Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»

УДК 681.3.06.004

ЗАХАРОВ
ВЛАДИМИР ВЛАДИМИРОВИЧ

СИНТЕЗ И ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ НА ОСНОВЕ РАНДОМИЗАЦИИ С АЛФАВИТОМ БОЛЬШОЙ МОЩНОСТИ

Специальность 05.13.17 – Теоретические основы информатики

Автореферат диссертации
на соискание ученой степени
кандидата технических наук

МИНСК 2004

Работа выполнена в Частном учреждении образования «Институт современных знаний им. А.М. Широкова»

Научный руководитель:	доктор технических наук, профессор Мищенко В.А. Частное учреждение образования «Институт современных знаний им. А.М. Широкова»
Официальные оппоненты:	Доктор технических наук, профессор, Голиков В.Ф. Государственное предприятие «Научно-исследовательский институт защиты информации»
	Кандидат физико-математических наук, старший научный сотрудник Лепин В.В. Институт математики НАН Беларуси
Оппонирующая организация:	Научно-исследовательское учреждение «Институт прикладных физических проблем им. А.Н. Севченко» Белгосуниверситета

Защита состоится « 8 » апреля 2004 г. в 14.00 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, I уч. корп., ауд. 232, тел. 2398989.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. Одним из важнейших направлений на пути решения проблемы защиты информации является ее шифрование. В то же время достоянием широкой гласности стали множество фактов взлома систем защищенных программными и аппаратными сертифицированными реализациями криптоалгоритмов, еще вчера считавшихся стойкими. Современные криптографические алгоритмы строятся по принципу последовательного выполнения нескольких элементарных криптографических преобразований, совокупность которых отвечает требованиям, предъявляемым к шифру. Известно, что одним из таких преобразований, представляющих существенную трудность при атаке на криптографический алгоритм, является рандомизация. Она обеспечивает случайность процесса зашифрования, или хотя бы отдельных его элементов. Рандомизация может выполняться путем подмешивания, например операцией XOR, гаммы с выхода псевдослучайного датчика к исходным данным перед или в процессе зашифрования, или простым добавлением короткой случайной строки к блоку зашифровываемого текста. Другим рандомизационным приемом, предложенным еще К.Гауссом, является случайная замена букв алфавита исходного текста буквами алфавита рандомизатора, причем мощность алфавита рандомизатора больше мощности алфавита исходного текста. Однако в известной автору литературе отсутствуют ответы на следующие вопросы:

Насколько большой должна быть мощность алфавита рандомизатора?

Как влияет мощность алфавита рандомизатора на свойства криптографического алгоритма?

В дальнейшем под большой мощностью алфавита рандомизатора будем понимать мощность, которая много больше мощности алфавита входного текста. Этот термин будет количественно уточнен по ходу изложения материала.

Таким образом, исследование влияние мощности алфавита рандомизатора на свойства криптографического алгоритма является актуальным.

Связь работы с крупными научными программами, темами. Основные результаты диссертационной работы использованы при выполнении:

НИР «Синтез и исследование рандомизационных преобразований на основе полиалфавитных подстановок с алфавитом больших размерностей» (регистрационный номер 20013254, дата регистрации 13-08-2001);

НИР «Исследование статистических свойств и информационных утечек в полиалфавитных рандомизационных преобразованиях» (регистрационный номер 20023166, дата регистрации 02-10-2002).

Цель и задачи исследования. Целью исследования является влияние рандомизаторов с алфавитом большой мощности на свойства криптографических алгоритмов.

В работе поставлены следующие задачи:

теоретически исследовать влияние мощности алфавита рандомизатора на свойства криптографической системы;

разработать методику синтеза рандомизаторов с алфавитом большой мощности;

синтезировать и исследовать синтезированные рандомизаторы;

на основе проведенного синтеза и исследования дать практические рекомендации по использованию таких рандомизаторов в практических системах.

Объект и предмет исследования. Объектом исследования являются рандомизаторы с алфавитом большой мощности, используемые в криптографических алгоритмах. В качестве предмета исследования в работе рассмотрены:

рандомизаторы, в которых отождествление букв алфавита исходного текста буквам алфавита рандомизированного текста выполняется:

на основе геометрического места точек, описываемых с помощью функций со случайными аргументами;

на основе кусочных разрывных функций со случайными аргументами (наибольшее внимание уделено целочисленным кусочно-линейным разрывным функциям);

возможность практического применения исследованных рандомизаторов в комплексе с другими криптографическими преобразованиями.

Гипотеза.

Использование рандомизаторов с бесконечной мощностью алфавита в комплексе с другими криптографическими преобразованиями обеспечивают статистическую независимость криптограммы от исходного текста.

Возможен синтез рандомизаторов с конечным, достаточно большим алфавитом, которые дают возможность получать с заданной вероятностью криптограммы статистически независимые от исходного текста.

Методология и методы проведенного исследования. На основе проведенного анализа современных криптографических алгоритмов выдвинута гипотеза о возможности синтеза рандомизаторов с конечным, достаточно большим алфавитом рандомизации, которые позволяют с заданной вероятностью получать криптограммы статистически независимые от исходного текста.

На основе статистической модели получена оценка мощности алфавита рандомизатора, при которой с заданной вероятностью достигается статистическая независимость исходного и рандомизированного текстов.

Выполнен синтез полных рандомизаторов с большим алфавитом рандомизации, позволяющий оценить их свойства с целью определения целесообразности практической реализации таких рандомизаторов в виде программного продукта.

Осуществлен анализ криптографической стойкости рандомизаторов, синтезированных на основе целочисленных кусочно-линейных разрывных функций, который позволяет сделать выводы об их практической стойкости.

Синтезированный алгоритм рандомизации реализован в виде программного продукта.

Выбрана модель для экспериментального доказательства свойств синтезированных рандомизаторов.

Синтезированный рандомизатор использован в комплексном криптографическом алгоритме MVZ, реализованном в двухканальной телекоммуникационной системе MVZ messaging.

В работе использованы методы: а) теории вероятностей; б) теории информации; в) теории чисел; г) теории множеств; д) дискретной математики.

Научная новизна и значимость полученных результатов.

1) Исследованы полные рандомизаторы с алфавитами больших размерностей. Показано, что такие рандомизаторы при мощности алфавита рандомизации $L \to \infty$ обеспечивают бесконечную энтропию криптосистемы и, статистическую независимость криптограммы от исходного текста. При этом возможно получение различной степени приближения к статистической независимости исходного и зашифрованного текстов путем использования рандомизатора с ограниченным, достаточно большим алфавитом рандомизации;

2) Дана численная оценка мощности алфавита рандомизатора, при которой достигается с заданной вероятностью статистическая независимость исходного текста и криптограммы;

3) Показано, что использование таких рандомизаторов в комплексе с другими известными практически стойкими криптопреобразованиями, приводит с заданной вероятностью к статистической независимости криптограммы на выходе комплексированной системы от исходного текста;

4) Предложен способ отождествления алфавита исходного текста алфавиту рандомизатора при помощи целочисленных кусочно-линейных разрывных функций;

5) Разработана методика синтеза и синтезированы криптографические преобразования на основе полной рандомизации с алфавитом большой мощности, а также получены оценки стойкости синтезированных рандомизаторов.

6) Экспериментально подтверждены свойства рандомизаторов с большой мощностью алфавита рандомизации.

Предложенные рандомизаторы могут использоваться в комплексе с другими криптографическими алгоритмами для повышения их криптографической стойкости. В связи с увеличением длины рандомизированного текста по сравнению с исходным, такие рандомизаторы наиболее целесообразно использовать для шифрования коротких сообщений. Реализован комплексный алгоритм, включающий синтезированный рандомизатор MZ4 в двухканальной телекоммуникационной системе MVZ messaging. Научная новизна результатов подтверждена полученными патентами [10,11].

Практическая (экономическая) значимость полученных результатов обусловлены актуальностью темы и заключаются в следующем:

разработано новое криптографическое преобразование на основе рандомизации с алфавитом большой размерности с использованием кусочно-линейных разрывных функций, стойкое к приведенным в работе атакам;

разработанное криптографическое преобразование может быть использовано совместно с известными алгоритмами с целью повышения их стойкости, дает дополнительные степени свободы в процессе синтеза новых криптографических алгоритмов со специфическими требованиями для специальных приложений.

Алгоритм синтезированнного криптографического преобразования использован в программном продукте SolanioE-Mail, обеспечивающем функционирование защищенной электронной почты ММПП «Салют» (г. Москва), ГВЦ «Интурист» (г. Москва), в коммерческих продуктах фирмы Hermelin ФРГ: CryptecMZ4; CryptecE-Mail двухканальная защищенная электронная почтовая служба; CryptecLabel – технология создания и проверки защищенных товарных ярлыков; CryptecWEB технология обмена конфиденциальной информацией через Internet, в программных продуктах УП «Творческая лаборатория» г.Минск.

Основные положения диссертации, выносимые на защиту:

- оценка мощности алфавита рандомизатора, обеспечивающей с заданной вероятностью статистическую независимость криптограммы и исходного текста;
- способ отождествления алфавита исходного текста алфавиту рандомизатора при помощи целочисленных разрывных кусочно-линейных функций;
- методика синтеза рандомизаторов с алфавитом большой мощности;
- рандомизатор MZ4, синтезированный на основе целочисленных разрывных кусочно-линейных функций;
- практическое применение рандомизатора MZ4 в двухканальной телекоммуникационной системе MVZ messaging.

Личный вклад соискателя заключается в:

получении численной оценки мощности алфавита рандомизатора, при которой с заданной вероятностью достигается статистическая независимость исходного текста и криптограммы;

предложении методики синтеза криптографических преобразований на основе полной рандомизации с алфавитом большой мощности;

синтезе криптографического преобразования на основе разработанной методики;

исследовании свойств синтезированных рандомизаторов;

разработке алгоритма функционирования двухканальной телекоммуникационной системы MVZ messaging на основе комплексного криптографического преобразования MVZ.

Апробация результатов диссертации проведена на семи международных выставках («CeBIT» – г. Ганновер, ФРГ 1997–2002 гг., «Модуль» – г. Москва,

Российская федерация 1998 г.), четырех международных конференциях («Комплексная защита информации» г. Минск 1998, 2001 г.г., «Информационные системы и технологии (IST'2002)» г.Минск, 5-8 ноября 2002 г., «Технические средства защиты информации» Минск-Нарочь 19-23 мая 2003 г.) и двух семинарах (Институт безопасности информации г. Минск, Белорусский государственный университет, кафедра прикладной математики).

Опубликованность результатов. По результатам исследований опубликовано 14 научных работ, в том числе 5 статей в научных журналах и сборниках, 3 материала докладов, 1 тезисы доклада, 2 патента, 3 заявки РСТ на международные патенты. Общий объем опубликованных материалов составляет 250 страниц.

Структура и объем диссертации. Диссертация включает в себя: введение, общую характеристику, 4 главы, заключение, 2 приложения, общим объемом 161 стр., в том числе: 36 иллюстраций – 15 стр., 5 таблиц – 2 стр., 2 приложения – 48 стр. Использованы 92 литературных источника на 7 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** обсуждается актуальность выбранной тематики.

В **первой главе** диссертации рассмотрены основные положения, допущения и методы криптографии. Выполнен анализ использования рандомизаторов в современных криптографических системах. Показана целесообразность и преимущества использования вероятностных методов шифрования. Сформулирована цель диссертационной работы и ставятся задачи исследования.

Процесс шифрования является вероятностным, если алгоритм шифрования, исходный текст и секретный ключ не определяют однозначно зашифрованный текст. Повышение стойкости известных шифров за счет задания неопределенности хода шифрования является одним из перспективных направлений криптографии.

В работе приведены варианты использования рандомизатора в качестве дополнительного исходного текста и в качестве дополнительного, секретного ключа, который заранее не известен на стороне расшифрования, для получения доказуемой стойкости шифров. Рандомизатор в качестве дополнительного исходного текста применяют в специальных режимах использования блочных криптографических алгоритмов с целью осложнить атаку на основании

подобранного текста. Однако такой прием существенно не влияет на стойкость шифра.

Рассмотрены варианты применения рандомизаторов с целью обеспечения доказуемой стойкости шифра. Об этом можно сказать следующее:

- лента одноразового использования непрактична из-за слишком большого размера ключа в большинстве приложений;
- совершенные локальные рандомизаторы основаны на нереалистичном предположении о том, что криптоаналитик может получить лишь небольшое число бит криптотекста;
- широкополосный канал Вайнера основан на нереалистичном предположении о том, что канал подслушивания более зашумлен, чем основной канал;
- алгоритм Рип ван Винкля и алгоритм вероятностного шифрования Месси основан на нереалистичных предположениях (время расшифрования пропорционально квадрату времени взлома);
- квантовая криптография (Беннет, Брассард и др.) по существу практична, основана на принципах квантовой физики, однако в настоящее время обладает низким быстродействием;
- существенное улучшение поточного шифра – динамическое преобразование подстановки (Т.Риттер);
- подход доказуемой безопасности, который основывается на предположении о наличии доступной всем большой строки случайных бит с произвольным доступом. Необходимый для этого открытый рандомизатор может быть физическим датчиком. Короткий секретный ключ используется для выделения подстрок длинной строки, которые затем используются для шифрования сообщения. По существу это направление является развитием давно известных "книжных" шифров.

Гомофоническая подстановка усложняет криптоанализ, основанный на простой статистике частотного распределения. Однако при малой мощности алфавита рандомизатора достаточное количество криптотекста может сделать успешным частотный анализ в совокупности с учетом дополнительных статистических свойств открытого текста переносимых в криптотекст.

Клод Шеннон определил криптосистему с бесконечным расстоянием единственности как идеально секретную. Если длина криптотекста менее

расстояния единственности, то даже при успешной атаке остается неопределенность, является ли восстановленный текст истинным. Поэтому желательно иметь расстояние единственности как можно большим.

При использовании в шифре рандомизатора с секретными параметрами выражения расстояние единственности ~ U можно определить как:

$$U = \frac{H(K) + H(R)}{D}, \quad (1.1)$$

где $H(R)$ – неопределенность параметров рандомизатора.

В таблице 1.1 приведены расстояния единственности для DES с 56-битовым ключом и AES со 128-битным ключом при использовании рандомизатора и различной $H(R)$, если языком исходного текста является английский.

Таблица 1.1

H(R), бит		0	100	1000	10000	100000
Uб бит	DES	65,6	183,5	1242	11830,5	117713
	AES	150,4	268,2	1327	11915	117797

Отсюда следует, что использование рандомизаторов позволяет увеличить ключевое поле и расстояние единственности, и улучшает характеристики шифра. В связи с вышесказанным представляет интерес ответить на вопрос, как влияют параметры рандомизатора на свойства шифра?

Можно предположить следующее:

- при устремлении мощности алфавита рандомизатора к бесконечности неопределенность рандомизированного текста также будет стремиться к бесконечности независимо от статистических свойств исходного текста;
- должна существовать ограниченная, достаточно большая мощность алфавита рандомизатора, при которой рандомизированный и исходный тексты становятся практически статистически независимыми;
- увеличение мощности поля рандомизации приведет к увеличению длины криптограммы по сравнению с исходным текстом.

В работе поставлены следующие задачи:

- теоретически исследовать влияние мощности алфавита рандомизатора на свойства криптографической системы;
- разработать методику синтеза рандомизаторов с алфавитом большой мощности;
- синтезировать и исследовать синтезированные рандомизаторы;

• на основе проведенного синтеза и исследования дать практические рекомендации по использованию таких рандомизаторов в практических системах.

Во **второй главе** рассмотрены принципы построения полных рандомизаторов с алфавитом большой мощности.

Под *полной рандомизацией* в дальнейшем будем понимать функцию отображения E из множества открытых текстов X_N в множество рандомизированных текстов Y_M, $M > N$ (M, N – мощности множеств открытых и рандомизированных текстов, соответственно), использующую элементы из пространства случайных чисел R_T, где Отображение $E: X_N \xrightarrow[k,r]{} Y_M$ такое, что для каждого ключа $k \in K$ и $r \in R$, $E(x,k,r)$ отображает $x \in X_N \to y \in Y_M$; и существует обратная функция, отображающая $Y_M \xrightarrow[k,r]{} X_N$. Причем, для каждого $x_i \in X_N$ существует множество образов $Y_{m_i} \in Y_M$, $m_i > 1$.

Совместная энтропия текста, зашифрованного с использованием эффекта рандомизации – $H(Y,X,K,R)$ определяется следующим образом:

$$H(Y,X,K,R) = H(X,K,R) + H(Y \mid X,K,R) = H(X,K,R) \qquad (2.1)$$

Если аргументы X, K, и R статистически независимы, то справедливо:

$$H(X,K,R) = H(X) + H(K) + H(R). \qquad (2.2)$$

Пусть L – мощность алфавита рандомизации, а $p(i)$ – вероятность появления i-го образа символа в рандомизированном тексте, в этом случае:

$$\lim_{\substack{L\to\infty \\ p\to 0}} H(R) = \lim_{\substack{L\to\infty \\ p\to 0}} \left(-\sum_{i=1}^{L} p(i) \times \log(p(i)) \right) = \lim_{L\to\infty} \left(-L \times \frac{1}{L} \times \log\left(\frac{1}{L}\right) \right) = \lim_{L\to\infty} (\log(L)) = \infty . \qquad (2.3)$$

Следовательно, при полной рандомизации с алфавитом $L \to \infty$ совместная энтропия зашифрованного текста становится бесконечной , что соответствует теоретически стойкой системе. Если мощность алфавита рандомизации не бесконечна, но достаточно велика, чтобы (2.1) имело бы тоже большую величину, то мы имеем достаточно близкое приближение к системе, в которой наблюдается статистическая независимость исходного и зашифрованного текстов [1,2,5].

Определение 1. *Пусть $T_0 \subset \{A\}$ – некоторый исходный текст, а K_I – операторы преобразования ($I \subset \{Q\}$). Тогда, если среди операторов K_I найдется хотя бы один, который бы переводил исходный текст в полностью рандомизированный, а последующие операторы не нарушают этого свойства, то цепочка операторов K_I является сохраняющей свойства полностью рандомизируемого текста.*

Теорема 1. *Реализация принципа полной рандомизации, при $L \to \infty$, в практически стойких системах шифрования переводит их в класс систем со статистической независимостью исходного текста и криптограммы.*

В работе дана оценка мощности, алфавита рандомизатора, позволяющая определить степень приближения к системе, обеспечивающей статистическую независимость исходного и зашифрованного текстов. Пусть:

m – количество одинаковых букв в исходном тексте;

распределение вероятностей образов буквы в рандомизированном тексте равномерно $P(i) = p = \frac{1}{L}$, $q = 1 - p$.

Тогда вероятность появления i – го образа буквы в рандомизированном тексте не более одного раза при $m << L$ найдем как:

$$P_{x \le 1} = q^m + mpq^{m-1} = \left(\frac{L-1}{L}\right)^m \left(1 + \frac{m}{L-1}\right) \approx \left(\frac{L-1}{L}\right)^m.$$

Отсюда для получения криптограммы статистически независимой от исходного текста с заданной вероятностью ρ при заданном числе повторяющихся букв в исходном тексте m требуется мощность поля рандомизации

$$L \approx \frac{1}{1 - \rho^{1/m}}.$$

При мощности алфавита рандомизации буквы исходного алфавита $L = 10^9$, а количестве одинаковых букв в исходном тексте $m = 10^5$, вероятность повторения i – го образа буквы в рандомизированном тексте не более одного раза составит

$P_{x \le 1} \approx \left(\frac{L-1}{L}\right)^m \approx 0{,}9999$, а при $m = 10^6$ $\quad P_{x \le 1} \approx 0{,}999$.

Таким образом, рандомизаторы с достаточно большой мощностью алфавита рандомизации могут быть мультиплексированы с практически стойкими, проверенными и сертифицированными криптографическими системами, обеспечивая приближение к статистической независимости криптограммы от исходного текста с заданной вероятностью.

Для решения задачи выполнения рандомизационного преобразования с большой мощностью алфавита $(L_i > 10^9)$, когда прямой перебор технически не рационален, предложен способ отождествления алфавита исходного текста алфавиту рандомизатора заключающийся в том, что для каждой буквы входного текста $a_i \in A$ генерируют псевдослучайное целое число x, вычисляют $E_x(a_i) = f_i(x)$, $x \in R$, $1 \le i \le N$, где $A\{a_1, a_2, ..., a_N\}$ – алфавит исходного текста, R – область определения функции f_i, причем $\forall\, i \ne j : f_i(x) \ne f_i(x)$.

Предложена комплексная система показателей криптосистем, характеризующей их защищенность от несанкционированного вскрытия криптоаналитиками и экономичность реализации, позволяющая оценить весомость операции рандомизации по сравнению с другими операциями криптопреобразования.

В **третьей главе** выполнены синтез и анализ криптографических преобразований типа MZ.

Пусть $A_n = \{a_1, ..., a_n\}$ – алфавит открытого текста и $B_n = \{b_1, ..., b_m\}$– алфавит криптотекста. Пусть $f_0, f_1, ..., f_n$ – целозначные функции определенные на множестве целых чисел $Z_{OS} = \{x \in Z \mid O < x \le S\}$. Далее функцию f_0 будем называть опорной. Каждую функцию $f_i, i = 1, ..., n$, взаимно однозначно соответствующую букве a_i, будем называть функцией преобразования, функцию w – результирующей функцией.

Под ***криптопреобразованием типа MZ*** будем понимать отображение $E : A_n \to B_m$ следующего вида: $E_{x x_0}(a_i) = w(f_i(x), f_0(x_0))$, где $w(i, x, x_0)$ – целозначное инъективное отображение, определенное на множестве $\{(i, x, x_0) \mid i \in \{1, ..., n\},\ x, x_0 \in Z,\ O < x, x_0 \le S\}$. Ключом преобразования является набор функций $f_0, f_1, ..., f_n$.

Определение криптопреобразования MZ может быть легко расширено в случае нескольких опорных функций как $E_{xy}(a_i) = w(f_i(x), f_{0i}(x_0))$.

На основе принципов построения полных рандомизаторов с алфавитом большой мощности можно предложить следующую методику синтеза такого рандомизатора:

- задание области определения функций преобразования $f_i(x)$ и опорных функций $f_{0i}(x_0)$, на множестве целых чисел Z_{OS} таких, что $Z_{OS} = \{x \in Z \mid O \le x \le S\}$;
- определение необходимого количества $f_i(x)$ и $f_{0i}(x_0)$;

- синтез функций преобразования $f_i(x)$;
- синтез опорных функций $f_{0i}(x_0)$;
- определение результирующей функции w;
- синтез генератора последовательности псевдослучайных чисел $x, x_0 \in Z_{OS}$.

Показано, что многообразие криптографических преобразований определяется выбором функций $f_i(x), f_{0i}(x_0)$ и $w(y, y_0)$, которые одновременно являются аналитическими ключами системы. Были предложены варианты таких функций, в соответствии с разработанной методикой синтезировано рандомизационное криптографическое преобразование MZ4 с использованием кусочно-линейных разрывных функций.

Все криптопреобразования MZ на основе кусочно-линейных разрывных функций можно разбить на классы MZ(n,S,δ,ρ,σ), где:

- n–мощность входного алфавита;
- S–мощность области определения функций преобразования;
- δ–количество абсцисс точек разрыва;
- ρ–количество опорных функций;
- σ–операция, определяющая результирующую функцию.

Теорема 2. *Кусочно-линейные разрывные преобразования из* MZ(n,S,δ,ρ,+) *разбиваются на классы эквивалентности, каждый из которых можно задать* 2(n+ρ)(δ+1)-1 *параметрами.*

Выполнен анализ упрощенного криптопреобразования MZ4 для случая, когда криптоаналитику известны подключи x, x_0. В этом случае справедлива следующая теорема.

Теорема 3. *Существует алгоритм криптоанализа преобразования MZ(n,S,δ,1,+), имеющий трудоемкость* $O(h^2t^2 + ht^3)$.

Полученные оценки позволяют сделать вывод о том, что стойкость шифра с использованием криптопреобразования MZ существенно зависит от механизма выборки подключей x, x_0 [4,5].

В криптопреобразовании MZ4 применен вариант механизма выборки подключей x, x_0, при использовании которого задача криптоанализа системы MZ является частным и сложным случаем известной NP-трудной задачи – системы нелинейных Диофантовых уравнений [4,5].

Ниже приведен алгоритм синтезированного криптопреобразования MZ4.

Системные параметры: Σ – алфавит исходного текста. $\Gamma = \{1,...,N-1\}$ – алфавит рандомизатора, $N \geq |\Sigma|$. Генератор псевдослучайных чисел (ПСЧ) генерирует значения в $I \subset N$. Инъективное отображение $B: \Gamma^* \to \{0,...,255\}$.

Ключ: параметры P генератора ПСЧ;

функции $f_\sigma : I \to \Gamma \; \forall \sigma \in \Sigma$, функция $g: I \to \Gamma$;

семейство перестановок Π которое для каждого текста длиной n определяет перестановку $\pi_n \in Sym_n$. Функции f_σ и g являются кусочно-линейными на семи отрезках. Функция g определена в ключе сортированными $x_i^{(g)} \in I, i = 1,...,6$ и семью парами $(a_i^{(g)}, b_i^{(g)}) \in I^2, \; i = 1,...,6$. $x_0^{(g)} = 0$ и $x_7^{(g)} = 2^{16}$,

$$g(x) = \sum \chi_{\left[x_i^{(g)}, x_{i+1}^{(g)}\right)}(x) * \left(a_i^g x + b_i^g\right), \; \chi_{\left[x_i^{(g)}, x_{i+1}^{(g)}\right)}(x) = \begin{cases} 1 \; if \; x \in \left[x_i^{(g)}, x_{i+1}^{(g)}\right| \\ 0 \; otherwise. \end{cases},$$

Все 256 функций f_σ определены аналогично g и так, что $\forall x \in I$ и $\forall \sigma_1 \neq \sigma_2 \in \Sigma$ справедливо $f_{\sigma 1}(x) \neq f_{\sigma 2}(x)$. Тогда $I \times \Sigma \to I \times \Gamma : (x, \sigma) \to (x, f_\sigma(x))$ является инъективным, что необходимо и достаточно для однозначного расшифрования. Таким образом, ключ состоит из $(P, \{f_\sigma : \sigma \in \Sigma\}, g, \Pi)$.

Зашифрование. Исходный текст: $m = (m_1,...,m_k) \in \Sigma^*$. Выбирается случайное $c_0' \in \Gamma$. Стартовым значением c_0' инициализируется генератор ПСЧ с ключевыми параметрами P. Пусть $r_1^{(1)}, r_1^{(2)}, r_2^{(1)}, r_2^{(2)}, ... \in I$. Положим $c' = (c_0', c_1', ..., c_k')$, при этом $c_i' = \left(f_{m_i}(r_i^1) + g_{m_i}(r_i^2)\right) \bmod N \; \forall i = 1,...,k$. В результате получаем байтовую строку $b = (b_1,...,b_n) = B(c')$. Криптотекст c получаем перестановкой байтов b согласно π_n: $c = (b_{\pi_n(1)},...,b_{\pi_n(n)})$.

Расшифрование. Шифротекст является байтовой строкой $c = (b_1',...,b_n')$. По ключу перестановкой инверсной π_n, восстанавливают байтовую строку:

$b = (b_1,...,b_n) = (b'_{\pi_n^{-1}(1)},...,b'_{\pi_n^{-1}(n)})$, где $b_i = b_{\pi_n(\pi_n^{-1}(i))} = b'_{\pi_n^{-1}(i)}$.

Пусть $c' = (c_0',...,c_k') = B^{-1}(b)$. Инициализируют генератор ПСЧ ключевым параметром P и стартовой величиной c_0'.

Пусть $r_1^{(1)}, r_1^{(2)}, r_2^{(1)}, r_2^{(2)}, ... \in I$ последовательность значений, выдаваемых генератором ПСЧ (Т.к. при зашифровании и расшифровании генератор ПСЧ инициализируется идентичными величинами, то генерируются одинаковые последовательности). Для всех $i = 1,...,k$ находятся методом проб $m_i \in \Sigma$ такие, что $f_{m_i}(r_i^{(1)}) = b_i - g(r_i^{(2)})$. Открытым текстом является $m = (m_1,...,m_k)$.

Выполнен анализ стойкости криптопреобразования MZ4, как наиболее перспективного с точки зрения практической реализации [2,4,5,7,8]. Выполненные атаки на криптопреобразование MZ4: на основе модели "двух миров", с

использованием выбранных криптотекстов, методом полного перебора, на основе аналитического подхода к задаче взлома алгоритма MZ4 позволяют сделать вывод о стойкости преобразования к проведенным атакам.

В таблице 3.1. приведены расстояния единственности для рандомизатора MZ4, DES, AES и комплексированных шифров в соответствии с выражением (1.1).

Таблица 3.1.

	DES	AES	MZ4	MZ4+DES	MZ4+AES
H(K)	56	128	115584	115640	115712
U	65,6	150,4	135981	136132	136132

Проведенные оценки показывают, что вклад в криптостойкость комплексированных систем предлагаемых рандомизаторов значительно превышает вклад традиционных систем, причем, с точки зрения быстродействия и увеличения длины криптограммы по сравнению с исходным текстом наиболее целесообразно в качестве функций преобразования использовать кусочно-линейные разрывные функции. Применение алгоритма MZ4 позволяет получить более высокое быстродействие по сравнению с алгоритмами DES, 3DES, IDEA, используемыми в режиме шифрования с простым вероятностным механизмом аналогичным по мощности MZ4.

Предлагаемое криптопреобразование MZ4 обладает дополнительно тем преимуществом, что позволяет в достаточно широком диапазоне изменять как количество, так и длину параметров функций преобразования, в зависимости от технического задания на проектируемую систему. Криптопреобразования типа MZ можно использовать для построения псевдовероятностных шифров. В этом случае параметры x, x_0 следует рассматривать как подключи. В зависимости от механизма выработки подключей можно строить как детерминированные, так и недетерминированные псевдовероятностные шифры.

В **четвертой главе** проведены статистические испытания и даны рекомендации по использованию системы MZ4.

Предложена модель для практической иллюстрации статистической независимости криптограммы MZ4 и исходного текста, основанная на парадоксе дня рождения. Была разработана специальная программа – полигон для проведения статистических испытаний. Проведенные статистические испытания продемонстрировали практическую статистическую независимость криптограммы, полученной в результате криптопреобразования MZ4, и исходного текста.

Аналогичные испытания криптограмм MZ4 дополнительно зашифрованных алгоритмом DES подтвердили теорему 1, практически доказав возможность комплексирования криптопреобразования MZ4 с другими криптоалгоритмами, при сохранении в этом случае основного свойства криптопреобразования MZ4 – статистической независимости получаемой криптограммы и исходного текста с заданной вероятностью.

Были предложены применения криптопреобразования MZ4 в комплексе с другими криптоалгоритмами [13] с целью повышения их криптографической стойкости [6]. Было показано, что наиболее целесообразно использовать криптопреобразование MZ4 для шифрования коротких сообщений, как это реализовано в криптоалгоритме MVZ в программном продукте – двухканальной телекоммуникационной системе MVZ messaging.

ЗАКЛЮЧЕНИЕ

1. В работе исследованы полные рандомизаторы с алфавитами большой мощности. Показано, что при использовании полной рандомизации с мощностью алфавита $L \to \infty$ энтропия зашифрованного текста становится бесконечной, что соответствует теоретически стойкой системе. Если мощность алфавита рандомизатора не бесконечна, но достаточно велика, то можно говорить о достаточно близком приближении к системе, в которой обеспечивается с заданной вероятностью статистическая независимость исходного и зашифрованного текстов [1,2,5,10].

2. Определены свойства таких рандомизаторов [1,10,11]: для одного и того же исходного текста зашифрованный текст в различных сеансах шифрования всякий раз является различным при неизменных параметрах рандомизатора; мощность множества зашифрованных текстов для одного и того же исходного при мощности множества кодов рандомизатора L и числе букв в тексте n оценивается числом L^n, что при достаточно больших L $\left(L > 10^9\right)$ делает практически невозможным частотный криптоанализ; в результате зашифрования образуется криптограмма, длина которой превышает длину исходного текста.

3. Выполнена численная оценка мощности алфавита рандомизатора, в зависимости от длины исходного текста, при которой с заданной вероятностью достигается статистическая независимость исходного текста и криптограммы [1,5]. Рандомизаторы, обладающие описанными свойствами, могут быть

мультиплексированы с другими криптографическими преобразованиями, значительно увеличивая расстояние единственности шифра.

4. Предложена методика синтеза полных рандомизаторов с алфавитом большой мощности [5]. В соответствии с предложенной методикой, выполнен синтез рандомизаторов на основе геометрического места точек и кусочно-линейных разрывных функций. Полученные оценки свидетельствуют о стойкости таких рандомизаторов к известным атакам [4,5,7,8].

5. Экспериментально подтверждены свойства рандомизаторов с большой мощностью алфавита рандомизации. Такие рандомизаторы могут использоваться в комплексе с другими криптоалгоритмами для повышения их стойкости. Наиболее целесообразно использовать синтезированные рандомизаторы для шифрования коротких сообщений в связи с увеличением длины рандомизированного текста по сравнению с исходным. Даны практические рекомендации по использованию синтезированных криптографических преобразований [3,5,6,14]. Реализован комплексный алгоритм, включающий синтезированный рандомизатор MZ4 в двухканальной телекоммуникационной системе *MVZ messaging* [3,14]. Новизна полученных результатов подтверждена патентами [9,10]

Список опубликованных работ

Статьи в журналах:

1. Захаров В.В. Синтез теоретически стойких криптографических систем// Вести Института современных знаний. – 1999. – №4. – С. 41–49.
2. Мищенко В.А., Захаров В.В. Теоретически стойкие системы кодирования класса MZ // Вести Института современных знаний. Специальный выпуск. – 2000. – №1. – С. 25–35.
3. Виланский Ю.В., Захаров В.В., Мищенко В.А. Система защищенного обмена сообщениями MVZ-messaging// Вести Института современных знаний. Специальный выпуск. – 2000. – №1. – С. 40–45.
4. Захаров В.В. Криптоанализ простейшего криптопреобразования типа MZ// Вести Института современных знаний. – 2001. – № 2. – С. 79–83.

Статьи в сборниках научных трудов:

5. Захаров В.В. Рандомизационные криптографические преобразования на основе разрывных функций //Современные информационные технологии: Сборник

научн.-технич. трудов Международная академия информатизации. – М., 2003. – Вып. 3. – С. 57–70.

Материалы докладов

6. Мищенко В.А., Захаров В.В. Теоретически стойкие системы кодирования информации и неподдельные электронные документы. Управление защитой информации – Минск – Москва, 1998. – Том 2. – № 1. – С. 29–30.
7. Захаров В.В. К вопросу о криптографической стойкости алгоритма MZ4// Вести Института современных знаний. Материалы научно-методической конференции "Наука и педагогика на рубеже XXI века". –2000. – № 3. – С. 10–12.
8. Захаров В.В., Виланский Ю.В. Атака на основе модели "двух миров" на криптопреобразование MZ4// Информационные системы и технологии (IST'2002): Материалы I Междунар. конф. (Минск, 5-8 ноября 2002 г.): ч.2. – Мн.: БГУ, 2002 – С. 51–55.

Тезисы докладов:

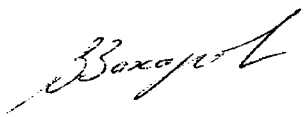
9. Захаров В.В., Рандомизационные преобразования с алфавитом большой мощности// Технические средства защиты информации: Тез. докл. научн. конф., Минск-Нарочь, 19-23 мая, 2003/ Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2003.– Т.1 №2/1 – С.19.

Патенты:

10. Mischenko V.A., Zakharau U.U. Пат. 6,301,361 США, МКИ H04K 001/00. Encoding and decoding information using randomization with an alphabet of high dimensionality. – № 271222; Заявл. 17.03.1999. – 29 с.
11. В.А.Мищенко, В.В. Захаров, Ю.В. Виланский, Д.И. Вержбалович. Пат. №003679 Евразийский, МКИ H04L9/06. Способ шифрования и дешифрования информации и устройство для его осуществления. – №200101127; Заявлено 27.04.1999; Опубл. 02.11.2000; Приоритет 27.04.1999. – 9 с.
12. Mischenko V.A., Zakharau U.U. Method and apparatus for encoding and decoding information. International Application Number: PCT/BY99/00004. International Publication Number: WO 00/56004. International Publication Date: 21.09.2000. Int. Filing Date: 27.04.1999. – 23 p.
13. Mischenko V.A., Zakharau U.U., Vilansky Y.V., Verzhbalovich D.I. Method for encrypting information and device for realization of the method. International Application Number: PCT/BY99/00005. International Publication Number: WO

00/65767. International Publication Date: 02.10.2000. Int. Filing Date: 16.3.1999. – 42 p.

14. Mischenko V.A., Zakharau U.U., Vilansky Y.V. Methods for encoding, decoding, transferring, storage and control of information, systems for carrying out the methods. PCT/BY99/00008. International Publication Number: WO 01/30017. International Publication Date: 26.4.2001. Int. Filing Date: 15.10.1999.– 105 p.



РЭЗЮМЭ

Захараў Уладзімір Уладзіміравіч

Сінтэз і даследаванне крыптаграфічных перавображанняў на падставе рандамізацыі з алфавітам вялікай магутнасці

Ключавыя словы: крыптаграфія, пераўтварэнне крыптаграфічнае, крыптаграфічная абарона даных, рандамізатар, статыстычная незалежнасць, стойкасць, сінтэз, кавалачна-лінейные разрыўныя функцыі.

Аб'ектам даследавання з'яўляюцца рандамізатары з алфавітам вялікай магутнасці. Прадмет даследавання – рандамізатары на падставе: а) геаметрычнага месца кропак; б) кавалачных разрыўных функцый.

Мэтай працы з'яўляецца павышэнне стойкасці крыптаграфічных алгарытмаў за кошт выкарыстання рандамізатараў з алфавітам вялікай магутнасці ў якасці дадатковага крыптаграфічнага пераўтварэння.

Мэтадалогія даследавання заснавана на: прапанове гіпотэзы аб магчымасці сінтэзу рандамізатараў з канчатковым алфавітам рандамізацыі, які забяспечвае атрыманне крыптаграм статыстычна незалежных ад зыходнага тэксту с заданаю імавернасцю; атрыманні адзнакі патрабуемай магутнасці алфавіта; сінтэзе і аналізе такіх рандамізатараў; праграмнай рэалізацыі алгарытма рандамізацыі і эксперыментальным доказе уласцівасцей сінтэзаваных рандамізатараў.

Атрыманыя вынікі і іх навізна заключаюцца ў: выкананні ацэнкі магутнасці алфавіту рандамізатара, пры якой з зададзенаю імавернасцю дасягаецца статыстычная незалежнасць крыптаграмы і зыходнага тэксту; аб'яднанні такіх рандамізатараў з практычна стойкімі крыптапераўтварэннямі, што прыводзіць да аналагічнага эффекту ў аб'яднанай сістэме; у прапанове методыкі сінтэзу крыптапераўтварэння на падставе цэлалікавых кавалачных разрыўных функцый; атрыманні ацэнкі стойкасці сінтэзіраваных рандамізатараў.

Алгарытм сінтэзіраванага рандамізатару выкарыстаны ў праграмным прадукце SolanioE-Mail, які забяспечвае функцыяванне абароненай электроннай пошты, камерцыйных вырабах: MZ4; Label; WEB.

Вобласцю прымянення атрыманых вынікаў з'яўляецца крыптаграфічная абарона даных у кампутарах, кампутарных сецях і сецях перадачы даных.

РЕЗЮМЕ

Захаров Владимир Владимирович

Синтез и исследование криптографических преобразований на основе рандомизации с алфавитом большой мощности

Ключевые слова: криптография, преобразование криптографическое, криптографическая защита данных, рандомизатор, статистическая независимость, стойкость, синтез, кусочно-линейные разрывные функции.

Объектом исследования являются рандомизаторы с алфавитом большой мощности. Предмет исследования – рандомизаторы на основе: а) геометрического места точек; б) кусочных разрывных функций.

Целью работы является повышение стойкости криптографических алгоритмов за счет использования рандомизаторов с алфавитом большой мощности в качестве дополнительного криптографического преобразования.

Методология исследования основана на: гипотезе о возможности синтеза рандомизаторов с конечным алфавитом, обеспечивающим получение криптограмм статистически независимых от исходного текста с заданной вероятностью; оценке требуемой мощности алфавита; синтезе и анализе таких рандомизаторов; программной реализации алгоритма рандомизации и экспериментальном доказательстве свойств синтезированных рандомизаторов.

Полученные результаты и их новизна заключаются в: оценке мощности алфавита рандомизатора, обеспечивающей с заданной вероятностью статистическую независимость криптограммы и исходного текста; комплексировании таких рандомизаторов с практически стойкими криптопреобразованиями, что приводит к аналогичному эффекту в объединенной системе; в разработке методики синтеза криптопреобразования на основе целочисленных кусочных разрывных функций; оценке стойкости синтезированных рандомизаторов.

Алгоритм синтезированного рандомизатора использован в программном продукте SolanioE-Mail, обеспечивающем функционирование защищенной электронной почты, коммерческих продуктах: MZ4; Label; WEB. Областью применения полученных результатов является криптографическая защита данных в компьютерах, компьютерных сетях и сетях передачи данных.

THE SUMMARY

Zakharov Vladimir Vladimirovitch

Synthesis and research of cryptographic transformations based on randomization with the large cardinality of alphabet

Key words: cryptography, cryptographic transformation, cryptographic protection of data, randomizer, statistical independence, resistance, synthesis, piecewise linear discontinuous functions.

Researched objects: randomizers with high-capacity alphabets. The research's subject is randomizers on the basis of: a) a geometrical place of points; б) piecewise discontinuous functions.

The purpose of the work is increase of security of cryptographic algorithms by use of randomizers with high-capacity alphabets playing the role of additional cryptographic transformations.

The methodology of research is based on the following: a proposed hypothesis of possible synthesis of randomizers with the finite randomization alphabet ensuring generation of cryptograms that would be statistically independent from the initial text with the desired probability; estimation of the required alphabet capacity; synthesis and analysis of such randomizers; software realization of the randomization algorithm and experimental proof of synthesized randomizers properties.

The results received and their novelty consist of the following: estimation of capacity of the randomizer alphabet at which statistical independence of a cryptogram and initial text is achieved with the desired probability; integration of such randomizers with practically resistant cryptographic transformations leading to the similar effect in the joint system; offer of a method of cryptographic transformation synthesis based on piecewise discontinuous functions; estimation of security of synthesized randomizers.

The algorithm of synthesized randomizer is used in the software product SolanioE-Mail ensuring functioning of protected electronic mail system of MMPP "Salut" (Moscow), GVC "Intourist" (Moscow); several commercial products of the Hermelin company (Germany) and UP "Creative Laboratory" (Minsk) - MZ4, E-Mail, Label, WEB.

Application area of the received results is cryptographic protection of data in computers, computer networks and networks of data transfer.

ЗАХАРОВ Владимир Владимирович

СИНТЕЗ И ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ НА ОСНОВЕ РАНДОМИЗАЦИИ С АЛФАВИТОМ БОЛЬШОЙ МОЩНОСТИ

Специальность 05.13.17 – Теоретические основы информатики

Автореферат диссертации

на соискание ученой степени кандидата технических наук

Подписано в печать	25.02.2004.	Формат 60x84 1/16.
Бумага офсетная.	Печать ризографическая.	Усл. печ.л. 1,63.
Уч. – изд. л. 1,2.	Тираж 80 экз.	Заказ 92.

Издатель и полиграфическое исполнение:
Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия ЛВ №509 от 03.08.2001. Лицензия ЛП №156 от 30.12.2002.
220013, Минск, П. Бровки, 6.