_{32/96}$ с вероятностью 2^{-6}. После перестановки подблоков данных активный бит попадает в левую ветвь, которую он проходит без порождения новых активных битов с вероятностью 2^{-6}. При этом он дважды воздействует через управляющий вход на операции $\mathbf{P}^{(e)}_{32/96}$. Вероятность того, что каждая из этих операций не порождает активных битов, равна 2^{-3}. Тогда вероятность двухраундовой характеристики равна

$$p(2) \approx 2^{-6}\cdot 2^{-6}\cdot 2^{-6}\cdot 2^{-3}\cdot 2^{-3} = 2^{-24}.$$

Двухраундовая характеристка вносит основной вклад в вероятность прохождения однобитовой разности через полное число раундов шифра PUO-2. Используя значение $p(2)$, можно вычислить дифференциальную характеристику для восьми раундов:

$$p(8) \approx (2^{-24})^4 = 2^{-96}.$$

Сравнение вероятности $p(8)$ с вероятностью рассматриваемой характеристики для случайного преобразования показывает, что шифр PUO-2 неотличим от случайного преобразования с помощью дифференциального анализа, т.е. является стойким к данной атаке.

Сравнительно малое число раундов в PUO-2 обеспечивается тем, что, как отмечено на рис. 7, переключаемые управляемые блоки $\mathbf{S}^{(e)}_{32/96}$, построенные на основе управляемых эле-

ментов **S**-типа, обладают лучшими дифференциальными характеристиками по сравнению с переключаемыми управляемыми блоками $\mathbf{P}^{(e)}_{32/96}$, построенными на основе элементарного переключателя $\mathbf{P}_{2/1}$.

В таблице 2 показаны оценки схемотехнической реализации для PUO-2 в сравнении с финалистами AES и 3DES.

Таблица 2

Оценка схемотехнической реализации шифра PUO-2

Шифр	Кол-во вентилей		Критический путь, τ	
	расп.ключа	зашифр.	предвыч.	зашифр.
PUO-2	500	22 300	-	112
3DES	23 000	120 000	-	220
Rijndael	94 000	520 000	83	95
RC6	900 000	740 000	3 000	880
Twofish	230 000	200 000	23	470

Очевидно, что наиболее экономичным в плане аппаратной реализации является PUO-2 (требует всего 22300+500 вентилей), и, хотя самая быстрая реализация соответствует 128-битовому шифру Rijndael (производительность $z \approx 1.35$ бит/τ), PUO-2 ($z \approx 0.57$ бит/τ) быстрее, чем RC6 ($z \approx 0.15$ бит/τ), Triple-DES ($z \approx 0.29$ бит/τ) и Twofish ($z \approx 0.27$ бит/τ).

Таким образом, можно сделать вывод о многообразии вариантов криптосхем, применяемых при разработке новых итеративных блочных шифров с использованием переключаемых управляемых операций в качестве основного криптографического примитива.

В **четвертой главе** описывается созданная для проверки статистических характеристик разработанных примитивов и шифров автоматизированная система проектирования и исследования блочных шифров. Данная система ориентирована на пользователя, хорошо знакомого с криптографией, но не имеющего опыта в программировании, и позволяет таким пользователям проводить эксперименты с криптоалгоритмами, представленными в графическом виде. Цель разработки данной системы - предоставить возможность специалистам в области разработки криптоалгоритмов самостоятельного (без посредников) проведения экспериментов по исследованию разрабатываемых ими криптоалгоритмов от момента создания схемы криптоалгоритма до момента получения ее характеристик. Таким образом, представляемая система решает следующие задачи:

1. Поддержка построения схемы криптоалгоритма (т.е. ввод криптоалгоритма в графическом редакторе в виде блок-схемы)

2. Проведение испытаний над построенной схемой криптоалгоритма (можно проводить как числовые вычисления, так и статистические эксперименты, соответствующие рекомендациям NESSIE по исследованию статистических свойств криптоалгоритмов).

В соответствии со стоящими перед системой задачами, в ее составе находятся графический редактор, подсистема синтаксического контроля, подсистема вычислений и подсистема обработки результатов. Графический редактор позволяет вводить криптоалгоритмы в виде графических схем. Подсистема синтаксического контроля анализирует правильность построений в графическом редакторе, причем осуществляется контроль трех типов:

1. Синтаксические проверки допустимости графических построений в рамках используемого графического языка.
2. Синтаксические проверки правильности настроек компонентов создаваемой схемы криптоалгоритма.
3. Синтаксические проверки правильности алгоритмических построений.

Проводя такие проверки, подсистема синтаксического контроля тем самым обеспечивает однозначность перевода графического представления в аналитическое. Если подсистема синтаксического контроля не выявила ошибок, то пользователь может приступать к тестированию созданного криптоалгоритма.

Таким образом, использование данной системы подразумевает выполнение разработчиком следующих этапов:

1. Создание криптоалгоритма на бумаге, желательно в виде блок-схемы, чтобы правильно оценить ее размеры при последующем вводе.
2. Перенос созданной криптосхемы с помощью средств, предоставляемых графическим редактором системы, в компьютер.
3. Задание параметров испытаний. При этом осуществляется настройка двух видов:

   а) Настройка параметров шифра. При этом указывается, какие данные являются ключами, какие данные необходимо задать вручную, какие нужно фиксировать на все время вычислений, откуда брать значения входных данных (они могут задаваться вручную, с помощью генератора случайных чисел или браться из готового файла).

   б) Настройка параметров вычислений. В системе имеется реализованный набор статистических тестов для блочных шифров, соответствующий рекомендациям NESSIE, несколько тестов, использовавшихся на конкурсе AES, а также возможность проводить численные вычисления. Для некоторых тестов указывается необходимое количество испытаний.
4. Анализ результатов. Система записывает результаты с пояснениями в текстовый файл, который можно посмотреть в любом текстовом редакторе.

5. В случае неудовлетворенности пользователя полученными результатами, он легко может внести изменения в свой криптоалгоритм и провести повторные исследования.

Таким образом, данная система позволяет автоматизировать большинство технических этапов разработки и тестирования криптоалгоритмов, причем в связи с использованием графического языка и простотой настроек все эти этапы могут быть выполнены непосредственно разработчиком криптоалгоритма.

В четвертой главе также приводится пример работы системы при построении и исследовании шифра PUO-2.

ЗАКЛЮЧЕНИЕ

В ходе диссертационных исследований были получены следующие **результаты**:

1. Предложен новый криптографический примитив, получивший название «переключаемые управляемые операции», использование которого в блочных шифрах с простым расписанием ключа позволяет избежать появления слабых и полуслабых ключей, и разработаны различные способы его построения.
2. Разработан способ построения модификации переключаемых управляемых операций, получивший название «расширенных переключаемых управляемых операций».
3. Предложены способы устранения однородности раундовых преобразований, заключающиеся в использовании в одном раунде различных переключаемых управляемых операций или в использовании расширенных переключаемых управляемых операций, что обеспечивает стойкость к слайд-атакам итеративных блочных шифры с простым расписанием ключа.
4. На основе разработанных переключаемых управляемых операций синтезированы блочные алгоритмы с простым расписанием ключа, стойкие к слайд-атаке, свободные от слабых и полуслабых ключей и соответствующие современным требованиям статистического тестирования.
5. Создана автоматизированная система проектирования и исследования блочных шифров.

Публикации по теме диссертации

1. Морозова Е.В. Использование системы визуального моделирования криптоалгоритмов в учебных целях // Труды всеармейской научно-практической конференции «Инновационная деятельность в Вооруженных силах Российской Федерации». 25-26 декабря 2003 года, Санкт-Петербург. - СПб.: ВУС, 2003. - С.115-117.
2. Морозова Е.В. Варианты построения переключаемых управляемых операций // Труды всеармейской научно-практической конференции «Инновационная деятельность в Воо-

руженных силах Российской Федерации». 28-29 ноября 2002 года, Санкт-Петербург. - СПб.: ВУС, 2002. - С.110-113.

3. Морозова Е.В. Управляемые операции в шифрах с простым расписанием использования ключа // Материалы VIII Санкт-Петербургской Международной Конференции «Региональная информатика – 2002» («РИ – 2002»), Санкт-Петербург, 26-28 ноября 2002г. Ч.1. – СПб, 2002. - С.123-124.
4. Молдовян А.А., Еремеев М.А., Молдовян Н.А., Морозова Е.В. Полная классификация и свойства нелинейных управляемых элементов минимального размера и синтез криптографических примитивов // Вопросы защиты информации. – 2003. - №3. - С.15-27.
5. Гуц Н.Д., Молдовян А.А., Морозова Е.В. Шифраторы на основе переключаемых операций // Известия вузов. Приборостроение. - 2003. - Т.46, № 7. - С.79-82.
6. Молдовян Н.А., Молдовян А.А., Морозова Е.В. Скоростные шифры с простым расписанием использования ключа // Вопросы защиты информации. - 2003. - №1. - С.12-22.
7. Молдовян Н.А., Морозова Е.В. Шифр с переменными перестановками в роли основного криптографического примитива // Вопросы защиты информации. - 2002. - №4. - С.8-18.
8. Бодров А.В., Гуц Н.Д., Молдовян А.А., Морозова Е.В. Графический редактор системы визуального моделирования криптоалгоритмов // Известия ТРТУ. Тематический выпуск. Материалы V Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2003. - №4. - С.255-259.
9. Бодров А.В., Гуц Н.Д., Морозова Е.В. Подсистема символьной математики в системе визуального моделирования криптоалгоритмов // Известия ТРТУ. Тематический выпуск. Материалы V Международной научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2003. - №4. - С.268-271.
10. Молдовян У.А., Морозова Е.В. Способ криптографического преобразования данных // Труды всеармейской научно-практической конференции «Инновационная деятельность в Вооруженных силах Российской Федерации». 28-29 ноября 2002 года, Санкт-Петербург. - СПб.: ВУС, 2002. - С.91-95.
11. Бодров А.В., Гуц Н.Д., Морозова Е.В. Система визуального моделирования блочных шифров // Сборник трудов научно-практической конференции «Информационная безопасность». - Таганрог: Изд-во ТРТУ, 2002. - С.43-45.