Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 681.3.06.004

ВИЛАНСКИЙ
Юрий Викторович

СИНТЕЗ И АНАЛИЗ ДВУХКАНАЛЬНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАТЕЛЯ

Автореферат диссертации на соискание ученой степени
кандидата технических наук
по специальности 05.13.17 – Теоретические основы информатики

МИНСК – 2007

Работа выполнена в частном учреждении образования Институте современных знаний имени А.М. Широкова

Научный руководитель: **Мищенко Валентин Александрович**, доктор технических наук, профессор, ЧУО «Институт современных знаний имени А.М. Широкова», проректор по научной работе.

Официальные оппоненты: **Курбацкий Александр Николаевич**, доктор технических наук, профессор, Белорусский государственный университет, заведующий кафедрой технологий программирования.
Бенедиктович Владимир Иванович, кандидат физико-математических наук, ГНУ «Институт математики Национальной академии наук Беларуси», старший научный сотрудник.

Оппонирующая организация: НИУ «Научно-исследовательский институт прикладных физических проблем им. А.Н. Севченко» Белгосуниверситета.

Защита состоится 28 февраля 2008 года в 14 часов на заседании совета по защите диссертаций Д 02.15.04 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013 г. Минск, ул. П. Бровки, 6, ауд. 232-1, email: dissovet@bsuir.by, тел. 2938989.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан 25 января 2008 г.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Компьютерные системы неумолимо преобразовывают традиционные технологии в медицине, торговле, государственном правовом регулировании, мультимедиа, транспорте и т.д., затрагивая огромные массы людей, иногда все населения страны. Информационные технологии становятся массовыми. При их использовании приходится решать множество проблем, среди которых проблемы целостности данных, аутентификации, защиты авторских прав, конфиденциальности и т.д. Возникает потребность в специальных защитных механизмах. При этом классические приемы защиты, такие как шифрование, контрольные суммы, электронно-цифровая подпись и т.д., не всегда обеспечивают достаточно степеней свободы разработчикам приложений для массовых информационных технологий.

Одним из способов решения некоторых проблем массовых информационных технологий может быть специфическое представление информации в виде текста, состоящего из несколько взаимосвязанных частей. Эти части можно раздельно хранить, обрабатывать и передавать. Наличие даже двух частей позволяет различным образом манипулировать ими в конкретных приложениях для обеспечения конфиденциальности, целостности, скрытия, авторства и т.д., что расширяет возможности разработчиков приложений.

Диссертационная работа посвящена синтезу специального двухканального преобразователя с дополнительными параметрами управления, с помощью которого можно получать такое представление информации. На основе анализа современных подходов к построению симметричных систем и криптографических протоколов в работе конструируются и исследуются классы отображений с выходами переменной длины, пригодные для синтеза двухканального преобразователя. Синтезируются конкретные алгоритмы, реализующие такой преобразователь, и выполняется его анализ в различных режимах использования.

Связь работы с крупными научными программами, темами

Диссертационная работа продолжает начатую в 2001 г. в Институте современных знаний под руководством доктора технических наук, профессора Мищенко В.А. научно-исследовательскую работу: «Синтез и исследование мультиканального вероятностного алгоритма преобразования данных со слабыми статистическими связями каналов» (№ ГР 20013795). Она связана с разработкой телекоммуникационных технологий и методов, обеспечивающих безопасность хранения и передачи информации. В соответствии с указом Президента Республики Беларусь № 315 от 6 июля 2005 г., разработка телекоммуникационных технологий, технических и аппаратно-программных систем и средств защиты информации и контроля ее защищенности является одним из приоритетных направлений научно-технической деятельности.

Цель и задачи исследования

Целью настоящей работы является синтез и анализ двухканального преобразователя, который может использоваться для создания новых приложений, обеспечивающих защищенность хранения и/или передачи данных в различных информационных технологиях. Для достижения этой цели необходимо решить следующие задачи:

1. Выбрать подходящий класс отображений, обеспечивающий разделение данных для их представления в виде двух частей.

2. Исследовать возможные режимы использования двуканальных систем и предложить общую схему построения двухканальных преобразователей на базе выбранного класса отображений.

3. Синтезировать алгоритм, реализующий двухканальный преобразователь с параметрами управления, в том числе и длинами выходов. Такой преобразователь должен обеспечивать новое представление информации в виде двух частей для раздельного хранения и/или передачи данных.

4. Разработать методику тестирования таких алгоритмов на базе информационных критериев зависимости, учитывающую особенности отображений с выходом переменной длины.

5. Выполнить анализ алгоритма и результатов тестирования по предложенной методике для различных режимов использования двухканального преобразователя.

6. Предложить технологию создания разнесенных систем, которая использует свойства синтезированного двухканального преобразователя, ориентирована на современные возможности сетей передачи данных и позволяет автоматически обеспечить конфиденциальность и аутентичность сообщений, а также прикладную систему, реализующую данную технологию.

Объектом исследования данной работы являются отображения с переменной длиной выхода. Предметом исследования являются алгоритмы, использующие такие отображения для разделения информации и получения ее представления с требуемыми свойствами.

В работе используются методы теории информации, теории вероятностей и математической статистики, дискретной математики.

Основные положения диссертации, выносимые на защиту

1. Специальный класс отображений с выходом переменной длины, который обеспечивает разделение входной информации на две части, что позволяет создавать двухканальные системы.

2. Общая схема построения двухканальных систем – подобных подстановочно-перестановочной сети, где в качестве подстановочных преобразований

выступает специальный класс отображений с выходами переменной длины, – которая позволяет синтезировать конкретные алгоритмы.

3. Алгоритм, реализующий двухканальный преобразователь с параметрами управления, построенный по предложенной общей схеме, который обеспечивает разделение данных на две части и может использоваться в различных режимах, что позволяет создавать новые приложения, обеспечивающие безопасное хранение и/или передачу данных, а также значительно повысить надежность современных методов защиты информации.

4. Методика тестирования на соответствие информационным критериям зависимости, учитывающая особенности отображений с выходом переменной длины, позволяющая проверить качества нелинейности выходных последовательностей и оценить влияние различных компонентов алгоритма на них.

5. Анализ двухканального преобразователя и результатов тестирования по предложенной методике, позволяющий определить наиболее выгодные режимы использования данной системы.

6. Технология построения разнесенных систем, использующая свойства синтезированного преобразователя, позволяющая решать многие актуальные задачи по обеспечению конфиденциальности информации, а также аутентификации сообщений и отправителей. Указанная технология реализована в программном комплексе SolanioE-Mail.

Личный вклад соискателя

Все основные результаты диссертации получены лично автором и обсуждены с научным руководителем. Программы, реализующие двухканальный преобразователь и тесты на соответствии информационным критериям разработаны автором полностью, а прикладной системы SolanioE-Mail – на 60%. При ссылке на совместные публикации подразумеваются результаты, полученные лично автором.

Апробация результатов диссертации

Результаты исследований докладывались автором на I международной конференции «Информационные системы и технологии» в 2002 году в г. Минске, на научной сессии МИФИ 28 января 2004 года в г. Москве, на III общероссийской конференции «Математика и безопасность информационных технологий» (МаБИТ-04) 29 октября 2004 года в г. Москва.

Опубликованность результатов диссертации

По результатам исследований опубликовано 15 научных работ (более 719 с.), в том числе: 6 статей в научных журналах (общим объемом 1,65(3,1) авторских листа), 2 книги, 1 доклад в материалах международной конференции, 2

тезиса докладов в материалах международных конференций, 2 евразийских патента, 2 заявки РСТ на международные патенты.

Структура и объем диссертации

Диссертационная работа состоит из перечня условных обозначений, введения, общей характеристики работы, четырех глав, заключения, библиографического списка и приложений. **Во введении** обсуждается актуальность работы. **В первой главе** рассматривается модель массовой технологии. Отмечается, что одним из способов решения некоторых проблем массовых технологий может быть специфическое представление информации в виде текста, состоящего из несколько взаимосвязанных частей. Эти части можно раздельно хранить, обрабатывать и передавать. Для эффективного использования необходимо иметь возможность управлять длинами выходных частей. Для реализации такого представления можно использовать отображения, подобные тем, которые используют при сжатии данных, для удаления информационной избыточности, и некоторые из принципов создания криптографических систем. Приводятся современные подходы к проектированию криптографических систем, в частности, некоторые критерии и основные подходы к выбору подстановочных преобразований, а также современная методика тестирования. Глава завершается постановкой задачи. **Вторая глава** посвящена синтезу двухканального преобразователя MV2. В этой главе определяются двухканальные системы, приводятся режимы их использования. Для двухканальных систем выводятся общие информационные соотношения, и строится аналог шенноновской модели безопасности. Исследуются отображения с выходом переменной длины, и выбирается класс подстановочных преобразований для представления исходных данных в виде двух частей. Разрабатывается общая схема преобразования исходного текста, в результате которого, выходной текст состоит из двух частей. Выполняется ее предварительный анализ. Синтезируется конкретный алгоритм, реализующий общую схему. **В третьей главе** анализируется безопасность использования алгоритма в различных режимах, разрабатывается методика тестирования, приводятся результаты тестирования, и выполняется их анализ. **В четвертой главе** рассматривается технология, использующая синтезированный преобразователь и конкретная прикладная система, реализующая данную технологию. **В приложениях** приведены некоторые математические факты и доказательства тождеств и леммы, используемые в работе, а также акты внедрения.

Диссертация изложена на 130 страницах машинописного текста, содержит 31 иллюстрацию (15 с.), 6 таблиц (3 с.), 2 приложения (7 с.) и библиографический список из 128 наименований на 11 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационной работы, сформулированы цель и задачи исследования, приведена краткая характеристика работы.

В первой главе рассмотрена модель массовой технологии. Отмечается, что одним из способов решения некоторых проблем массовых технологий может быть специфическое представление информации в виде текста, состоящего из несколько взаимосвязанных частей. Эти части можно раздельно хранить, обрабатывать и передавать. Для эффективного использования необходимо иметь возможность управлять длинами выходных частей. Для реализации такого представления можно использовать отображения, подобные тем, которые используют при сжатии данных для удаления информационной избыточности, и некоторые из принципов создания криптографических систем.

В связи с этим, в главе рассмотрены основные криптографические модели и современные подходы к проектированию блочных симметричных шифров. Эти подходы базируются на принципах перемешивания и рассеивания, сформулированных К. Шенноном. Одной из фундаментальных архитектур блочных шифров, реализующих принципы перемешивания и рассеивания, является подстановочно-перестановочная сеть (ППС). В этой архитектуре криптографические функции реализуются посредством комбинации подстановочных и перестановочных преобразований. Перестановочные преобразования являются линейными, а подстановочные – основной источник нелинейности в шифре. Исследованию ППС и подстановочных преобразований посвящено множество работ разных авторов – C.M. Adams, K. Kim, B. Preneel, S.E. Tavares и др. В этих работах отмечается, что подстановочные преобразования не должны быть ни линейными, ни аффинными, ни даже близкими к ним. Используемые криптографические преобразования должны быть сбалансированными. Не должно быть корреляций между различными комбинациями бит. При изменении любого входного бита выходные биты должны вести себя независимо.

Для оценки качества криптографических преобразований в блочных шифрах используется ряд информационных критериев, названных критериями зависимости. В главе приводится методика тестирования на соответствие критериям зависимости, которая применялась при оценке финалистов AES.

В результате проведенного анализа ставится задача разработки специального двухканального криптографического преобразователя, реализующего механизм представления информации в виде двух частей. Такой преобразователь можно создавать как итерационный, симметричный, вероятностный шифр, каждая итерация которого напоминает раунд ППС.

Вторая глава посвящена синтезу двухканального преобразователя, который может рассматриваться как частный случай двухканального шифра вида

$$\begin{array}{ll} \textit{зашифрование}: & Y_1 = E_1(M,K) \\ & Y_2 = E_2(M,K), \\ \textit{расшифрование}: & M = E_{12}^{-1}(Y_1,Y_2,K), \end{array} \qquad (1)$$

где M – исходный текст, K – ключ, а Y_1 и Y_2 – две части выходного текста, E_1 и E_2 – необратимые функции, E_{12}^{-1} – обратное преобразование .

Существенной особенностью системы (1) является то, что выходной текст состоит из двух частей и для восстановления исходного текста M необходимо знание всех трех компонентов – ключа K и обеих – Y_1 и Y_2 – частей выходного текста. Это позволяет ввести различные режимы использования. В зависимости от режима использования атакующий систему (1) располагает различной информацией. Для системы (1) выписаны общие информационные зависимости, на основании которых предложена модель безопасности, аналогичная шенноновской.

Для построения конкретных систем вида (1) предложено использовать отображения с выходами переменой длины вида

$$f:\{0,1\}^n \to \bigcup_{i=r}^{m}\{0,1\}^i, \qquad (2)$$

которые отображают двоичные n-разрядные строки в строки, содержащие от r до m разрядов. На основании анализа таких отображений предложено рассмотреть преобразования, которые заменяют двоичные строки длиной n бит строками переменной длины *меньшей*, чем n. Так как число элементов в области определения таких преобразований больше, чем число элементов в области значения, то такие преобразования не являются обратимыми отображениями. Однако для восстановления исходного текста из преобразованного требуется, чтобы преобразование исходного текста было обратимым отображением. Это можно сделать следующим образом:

Зададим целые положительные значения r и n такие, что $0 < r < n$. Рассмотрим отображения вида $c:\{0,1\}^n \to \bigcup_{i=r}^{n-1}\{0,1\}^i$, которые обладают следующими свойствами:

- для любого элемента $y \in \bigcup_{i=r}^{n-1}\{0,1\}^i$ существует хотя бы один элемент $x \in \{0,1\}^n$, который является его прообразом при отображении c, т.е. $c(x) = y$;

- для любого элемента $y \in \bigcup_{i=r+1}^{n-1}\{0,1\}^i$ у отображения c имеется ровно один прообраз, и различные элементы имеют различные прообразы;
- для любого элемента $y \in \{0,1\}^r$ у отображения c существует ровно два прообраза.

Для каждого отображения c определим связанную с ним целочисленную функцию $f : \{0,1\}^n \to \{1,...,n-r+1\}$ следующим образом:

- $f(x) = n - |c(x)|$, если $|c(x)| > r$;
- для любых $x_1 \neq x_2 \in \{0,1\}^n$, имеющих одинаковые образы $c(x_1) = c(x_2) \in \{0,1\}^r$, значение функции f равно либо n-r, либо n-r+1.

Пара отображений (c,f) называется MV2-преобразованием.

Значения выходов отображения f можно закодировать двоичным кодом (ДК), как показано в таблице.

Таблица - Кодирование значений *f*

f(x)	1	2	3	…	*n-r*	*n-r*+1
ДК	1	01	0^21	…	$0^{n-r-1}1$	0^{n-r}

В таблице 0^i обозначает битовую строку из i нулей. Такой код будет оптимальным, если входы равномерно распределены. Под выходом отображения f можно понимать его представление двоичным кодом. В этом случае отображение f также является отображением с выходом переменной длины.

Проведен анализ информационных зависимостей между входами и выходами MV2-преобразования.

Введенное таким образом MV2-преобразование определено на множестве двоичных строк из n разрядов. Для применения в прикладных системах, оно распространяется на множество текстов, состоящих из символов алфавита $\{0,1\}^n$, следующим образом:

Пусть дан текст $M = x_1 \| x_2 \| ... \| x_L$, где $x_i \in \{0,1\}^n$ и $\|$ – операция конкатенации. Тогда MV2-преобразованием от текста M называется пара двоичных строк:

$$c(M) = c(x_1) \| c(x_2) \| ... \| c(x_L),$$
$$f(M) = f(x_1) \| f(x_2) \| ... \| f(x_L),$$

составленных из конкатенации соответствующих образов символов исходного текста. Для удобства выход MV2-преобразования $c(M)$ называется *остатком*, а выход $f(M)$ – *флагами*.

Каждой паре выходов $(c(M), f(M))$ фиксированного MV2-преобразования соответствует единственный исходный текст M, однако любому конкретному

выходу остатка $c(M)$ и флагов $f(M)$ соответствует некоторое множество возможных прообразов $\{\tilde{M}\}$. Для выходов остатка и флагов получены точные формулы количества прообразов в зависимости от длины входа и выхода. Получены информационные и статистические оценки для выходов MV2-преобразования, а также оценки длин выходов. При равномерном распределении входов M для энтропий выходов справедливы следующие информационные соотношения

$$(n-2+2^{r-n+1})L \le H(Y_C) \le \log(2^{(n-1)L+1}-2^{rL}),$$

$$L-1 \le H(M \mid Y_C) \le (2-2^{r-n-1})L,$$

$$H(Y_F) = (2-2^{n-r-1})L,$$

$$H(M \mid Y_F) = H(Y_C \mid Y_F) = (n-2+2^{r-n+1})L,$$

где L – длина входного сообщения в n-разрядных символах, $H(Y_C)$ – энтропия выхода остатка, $H(Y_F)$ – энтропия выхода флагов, а Y_C и Y_F – выходы остатка и флагов соответственно. Доказано следующее.

Утверждение. *Пусть текст* $M = x_1 \| x_2 \| ... \| x_L$ *состоит из* L *символов* $x_i \in \{0,1\}^n$, *которые случайно и равномерно выбираются из* $\{0,1\}^n$, *задано некоторое MV2-преобразование и* $Y_C = c(M)$, $Y_F = f(M)$ *– соответственно остатки и флаги,* полученные *в результате применения этого преобразования, а* $|Y_C|$ *и* $|Y_F|$ *– их длины. Тогда для математических ожиданий длины остатка* $E(|Y_C|)$ *и флагов* $E(|Y_F|)$ *выполняется:*

$$E(|Y_C|) = (n-2+2^{n-r+1})L, \quad (3)$$

$$E(|Y_F|) = (2-2^{r-n+1})L. \quad (4)$$

На основании утверждения вводятся коэффициенты, позволяющие оценить уменьшение длины выхода относительно исходного текста:

коэффициент сжатия остатка: $$K_c = 1 - \frac{n-2+2^{n-r+1}}{n}, \quad (5)$$

коэффициент сжатия флагов: $$K_f = \frac{2-2^{n-r+1}}{n}. \quad (6)$$

MV2-преобразование является нелинейным и может использоваться для синтеза двухканальных шифрсистем. Показано, что оно является сбалансированным, в том смысле, что при равномерном распределении входов вероятности того, что некоторый бит выхода остатка принимает значение 0 или 1, равны. Это свойство полезно для подстановочных преобразований.

На основании предложенного в [14-A] и [15-A] способа шифрования, разработана общая схема шифра с двумя выходами, использующая MV2-

преобразования. Для построения этой схемы зафиксируем параметры r и n, и выберем случайный упорядоченный набор $T_1, T_2, ..., T_k$ MV2-преобразований. Этот набор в дальнейшем будет рассматриваться как ключ. Весь процесс работы разобьем на раунды. На каждом раунде над входными данными будем выполнять перестановочное преобразование и некоторое MV2-преобразование, взятое из ключа. Выходом MV2-преобразования является остаток и флаги. Полученный остаток будем отправлять на вход следующего раунда, а флаги накапливать. Таким образом, на вход раунда поступает текст произвольной длины, а на выходе получается два текста.

Количество раундов может быть задано явно или косвенно. Остаток MV2-преобразования имеет меньшую, чем входной текст, длину. Поэтому вместо числа раундов можно указать максимальную длину для последнего остатка. В этом случае раунды будут повторяться до тех пор, пока на выходе не появится остаток с длиной, меньшей, чем заданная. Остаток последнего выполненного раунда называется ядром.

Такая схема напоминает ППС. Однако в архитектуре общей схемы разделения данных имеется существенное отличие от архитектуры ППС блочных шифров. При выполнении каждого раунда обрабатывается весь текст, а не один блок, как в блочных шифрах.

При преобразовании по предложенной схеме используется раундовая процедура *Raund(M)*, которая является вероятностной и выполняется по схеме:

$$Round(M) = \left(R \,\|\, c(M,R,K), f(M,R,K)\right),$$

где R – случайно сгенерированный блок бит, $c(K,R,M)$ и $f(K,R,M)$ – первая и вторая компоненты выхода подстановочного преобразования, M – сообщение и K – ключ.

При обратном преобразовании работает детерминированная процедура $Round^{-1}$ по следующей рекуррентной схеме:

$$\left(R_i \,\|\, C_i, F_i\right) = Round^{-1}\left(R_{i+1} C_{i+1}, F_{i+1}, K\right),$$

$$\left(M, \Lambda\right) = Round^{-1}\left(R_1 C_1, F_1, K\right),$$

где i – номер раунда, C_i, F_i – выходы соответствующего раунда, а Λ – пустая строка.

Таким образом, предложена общая схема реализации системы вида (1).

На основании полученных общих информационных зависимостей, введенной модели безопасности и свойств MV2-преобразования выполнен предварительный анализ предложенной схемы. Полученные оценки показали эффективность предварительного зашумления исходного текста и возможность рандомизации шифра в целом. Кроме того, показано, что для безопасности шифра необходимо выполнять не менее определенного числа раундов преобразования.

Все это позволило синтезировать двухканальный криптографический преобразователь, который, фактически, представляет собой симметричный вероятностный шифр, выход которого состоит из двух частей – ядра и флагов.

В двухканальном преобразователе в качестве подстановочных преобразований используются MV2-преобразования с параметрами n=8 и r =3. В качестве линейного преобразования используется 128-битный линейный преобразователь с высокой степенью диффузии (MIX), а для зашумления исходного текста применяется шифр RC4, ключи которого совпадают со способом задания MV2-преобразования. Алгоритм двухканального преобразования может быть представлен следующим псевдокодом:

Вход:

исходный текст M

ключ $T_1, T_2 ..., T_{32}$ – упорядоченный набор из 32 MV2-преобразований

число раундов m

if (m < minRound) m := minRound; (* выполнить не менее minRound раундов *)

Выбрать случайно $j_0 \in \{1,...,32\}$;

$C = M \oplus RC4(T_{j_0})$; (* забеливание текста M *)

Flags := (); (* пустая строка *)

Core := AUX (j_0,C)||C; (* добавляется служебная часть *)

for $1 \le i \le$m :

1. Выбрать случайное $j_i \in \{1,...,32\}$ (* j_i – индекс преобразования в ключе *)
2. Core := MIX(Core); (* выполнить перестановочное преобразование *)
3. Разобрать Core как Core[1],..., Core[L]; (* L – длина Core в байтах *)
4. for $1 \le l \le$ L: $(C[l], F(L) = T_{j_i}(\text{Core}[l])(C[l], F[l])$ (* применить преобразование T_{j_i} *)
5. Core:= AUX (j_i, Core)||C[1]||C[2]||...||C[L]|| b(Core); (* b(Core)обеспечивает кратность длины Core 8 *)
6. Flags := F[1]||F[2]||...||F[L]|| Flags;

Выход: текст (Core, Flags);

Синтезированный двухканальный криптографический преобразователь имеет следующие основные особенности:

- выходной текст состоит из *двух частей* – ядра и флагов;
- для восстановления исходного текста необходимо обладать всеми тремя компонентами – ключом, ядром и флагами;
- независимо от размера и содержания исходного текста, ядро можно сделать достаточно малым (но не меньше некоторой, зависящей от реализации величины);
- длина ключа, фактически примененного для преобразования, пропорциональна количеству раундов преобразования (в существующих реализациях: $\approx 1684 \cdot m$ двоичных разрядов, где m – число шагов);

- синтезированный алгоритм – псевдослучайный, при многократном преобразовании одного и того же исходного текста получаются различные пары ядер и флагов, что позволяет использовать долговременные ключи.

В третьей главе проводится анализ и тестирование синтезированного алгоритма. Анализируется безопасность синтезированного алгоритма при неизвестном выходе ядра или неизвестном выходе флагов. Из проведенного анализа следует, что для стойкости алгоритма необходимо, чтобы длина выхода ядра была не слишком малой; псевдослучайный выбор подстановочного преобразования из ключа увеличивает стойкость алгоритма в случае, когда один из выходов неизвестен; использование алгоритма небезопасно, если атакующий знает выход флагов, исходное сообщение и ключ.

На основании свойств MV2-преобразования, получены статистические оценки, такие, как математическое ожидание для длин выходов и количество возможных исходных текстов в различных режимах использования.

Математическое ожидание длин выхода определяется по формулам

$$\mathrm{E}\big(L(\mathrm{Core})\big) \approx K_c^m \cdot (L(M)+1) + \frac{159}{128} \cdot \frac{1-K_c^{m+1}}{K_f}, \tag{7}$$

$$\mathrm{E}\big(L(\mathrm{Flags})\big) \approx (1-K_c^{m+1}) \cdot (L(M)+1) + \frac{225}{128} m - 1 - \frac{1-K_c^{m+1}}{K_f}, \tag{8}$$

где, $L(M)$ – длина сообщения в байтах, $L(\mathrm{Core})$ – длина ядра в байтах, $L(\mathrm{Flags})$ – длина выхода флагов в байтах, K_c и K_f – коэффициенты определяемые по формулам (5) и (6).

Анализ алгоритма показал, что если известно только ядро и нет ограничения на количество раундов, то даже при известных ключах имеется бесконечное множество текстов, которые дают такое ядро. При ограниченном числе раундов множество соответствующих данному ядру исходных текстов конечно, но не меньше, чем: $N_C \geq 2^{\left(\frac{128}{31}\left(\frac{128}{97}\right)^m \frac{1}{31}\right)L(\mathrm{Core})}$. Если известны только флаги и неизвестна длина исходного текста и число раундов, то резко уменьшается вероятность угадывания исходного текста. Задача нахождения M по известным K и флагам имеет сложность $2^{H(|\mathrm{Core}|)}$. В реальных приложениях в результате шифрования длина ядра |Core|>128 бит, поэтому сложность задачи нахождения M по известным K и выходу флагов соответствует современным требованиям. Частотная характеристика выхода первых флагов не коррелирует с частотной характеристикой модельного языка.

Методика тестирования на соответствие критериям зависимости, которая применялась при тестировании финалистов AES, неприменима при использовании преобразований с выходом переменной длины. Между тем критерии за-

висимости, в особенности строгий лавинный критерий, позволяют оценить качества подстановочных преобразований. В критериях зависимости для измерения степени отличия двоичных строк используется расстояние Хемминга. Для строк различной длины построен следующий аналог расстояния Хемминга.

Определение. *Расстоянием между двоичными строками* x *и* y *называется число* $h(x,y) = w(\bar{x}^k, \bar{y}^k) + \|x| - |y\|$, *где* $k = min\{|x|, |y|\}$, *а* $\bar{x}^k$ *и* $\bar{y}^k$ *обозначают* k*-разрядные* двоичные *строки, соответствующие разряды которых совпадают с соответствующими разрядами двоичных строк* x *и* y; $w(\bar{x}^k, \bar{y}^k)$ – *расстояние Хемминга.*

Применение критериев зависимости для исследования синтезированного алгоритма требует пересмотра определений и формул для вычисления матриц расстояний и зависимости.

Матрицей зависимости функции g называется $n \times m$ матрица A с элементами a_{ij}, равными числу таких входов, для которых в результате изменения i-го входного бита изменяется j-й выходной бит, т.е.

$$a_{ij} = |\{x \in X \,|\, (g(x^{(i)}))_j \neq (g(x))_j\}|$$

для $i = 1, \ldots, n$ и $j = 1, \ldots, m$.

Матрицей расстояний функции g называется $n \times (m+1)$ матрица B с элементами b_{ij}, равными числу таких входов, для которых в результате изменения i-го входного бита изменяется j выходных бит, т.е.

$$b_{ij} = \left|\{x \in X \,|\, h((g(x^{(i)}))_j - (g(x))_j) = j\}\right|.$$

Показатели критерия лавины $\bar{d}_a$ и показатель критерия строгой лавины $\bar{d}_{sa}$ рассчитываются по формулам

$$\bar{d}_a = 1 - \frac{1}{m \cdot n} \sum_{i=1}^{n} \left| \frac{2}{\#X} \sum_{j=1}^{\bar{m}} j \cdot b_{ij} - \bar{m} \right|,$$

$$\bar{d}_{sa} = 1 - \frac{1}{m \cdot n} \sum_{i=1}^{n} \sum_{j=1}^{\bar{m}} \left| \frac{2a_{ij}}{\#X} - 1 \right|.$$

Здесь, в отличии от обычных критериев зависимости $m = \bar{m}$ или $\tilde{m}$, где $\bar{m} = \max\{|g(x^{(i)})| : x \in X\}$ или $\tilde{m} = \frac{1}{\#X} \sum_{x \in X} |g(x^{(i)})|$.

При тестировании на соответствие критериям полноты, лавины и строгой лавины, брались входные последовательности длиной по 16, 32, 64 и 128 байт. Исходные данные брались из файла, содержащего последовательность, полученную с физического генератора случайных чисел. Определялись максимальная длина выхода, средняя длина ядра L_c^* и флагов L_f^*, среднее число изменив-

шихся бит при изменении 1 бита входного текста и вычислялись по (13) отдельно для ядра и флагов степени полноты, лавины (d_a^c и d_a^f) и строгого лавинного критерия (d_{sa}^c и d_{sa}^f).

$$d_a = \frac{d_a^c \cdot L_c^* + d_a^f \cdot L_f^*}{L_c^* + L_f^*}, \qquad d_{sa} = \frac{d_{sa}^c \cdot L_c^* + d_{sa}^f \cdot L_f^*}{L_c^* + L_f^*}.$$

Анализ результатов тестирования по предложенной методике позволил выбрать оптимальное перестановочное преобразование, оценить влияние забеливания, а также значение псевдослучайного выбора подстановочных преобразований. Результаты тестирования подтверждают, что стойкость алгоритма зависит от длины входа и количества выполненных раундов. Они подтверждают предположение о повышении эффективности алгоритма при увеличении длины исходного текста.

Из проведенного анализа следует, что реализация алгоритма должна быть построена таким образом, чтобы не допускать коротких (менее 128 бит) выходов остатка. В общем случае рекомендуется выполнять не менее 16 раундов преобразования. Используемое в алгоритме забеливание исходного текста, скрывая специфику входов на первом раунде, значительно увеличивает трудность атаки по известным флагам. Его влияние усиливается при увеличении длины входа. Псевдослучайная смена перестановочных преобразований значительно сильнее влияет на показатели критериев зависимости, чем вид линейного преобразователя и существенно усложняет взлом, когда известны оба выхода (ядро и флаги).

Результаты тестирования показывают, что выбранный класс преобразований обеспечивает высокую степень нелинейности, и позволяют сделать вывод о стойкости двухканального преобразователя как алгоритма шифрования.

Результаты статистического тестирования показывают, что выходы алгоритма статистически неотличимы от случайных при наблюдении выходов "разумной" с точки зрения практики длины, независимо от вида входных данных, и подтверждают правильность полученных для оценки длин выходов формул (7) и (8).

Синтезированный двухканальный преобразователь обладает достаточно высокими скоростными характеристиками, которые, однако, существенно ниже, чем у стандартных криптосистемы (например, AES работает примерно в 3 раза быстрее для Intel-совместимых системах). В отличие от стандартных систем он разделяет исходные тексты на две части и может использоваться в таких режимах, которые у стандартных систем отсутствуют. На основании свойств синтезированного двухканального алгоритма появляется возможность разрабатывать принципиально новые многоканальные системы защиты информации.

В четвертой главе рассмотрены вопросы применения двухканального преобразователя в реальных приложениях. Одним из способов такого применения является запатентованная технология MVZ Messaging, предназначенная для создания разнесенных телекоммуникационных систем. В этой технологии использован комбинированный криптографический алгоритм MVZ. При использовании этого алгоритма ядро, полученное после применения синтезированного алгоритма, подвергается вторичному криптографическому преобразованию. В качестве дополнительного криптографического преобразования может быть использовано любое стойкое криптографическое преобразование – симметричное или асимметричное. В такой системе ключи первичного преобразования обеспечивают параметр безопасности клиента, а ключи вторичного криптографического преобразования – параметр безопасности владельца системы (например, платежи).

Свойства технологии определяются наличием различных режимов использования двухканального преобразователя и возможностью управления длинами выходных частей. Так как без ядра невозможно восстановление исходного сообщения, то пересылка информации через центральный узел обеспечивает его контроль над системой в целом. С другой стороны, поскольку длина ядра ограничена, то для функционирования центрального узла не требуется сверхвысоких ресурсов. Таким образом, возникает система с архитектурой, подобной схеме "звезда", лишенная основного недостатка таких систем – повышенной нагрузки на центральный узел системы.

Если клиенты системы доверяют центральному узлу, то обеспечивается аутентификация сообщений и отправителей.

Аналогично, пользователи имеют возможность обменяться ключами удаленно, без привлечения методов асимметричной криптографии.

Манипуляция короткими ядрами, флагами и ключами позволяет синтезировать системы распределенного хранения данных, обмена конфиденциальными данными, создания и санкционированного воспроизведения неподдельных цифровых носителей данных (например, CD), защиты интеллектуальной собственности и др. На основе технологии MVZ Messaging были синтезированы новые продукты:

- системы безопасного обмена сообщениями по электронной почте между абонентами;
- электронная система идентификации товарных ярлыков;
- система раздельного хранения данных на PC и электронном ключе;
- система создания некопируемых CD и санкционированного их воспроизведения.

Одним из вариантов применения технологии MVZ Messaging является синтез систем обмена конфиденциальной информацией между абонентами.

Клиенты системы обмениваются сообщениями, преобразованными двухканальным алгоритмом MV2. Полученное после преобразования ядро передается через провайдера системы по одному информационному каналу, а флаги по другому информационному каналу – напрямую получателю сообщения. Ядро дополнительно зашифровывается вторичным криптографическим преобразованием. Ключами этого преобразования управляет провайдер системы.

В таком варианте MVZ Messaging обеспечивает:

- высокую степень криптографической защиты передаваемой информации;
- возможность наращивания абонентской сети путем добавления новых абонентов;
- возможность идентификации и аутентификации сообщений и клиентов;
- возможность обмена между клиентами новыми ключами по открытым каналам связи; возможность контроля клиентов без нарушения конфиденциальности информации;
- защиту финансовых интересов владельца.

Одним из вариантов реализации системы обмена конфиденциальной информацией на основе технологии MVZ Messaging является система защищенного обмена почтовыми сообщениями – SolanioE-Mail, предназначенная для осуществления защищенной связи между пользователями, которые обмениваются конфиденциальными сообщениями по открытым каналам связи. Она представляет собой разнесенную телекоммуникационную систему и основывается на использовании двухканального криптографического преобразователя и симметричного алгоритма шифрования MZ4. Особенностью этой системы является защищенность передаваемой информации от несанкционированного чтения и фальсификации. Solanio E-Mail обеспечивает высокую степень криптографической защиты передаваемой информации, простоту добавления новых абонентов, возможность идентификации и аутентификации сообщений и возможность обмена между клиентами новыми ключами по открытым каналам связи.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Результаты, полученные в ходе диссертационного исследования можно сформулировать следующим образом.

1. В работе установлено, что конкретный класс отображений с выходом переменной длины можно использовать в качестве подстановочных преобразований для синтеза двухканального преобразователя [1-А, 2-А, 6-А, 7-А,10-А, 11-А].
2. На основании выбранного класса отображений предложена общая схема разделения исходного текста на две части, а также способ и устройство

обобщающую эту схему. Новизна способа подтверждена патентами [13-А, 14-А].

3. Разработан двухканальный преобразователь, являющийся симметричным шифром, выход которого состоит из двух частей. Разработанный преобразователь обеспечивает представление исходной информации в виде двух частей, имеет дополнительный параметр, позволяющий управлять их длинами, и может использоваться в различных режимах [1-А, 2-А, 3-А, 4-А, 7-А, 10-А].
4. Выполнен анализ безопасности для различных режимов использования двухканального преобразователя [1-А, 2-А, 4-А, 8-А].
5. Предложена методика тестирования алгоритма на соответствие информационным критериям зависимости. Анализ результатов тестирования в соответствии с предложенной методикой позволил выбрать оптимальное перестановочное преобразование, оценить влияние забеливания, а также значение псевдослучайного выбора подстановочных преобразований. Кроме того, тестирование на соответствие критериям зависимости подтвердило предположение о повышении эффективности алгоритма при увеличении длины исходного текста. Результаты тестирования позволяют сделать вывод о стойкости алгоритма шифрования [1-А, 2-А, 8-А, 9-А].
6. Предложена технология MVZ Messaging, использующая алгоритм MV2. Новизна предложенной технологии подтверждена патентами [13-А, 16-А]. Предложена прикладная система защищенного обмена почтовыми сообщениями, реализующая технологию MVZ Messaging, которая использует свойства синтезированного алгоритма [5-А].

Рекомендации по практическому использованию результатов

Синтезированный в данной диссертационной работе двухканальный преобразователь обеспечивает новый способ представления информации и обладает рядом свойств, которые позволяют создавать новые эффективные приложения для защиты данных, авторизации, удаленного хранения данных, управления ключами, защиты прав собственности, проверки подлинности сообщений и др. Его использование, в совокупности с известными и доказанными технологиями шифрования, может значительно повысить их надежность без изменения существующих корпоративных технологий и политик безопасности. Примером применения синтезированного преобразователя является предложенная в работе технология MVZ Messaging. Эта технология реализована в программном продукте Solanio E-Mail, который используется в нескольких организациях.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Монографии

1-А. Мищенко, В.А. Ущербные тексты и многоканальная криптография / В.А. Мищенко, Ю.В. Виланский; под общ. ред. В.А. Мищенко. – Минск: Энциклопедикс, 2007. – 292 с.

2-А. Мищенко, В.А. Криптографический алгоритм MV2 / В.А. Мищенко, Ю.В. Виланский, В.В Лепин; под общ. ред. В.А. Мищенко. – Минск: Энциклопедикс, 2007. – 176 с.

Статьи в журналах

3-А. Виланский, Ю.В. Кодирование информации на основе алгоритма универсального сжатия / Ю.В Виланский, В.А. Мищенко // Вести Института современных знаний. – 2000. – №1. – С. 36-39.

4-А. Виланский, Ю.В. Алгоритм шифрования MV2 – дверь с двумя замками / Ю.В. Виланский // Вести Института современных знаний. – 2001. №2. – С. 84–89.

5-А. Виланский, Ю.В. Система защищенного обмена сообщениями MVZ-messaging / Ю.В. Виланский, В.В. Захаров, В.А. Мищенко // Вести Института современных знаний. – 2000. – №1. – С. 40-45.

6-А. Виланский, Ю.В. Информационные утечки в отображениях с образами различной длины / Ю.В. Виланский, В.В. Лепин // Весці НАН Беларусі. Сер. фіз.-мат. навук. – 2004. – №3. – С. 47–53.

7-А. Виланский, Ю.В. Двухканальный алгоритм шифрования MV2 / Ю.В. Виланский, В.В. Лепин, В.А. Мищенко // Вести Института современных знаний. – 2003.– №3-4. С. 113–121.

8-А. Виланский, Ю.В. Двухканальный алгоритм шифрования MV2 / Ю.В. Виланский, В.В. Лепин, В.А. Мищенко // Вести Института современных знаний. 2004.– №1. – С. 77-88.

Материалы докладов

9-А. Лепин, В.В. Криптографические критерии для нелинейных преобразований с образами различной длины / В.В. Лепин, Ю.В. Виланский // Научная сессия МИФИ-2004 г. Москва.: Труды научных сессий МИФИ. Т.12. Информатика и процессы управления. Компьютерные системы и технологии. – С. 166-167.

10-А. Виланский, Ю.В. Криптографический примитив MV2 / Ю.В. Виланский // Материалы конференции «Математика и безопасность информационных технологий» ИПИП, МГУ им. М.В. Ломоносова, Академия криптографии МаБИТ-04, 28-29 октября 2004 г. Москва. М.: МЦНМО, 2005. – С. 156.

11-А. Лепин, В.В. Информационные утечки в случайных отображениях с образами различной длины / В.В. Лепин, Ю.В. Виланский // Информационные системы и технологии: материалы I международной конф., г. Минск, 5–8 ноября 2002г.: в 2 ч. / БГУ; ред. кол.: А.Н. Курбацкий [и. др.]. – Минск, 2002. – Ч. 2. – С. 17–22.

Патенты

12-А. Способ шифрования, передачи, хранения конфиденциальных сообщений и система для осуществления способа: Пат. № 004904 Евразийский, МКИ H04L9/06. / В.А Мищенко, В.В. Захаров, Ю.В. Виланский; Заявитель В.А. Мищенко – Заявка – № 200200467. Заявлено 15.10.1999; Дата выдачи 26.08.2004. – 90 с.

13-А. Способ шифрования и дешифрования информации и устройство для его осуществления: Пат. № 003679 Евразийский, МКИ H04L9/06. В.А Мищенко, В.В. Захаров, Ю.В. Виланский, Д.И. Вержбалович; Заявитель В.А Мищенко – Заявка – № 200101127. Заявлено 27.04.1999; Опубл . 02.11.2000; Приоритет 27.04.1999. – 9 с.

14-А. Method for encrypting information and device for realization of the method / V.A. Michtchenko, U.U. Zakharau, Y.V. Vilansky, D.I. Verzhbalovich; Заявитель: V.A. Michtchenko // International Application Number: PCT/BY99/00005. International Publication Number: WO 00/65767. International Publication Date: 02 November 2000. Int. Filing Date: 16 Mart 1999. http://pctgazette.wipo.int/. – 23 p.

15-А. Methods for encoding, decoding, transferring, storage and control of information, systems for carrying out the methods / V.A. Michtchenko, U.U. Zakharau, Y.V. Vilansky; Заявитель V.A. Michtchenko // International Application Number: PCT/BY99/00008. International Publication Number: WO 01/30017. International Publication Date: 26 April 2001. Int. Filing Date: 15 October 1999. http://pctgazette.wipo.int/. – 105 p.

РЭЗЮМЭ

Віланскі Юрый Віктаравіч

Сінтэз і аналіз двухканальнага крыптаграфічнага пераўтваральніка

Ключавыя словы: двухканальныя сістэмы, паданне інфармацыі ў выгляду двух частак, пераўтварэнне крыптаграфічнае, пераўтварэнні с выхадамі рознай даўжыні, крытэрыі залежнасці, стойкасць, сінтез.

Аб'ектам даследавання з'яўляюцца пераўтварэннії з выхадамі рознай даўжыні. Прадмет даследаванія – алгарытмы, якія выкарыстоўваюць гэтыя пераўтварання для падзелу інфармацыі і аттрымання яе падання з патрабнымі магчымасцямі.

Мэтай даследавання з'яўляецца сінтэз двухканальнага кріптаграфічнага пераўтваральніка.

Метадалогія даследавання грунтуецца на аналізе сучасных падыходаў да пабудавання сіметрычных шыфрсістэм і крыптаграфічных пратаколаў і гіпотэзе аб прымянімасці пэўнага класа пераўтварэнняў з выхадамі рознай даўжыні для сінтэзу сіметрычных шыфрсістэм.

Атрыманыя вынікі і іх навізна заключаюца ў тым, што ўпершыню ў якасці падстановачных пераўтварэнняў прапануецца выкарыстаць пераўтварэнні з выхадамі рознай даўжыні, праводзіцца даследаванне такіх пераўтварэнняў, выбіраюцца класы пераўтварэнняў, дастасаваныя да сінтезу новых крыптасістэм. Вынікам выкарыстання таких пераўтварэнняў з'яўляеца паданне інфармацыі у выглядзе двух частак, і сінтэз двухканальнага пераўтваральніка. Даследуюцца ўласцівасці сінтэзаванага алгарытму, і прапаноўваецца методыка яго тэстыравання.

Абсягам выкарыстання атрыманых вынікаў з'яўляецца масавыя інфармацыйныя тэхналогіі. Сінтэзаваны алгарытм выкарыстоўваецца ў праграмным прадукце SolanioE-Mail, які забяспечвае функцыянаванне абароненай электроннай пошты.

РЕЗЮМЕ

Виланский Юрий Викторович

Синтез и анализ двухканального криптографического преобразователя

Ключевые слова: двухканальные системы, представление информации в виде двух частей, преобразование криптографическое, отображения с выходами разной длины, критерии зависимости, стойкость, синтез.

Объектом исследования данной работы являются отображения с переменной длиной выхода. Предметом исследования являются алгоритмы, использующие такие отображения для разделения информации и получения ее представления с требуемыми свойствами.

Целью исследования является синтез двухканального криптографического преобразователя.

Методология исследования основывается на анализе современных подходов к построению симметричных систем и криптографических протоколов и гипотезе о применимости некоторого класса отображений с выходами переменной длины для синтеза симметричных криптосистем.

Полученные результаты и их новизна выражаются в том, что впервые в качестве подстановочных преобразований предлагаются отображения с выходами переменной длины, проводится анализ таких отображений, выбираются классы таких преобразований, пригодные для синтеза новых криптосистем. Естественным следствием применения таких преобразований становится представление информации в виде двух частей, в результате применения таких подстановочных преобразований синтезируется алгоритм двухканального преобразователя. Исследуются свойства синтезируемого алгоритма, и предлагается методика его тестирования.

Областью применения полученных результатов являются массовые электронные технологии. Синтезированный алгоритм встроен в программный продукт SolanioE-Mail, который обеспечивает функционирование защищенной электронной почты.

THE SYMMARY

Vilanski Yury Viktorovich

The synthesis and analysis two-channel cryptographic reorganizer

Key words: two-channel ciphersystems, representation of the information in two parts, cryptographic transformation, transformation with outputs of different length, dependence criteria, resistance, synthesis.

The subject of the research is transformations with variable length of an output. The object of the research is opportunity of applying of such mappings for representation of the information in two parts which can be kept, processed and/or transferred separately.

The purpose of research is synthesis of two-channel reorganizer.

The methodology of the research is based on the analysis of modern approaches to construction of symmetric systems and cryptographic protocols and a hypothesis about applicability of some class of transformations with outputs of variable length for synthesis of symmetric cipher systems.

The received results and their novelty are that mappings with outputs of variable length are offered as substitutional transformations, analysis of such transformations is carried out and classes of such transformations suitable for synthesis new ciphersystem are selected for the first time. The natural consequence of using such transformations becomes representation information in two parts. Two-channel cryptographic reorganizer is synthesized as a result of using such transformations. Properties of synthesized algorithm are researched, and the technique of its testing is offered.

The field of application of the received results is mass electronic technologies. The synthesized algorithm is built in the software product SolanioE-Mail that provides functioning of protected e-mail.

Научное издание

ВИЛАНСКИЙ Юрий Викторович

СИНТЕЗ И АНАЛИЗ ДВУХКАНАЛЬНОГО КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАТЕЛЯ

Специальность 05.13.17 – Теоретические основы информатики

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 22.01.2008. Формат 60×84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л. 1,63.
Уч.-изд. л. 1,3. Тираж 60 экз. Заказ 51.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П. Бровки, 6