Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 681.3.006

АБДОЛЬВАНД
Фарид

ОТКРЫТОЕ ФОРМИРОВАНИЕ КОНФИДЕНЦИАЛЬНЫХ ИДЕНТИЧНЫХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск 2012

Работа выполнена в Белорусском национальном техническом университете.

Научный руководитель	**Голиков Владимир Фёдорович**, доктор технических наук, профессор, заведующий кафедрой «Информационные технологии в управлении» Белорусского национального технического университета
	Мищенко Валентин Александрович, доктор технических наук, профессор, проректор по научной работе частного учреждения образования «Институт современных знаний»; **Соломатин Сергей Борисович**, кандидат технических наук, доцент, доцент кафедры радиотехнических систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».
Оппонирующая организация	Учреждение образования «Белорусский государственный технологический университет»

Защита состоится 22 марта 2012 г. в 14.00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232-1, тел. (8-017) 293-89-89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования

КРАТКОЕ ВВЕДЕНИЕ

Современные информационные технологии позволяют решать большое количество задач во всех сферах человеческой деятельности. Телекоммуникационные системы обеспечивают интенсивный обмен информацией огромного числа людей и организаций. Однако многопользовательский характер современных информационных сетей наряду с теми благами, которые он несет участникам информационного обмена, является предпосылкой к возможным злоупотреблениям по отношению к частной информации.

В связи с этим возникла потребность в защите информационных ресурсов от нарушения их конфиденциальности, целостности, доступности, авторских прав и т.д. Эти задачи решаются в настоящее время методами и средствами защиты информации. В защите информации, циркулирующей в компьютерных сетях, локальных и глобальных, важную роль играют криптографические методы. Современные криптосистемы строятся таким образом, что их надежность обеспечивается стойкими криптографическими алгоритмами, взлом которых без знания секретных параметров, называемых ключевой информацией, даже с использованием самых передовых математических методов и мощных компьютеров невозможен за обозримое человеком время. Однако в условиях удаленных сеансов связи с использованием открытых электронных каналов с учетом территориальной рассосредоточенности и высокой мобильности абонентов возникает задача конфиденциальной доставки ключевой информации.

Эта задача в настоящее время решается методами асимметричной криптографии, в основе которой лежит использование односторонних функций. Несмотря на внешнее благополучие асимметричной криптографии, развитие математической науки и компьютерной техники вносит существенные коррективы в ее параметры. В последние годы во многих развитых странах ведутся интенсивные работы по созданию квантовых компьютеров, а математиками разработаны эффективные алгоритмы решения обратных задач на базе этих компьютеров. Это потенциально ставит под сомнение безопасность всей асимметричной криптографии. В связи с этим в настоящее время появился ряд работ, направленных на решение задач доставки ключевой информации абонентам сети без использования классических односторонних функций. Наиболее известным и успешным продвижением в этом направлении можно считать метод, использующий синхронизированные искусственные нейронные сети, а также метод передачи ключевой информации по квантовому каналу.

В диссертационной работе предлагается новое решение задачи формирования ключевой информации у абонентов сети, использующее оригинальный подход к формированию исходных ключевых последовательностей с их последующим итерационным согласованием.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Работа выполнялась в рамках НИР ГБ 06-211 «Программное и информационное обеспечение дистанционного обучения» на кафедре информационных технологий в управлении Белорусского государственного технического университета, а также ГБ 11-2022 «Разработка средств защиты информации от утечки по техническим каналам» на кафедре защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Цель и задачи исследований

Целью диссертационной работы является разработка метода формирования идентичных бинарных последовательностей у абонентов сети для использования их в качестве ключевой информации в алгоритмах аутентификации или шифрования. При этом в системе не должны использоваться процедуры, криптостойкость которых основывается на математической или вычислительной сложности решения какой-либо задачи.

Для достижения поставленных целей необходимо было решить следующие задачи:

1) проанализировать современные методы распределения ключевой информации в компьютерных сетях и выявить общие закономерности используемых процедур;

2) разработать обобщенную модель формирования идентичных бинарных последовательностей у абонентов сети;

3) разработать метод формирования идентичных бинарных последовательностей у абонентов сети для использования их в качестве ключевой информации в алгоритмах аутентификации или шифрования;

4) разработать программный комплекс для моделирования и экспериментального определения параметров метода формирования идентичных бинарных последовательностей.

Объект исследования – закономерности формирования ключевой информации (КИ) в компьютерных сетях.

Предмет – способ формирования идентичных бинарных последовательностей (ИБП) у абонентов сети без использования односторонних функций.

Положения, выносимые на защиту

1. Обобщенная модель открытого формирования идентичных бинарных последовательностей, основанная на выявленных закономерностях известных способов, представляющая этот процесс как последовательность выполнения определенных действий, присущих этим способам, несмотря на их внешние различия.

2. Метод открытого формирования идентичных бинарных последовательностей, включающий генерацию бинарных последовательностей с управляемым уровнем несовпадений и конфиденциальности битов, отыскание и устранение несовпадающих битов в сформированной слабосовпадающей последовательности, усиление конфиденциальности итоговой последовательности до приемлемого уровня, позволяющий сравнительно просто и без использования односторонних функций решать задачу распределения ключевой информации.

3. Модифицированный итерационный метод отыскания и устранения несовпадающих битов в согласовываемых слабосовпадающих бинарных последовательностях, позволяющий эффективно устранять ошибки при проценте несовпадений, близком к 50, основанный на сравнении четностей пар битов, выбранных случайно и согласованно в обеих последовательностях, с последующим удалением пар, содержащих одно несовпадение, а также согласованным удалением по одному биту из каждой оставляемой пары, причем для первой итерации этот бит может выбираться каждым абонентом случайно, что обеспечивает повышение неопределенности итоговой согласованной последовательности.

4. Компьютерная имитационная модель взаимодействия абонентов при формировании ключевой информации в соответствии с разработанным методом, позволяющая экспериментально выбирать параметры используемых процедур и оценить работоспособность и эффективность предложенных решений.

Личный вклад соискателя

Все основные результаты, изложенные в диссертации, получены автором самостоятельно. В публикациях с соавторами вклад соискателя определяется рамками представленных в диссертации результатов.

Апробация результатов диссертации

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: Вторая научная конференция иранских студентов, проживающих в Беларуси (г. Минск, 2009 г.),

VII Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (г. Минск, 2009 г.), XIV международная конференция «Комплексная защита информации» (г. Могилев, 2009 г.), 7-я Международная научно-техническая конференция «Наука – образованию, производству, экономике» (г. Минск, 2009 г.), VIII Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (г. Минск, 2010 г.), 8-я Международная научно-техническая конференция «Наука – образованию, производству, экономике» (г. Минск, 2010 г.), VI Международная научная конференция «Информационные системы и технологии» (г. Минск, 2010 г.), XVI научно-практическая конференция «Комплексная защита информации» (г. Гродно, 2011 г.).

Опубликованность результатов диссертации

По результатам исследований, изложенных в диссертации, опубликовано 13 печатных работ, в том числе 3 статьи в рецензируемых журналах из списка ВАК, 3 статьи в сборниках материалов конференций и 7 тезисов докладов конференций. Общий объем публикаций по теме диссертации, соответствующих пункту 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, составляет 2,5 авторских листа.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики, четырех глав, заключения, библиографического списка и приложений. В первой главе рассмотрены роль и значение ключевой информации в криптографических системах защиты информации. Проведен сравнительный анализ известных способов распределения ключевой информации. Во второй главе показано, что несмотря на внешние различия проанализированных способов распределения ключевой информации, им присущи общие закономерности. Разработана обобщённая модель конфиденциального формирования идентичных бинарных последовательностей. В третьей главе разработан метод формирования идентичных бинарных последовательностей без использования односторонних функций, включающий генерацию бинарных последовательностей с управляемым уровнем несовпадений и конфиденциальности битов, устранение несовпадающих битов в сформированных слабосовпадающих последовательностях, усиление конфиденциальности итоговой последовательности до приемлемого уровня. В четвертой главе описывается компьютерная имитационная модель взаимодействия абонентов при формировании ключевой информации, созданная в соответствии с разработанным методом.

Общий объем диссертационной работы составляет 111 страниц, из них 71 страницы основного текста, 44 иллюстрации на 33 страницах, 7 таблиц на 4 страницах, 2 приложения на 17 страницах, библиографический список из 40 наименований на 3 страницах и список работ соискателя из 13 наименований на 2 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** показана актуальность темы, обоснована необходимость решения задачи формирования ключевой информации у абонентов сети, использующая оригинальный подход к формированию исходных ключевых последовательностей с их последующим итерационным согласованием.

В **первой главе** рассматривается современное состояние изучаемого вопроса, определяется место и роль ключевой информации в криптографических системах защиты информации. Проводится сравнительный анализ способов распределении ключевой информации в современных криптосистемах.

Высокая криптостойкость современных криптографических систем базируется на надежности, используемых несекретных алгоритмов и секретности ключей. Под криптостойкостью системы понимают ее способность противостоять криптоанализу. Ключевая информация (ключ) – некоторые параметры криптографического преобразования, определяющие выбор конкретной операции из множества допустимых. В компьютерной криптографии под ключевой информацией понимается некоторое число в двоичной или иной форме исчисления. Это число должно быть случайным и секретным. Процесс распределения ключевой информации должен обеспечивать ее максимальную конфиденциальность. Согласно существующей в криптографии терминологии под распределением понимается доставка готовой ключевой информации или ее формирование у абонентов системы.

Для обеспечения коммуникаций большого количества абонентов, размещенных в произвольных точках пространства, для распределения ключевой информации приходится использовать открытые каналы связи, обеспечивая при этом необходимую конфиденциальность.

Наиболее распространенными способами формирования общей конфиденциальной ключевой информации у различных абонентов, имеющих открытые каналы связи, являются способы, использующие специальные математические функции, получившие в криптографии следующее название – односторонние или однонаправленные функции. Из них чаще всего используется способ, предложенный Диффи – Хеллманом. Безопасность способа обусловлена трудностью вычисления дискретных логарифмов в конечном поле, в отличие от легкости дискретного возведения в степень в том же конечном поле.

Однако для всех алгоритмов, в том числе и Диффи – Хеллмана, основанных на использовании односторонних функций, несмотря на то, что они обеспечивают достаточно высокое быстродействие, высокую конфиденциальность, присущ ряд недостатков.

Во-первых, они требуют большой подготовительной работы и сложны в реализации. Действительно, асимметричная криптография использует очень большие числа, размер которых составляет сотни десятичных разрядов. Причем по мере развития математических методов решения обратных задач и производительности компьютерной техники размер этих чисел систематически нарастает. Это требует больших временных и материальных ресурсов на подготовку к генерации ключей. Во-вторых, конфиденциальность КИ, распределяемой методами, базирующимися на односторонних функциях, зависит от уровня развития компьютерной техники и успехов математических методов в области теории чисел. Так, в настоящее время разработаны эффективные алгоритмы решения обратных задач с использованием квантового компьютера, позволяющие решать эти задачи практически мгновенно. И хотя такого компьютера еще нет, тем не менее, работы по его созданию ведутся во многих странах.

Квантовое распределение ключей – это технология, позволяющая создать у двух удаленных пользователей строку случайных битов, которая может использоваться в качестве криптографического ключа. Квантовое распределение ключей основывается на квантовом эффекте, который заключается в невозможности измерить состояние одиночного фотона света, не нарушив его состояние, в то время как электрические сигналы можно копировать неограниченное число раз, совершенно незаметно для отправителя и получателя. Квантовый способ формирования КИ длительное время рассматривался как альтернатива способам, основанным на использовании однонаправленных функций. Однако, несмотря на теоретическую привлекательность, обеспечивающую достаточную конфиденциальность, практического распространения эта технология до сих пор не получила. Причиной этого являются нерешенные проблемы технологического характера: ненадежное генерирование одиночных фотонов; большое количество ложных регистраций в приемных устройствах, малая дальность передачи оптических сигналов, сложность и высокая стоимость используемого оборудования. Кроме того, имеются трудности системного характера – проблемы встраивания квантовых каналов в компьютерные сети; невозможность использования технологии в условиях прослушивания квантового канала.

Попытка решить задачу распределения ключей без использования классических односторонних функций привела к разработке технологии синхронизируемых искусственных нейронных сетей.

Абоненты A и B имеют одинаковые ИНС, отличающиеся только значениями вектора весовых коэффициентов персептронов. На их входы подается

один и тот же случайный вектор, вычисляются выходные векторы сетей, сравниваются между собой, корректируются значения вектора весовых коэффициентов персептронов сетей. Затем изменяют входной вектор и проводят следующий сеанс синхронизации с последующей коррекцией векторов весовых коэффициентов персептронов. При многократном повторении сеансов синхронизации значения векторов весовых коэффициентов персептронов сетей становятся одинаковыми, т.е. происходит синхронизация сетей. Если начальные значения векторов весовых коэффициентов персептронов сетей сделать секретными, то итоговые значения, равные в обеих сетях, можно использовать в качестве общего криптографического ключа. Однако есть опасность, что. криптоаналитик, наблюдающий за процессом обмена и синхронизирующий свою сеть с одной из синхронизируемых сетей, может получить вектор весов своей сети, равный итоговому значению векторов сетей A и B. Также для полной синхронизации требуется большое число итераций (сотни, тысячи).

Целью диссертации является разработка метода формирования ИБП у абонентов сети для использования их в качестве ключевой информации. Метод должен использовать открытый электронный канал связи, не использовать односторонние функции, количество сеансов связи должно быть минимально возможным, метод должен работать в стандартных компьютерных сетях.

Во **второй главе** разработана обобщённая модель конфиденциального формирования идентичных бинарных последовательностей.

Рассмотрены закономерности процесса формирования общего ключа. Показано, что несмотря на внешние различия проанализированных способов распределения КИ им присущи некоторые общие закономерности, заключающиеся в формировании секретных индивидуальных исходных чисел (последовательностей), с некоторой долей подобия; устранении различий путем обмена информацией об ошибках по открытом каналу связи.

В соответствии с выявленными закономерностями обобщенная модель формирования идентичных бинарных последовательностей (ИБП) должна отражать следующие функции: генерацию индивидуальной секретной информации, удовлетворяющую определенным требованиям; генерацию открытой информации для абонентов системы, обеспечивающую процесс формирования ИБП; алгоритм формирования открытой информации обмена, с помощью которого осуществляется процесс формирования ИБП; протокол взаимодействия перечисленных выше процедур. Данная модель изображена на рисунке 1.

Наиболее очевидной процедурой, реализующей необходимые функции обобщенной модели и соответствующей сформулированным ограничениям, представляется следующая последовательность действий.

Величины Y_i^A, Y_i^B вычисляются синхронно с использованием синхронизируемых последовательностей чисел S_i и текущих значений согласуемых БП

X_i^A, X_i^B. Процесс устранения ошибок итерационный. Процедура должна заканчиваться анализом конфиденциальности ИБП с возможной коррекцией результата.

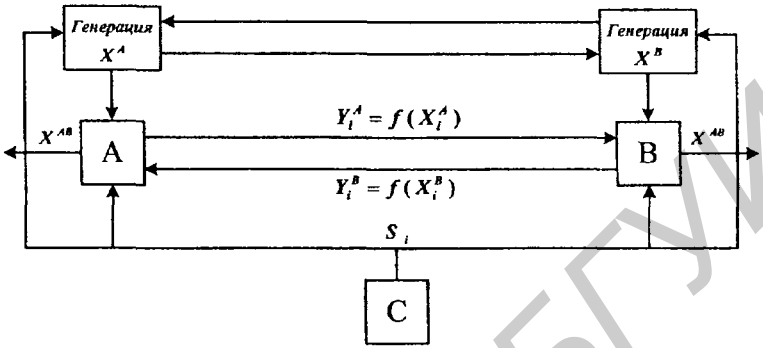

Рисунок 1 – Модель формирования ИБП

При формировании требований к разрабатываемым процедурам будем учитывать опыт построения аналогичных процедур в известных методах формирования ИБП.

Предположим, что на первом этапе мы генерируем исходные БП X^A и X^B с долей ошибок e. Данные ошибки следует устранить на втором этапе. Так как устранение ошибок должно осуществляться с минимально возможными потерями конфиденциальности согласуемых БП, то следует ожидать, что с ростом e будут возрастать потери конфиденциальности, т.е. существуют серьезные ограничения на величину e. Согласно теореме о кодировании Шеннона применительно к рассматриваемой задаче соотношение, позволяющее оценить средние потери конфиденциальности в битах при устранении ошибок потенциально наилучшим способом, имеет вид:

$$r = -n[e\log_2 e + (1-e)\log_2(1-e)], \qquad (1)$$

где r – число разглашаемых битов (потерянных); n – длина согласуемых БП в битах; e – доля ошибок $e = d/n$; d – число несовпадающих битов.

Зависимость r/n от e приведена на рисунке 2. Таким образом:

– генерация БП X^A и X^B должна осуществляться таким образом, чтобы доля ошибок $e \neq 0,5$, т.е. должно выполняться либо $e < 0,5$, либо $e > 0,5$;

– при доле ошибок $e \approx 0,5$ длина исходных БП X^A и X^B должна выбираться с большим запасом, т.к. при устранении ошибок произойдет существенное ее уменьшение;

– метод обеспечения требуемой конфиденциальности должен либо гарантировать требуемый уровень, либо, если это окажется невозможным, однозначно оценивать достигнутый уровень.

В анализируемых ранее методах наиболее проработанным является задача удаления ошибок в согласуемых последовательностях, полученных с использованием квантового канала. Задача формирования исходных конфиденциальных БП с определенным уровнем подобия является новой и требует детальной проработки.

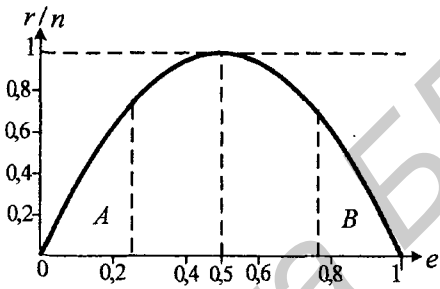

Рисунок 2 – Потери при устранении ошибок

Третья глава посвящена разработке способа формирования идентичных бинарных последовательностей без использования односторонних функций.

Устранение ошибок в слабосовпадающих бинарных последовательностях. Рассматривается задача согласования двух БП. Эта задача формулируется следующим образом. Пусть абоненты A и B некоторым образом сформировали у себя секретные БП, соответственно X^A и X^B, где $X^A = \{0,1\}^n$, $X^B = \{0,1\}^n$, где n – длина последовательности в битах. Последовательности X^A и X^B имеют d несовпадающих битов, $0 \le d \le n$. Процесс согласования X^A и X^B сводится к устранению несовпадающих битов последовательностей. Поскольку открытый канал связи потенциально прослушивается криптоаналитиком, то передаваемая по этому каналу информация по возможности не должна снижать конфиденциальность битов, остающихся в согласуемых последовательностях, больше чем допустимо.

Показано, что известные методы устранения несовпадающих битов в согласовываемых БП, такие как метод половинного разбиения, метод вероятностного разбиения, ориентированные на относительно небольшую долю несовпадений (до 0,25), не содержат четких рекомендаций о согласовании слабосовпадающих БП, которыми нам придется оперировать в силу выбранной стратегии.

Взяв за основу метод вероятностного разбиения, получили, что оптимальная длина фрагментов, на которые следует разбивать БП для поиска ошибок,

равна

$$L_{opt} = -\frac{1}{\ln(1-P_0)}, \qquad (2)$$

где $P_0 = \frac{d}{n}$.

Зависимость L_{opt} от P_0 изображена на рисунке 3.

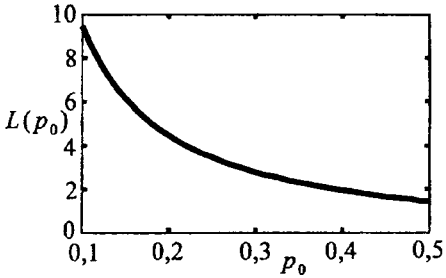

Рисунок 3 – Зависимость длины фрагмента от доли ошибок

Из неё следует, что для слабосовпадающих БП ($e > 0{,}25$) последовательности следует разбивать на пары битов. Исследованы статистические закономерности образования пар с точки зрения содержания в них ошибок. Для этого введено понятие общая виртуальная бинарных последовательностей W^{AB}. Общая виртуальная БП W^{AB} получается путем поразрядного сложения по $mod\,2$ X^A и X^B, т.е. $W^{AB} = X^A \oplus X^B$, что означает $w_i = a_i \oplus b_i$, $i = \overline{1, n}$. Несложно видеть, что если $a_i = b_i$, то $w_i = 0$, в противном случае $w_i = 1$, т.е. на месте несовпадающих битов в X^A и X^B в общей виртуальной БП стоят единицы, на месте совпадающих – нули. Очевидно, что $\sum_{i=1}^{n} w_i = d$. Введение понятия общая виртуальная БП не влияет на процедуру устранения ошибок, а лишь упрощает описание и исследование свойств согласовываемых БП.

Каждая пара битов может содержать следующие комбинации битов: (0,0) – оба бита правильные, (1,0 или 0,1) – один бит правильный, один ошибочный, (1,1) – оба бита ошибочные. Очевидно, что количество сформированных пар каждого типа величина случайная, обозначим: m_0 – количество пар типа (0,0); m_1 – количества пар типа (0,1) и (1,0); m_2 - количество пар типа (1,1). Очевидно, что

$$\begin{aligned} m_0 + m_1 + m_2 &= n/2, \\ m_1 + 2\,m_2 &= d. \end{aligned} \qquad (3)$$

Определен закон распределения вероятностей системы случайных величин: m_0, m_1, m_2:

$$P(i, j, u) = \frac{(n/2)!}{i!\,j!\,u!} P_0^i\, P_1^j\, P_2^u \qquad (4)$$

и математические ожидания этих величин. Показано, что $M(m_0)$, $M(m_1)$, $M(m_2)$ зависит от d/n (рисунок 4). Установлено, что число пар с одной ошибкой преобладает в диапазоне $0{,}35 < e < 0{,}5$. С учетом этого разработан метод устранения ошибок в слабосовпадающих бинарных последовательностях.

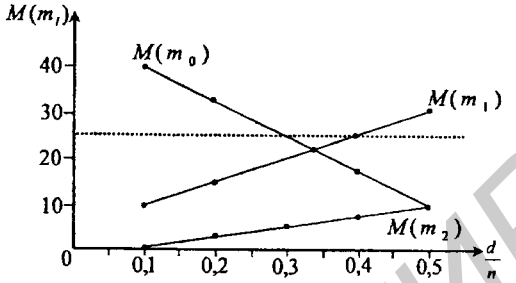

Рисунок 4 – Изменение количества пар

Основная идея метода [2–А] заключается в том, чтобы разбив X^A и X^B согласованно на пары, следует обнаруживать пары, содержащие одну ошибку, и удалять эти пары, оставляя пары без ошибок или с двумя ошибками. Оставшиеся биты необходимо снова согласовать: перемешать и образовать новые пары битов, из которых следует вновь удалить пары с одной ошибкой. Процедура повторяется до тех пор, пока все ошибочные биты не будут удалены.

Для обнаружения пар, содержащих одну ошибку, в качестве критерия обнаружения ошибок используется неравенство четностей соответствующих пар последовательностей X^A и X^B: если $C_A^{(i)} \neq C_B^{(i)}$, то в паре битов содержится одна ошибка, если $C_A^{(i)} = C_B^{(i)}$, то в паре битов содержится 0 или 2 ошибки. Здесь $C_A^{(i)} = a_j \oplus a_{j+1}$, $C_B^{(i)} = b_j \oplus b_{j+1}$. Для определения числа необходимых итераций проанализирована динамика изменения доли ошибок от числа итераций, что позволило прогнозировать число итераций при известной доле ошибок.

Предложенный способ позволяет согласовывать последовательности с долей ошибок, близкой к предельной (в соответствии с ограничением Шеннона), однако при этом длина итоговой последовательности существенно сокращается относительно исходной.

Формирование исходных бинарных последовательностей с управляемым уровнем ошибок и конфиденциальности. Согласно разработанной общей модели формирования КИ и схемы её реализации, абоненты A и B должны сформировать каждый у себя исходную бинарную последовательность X^A (X^B), которая должна быть случайной и конфиденциальной, иметь необходимую длину с учетом её уменьшения в процессе согласования. Процент несовпадающих битов должен позволять согласовывать последовательности. Устранение ошибок возможно, если доля ошибок в последовательностях $e < 0{,}5$ или $e > 0{,}5$, но какой случай имеет место, должно быть известно достоверно.

Проведено исследование статистических свойств бинарных последовательностей, сформированных независимо друг от друга. Установлено, что две БП, сформированные независимо друг от друга, не могут быть согласованны с

заданной вероятностью. Значит, их следует формировать с определенной долей зависимости. Предложен способ формирования исходных последовательностей с $e < 0,5$. Его суть заключается в следующем.

Абонент A генерирует базовую бинарную последовательность X_0 длиной n и посылает ее абоненту B. Затем абоненты A и B независимо друг от друга задаются количеством изменяемых битов r_A, r_B, где $0 \le r_A \le n, 0 \le r_B \le n$ и генерируют независимо друг от друга случайные секретные последовательности чисел соответственно S_A и S_B, при этом $S_A = \{s_1^a, s_2^a, ..., s_{r_a}^a\}$, $S_B = \{s_1^b, s_2^b, ..., s_{r_b}^b\}$, где $S_i^a \in \{1,2,...,n\}$, $S_i^b \in \{1,2,...,n\}$, причем $s_i^a \ne s_j^a$, $i, j = 1,2, ..., r_A$ для S_A, $s_i^b \ne s_j^b$, $i, j = 1,2, ..., r_B$ для S_B. Абоненты A и B в соответствии с полученными номерами битов S_i^a и S_i^b инвертируют эти биты в X_0 и получают БП X^A и X^B, обладающие следующими свойствами:

– в последовательностях X^A и X^B имеется n_C совпадающих и n_H несовпадающих битов;

– наличие совпадающих битов обусловлено: для части битов взаимным инвертированием в X^A и X^B, для части – взаимным неинвертированием;

– наличие несовпадающих битов обусловлено для части битов инвертированием в X^A и неинвертированием в X^B и наоборот.

Тогда из рисунка 5 следует, что общее число совпадающих битов равно

$$n_C = n - (r_A + r_B) + 2n_{ИС}, \tag{5}$$

где $n_{ИС}$, $n_{НИС}$ – число взаимно инвертированных и неинвертированных совпадающих битов соответственно, причем $n_C = n_{ИС} + n_{НИС}$, а число несовпадающих битов равно

$$n_H = (r_A + r_B) - 2n_{ИС}. \tag{6}$$

Доля несовпадающих битов в БП X^A и X^B будет равна

$$e_H = \frac{n_H}{n} = \frac{r_A + r_B - 2n_{ИС}}{2}. \tag{7}$$

$n_C, n_H, n_{ИС}, e_{НИС}$ являются случайными величинами и зависят от r_A, r_B.

Выберем значения r_A, r_B такими, чтобы выполнилось $e_H < 0,5$, или

$$P(e_H < 0,5) = P\left(\frac{r_A + r_B - 2n_{ИС}}{n} < 0,5\right) \ge \alpha, \tag{8}$$

где α – вероятность, близкая к 1, или

$$P(n_{ИС} > \frac{r_A + r_B}{2} - \frac{n}{4}) \geq \alpha . \qquad (9)$$

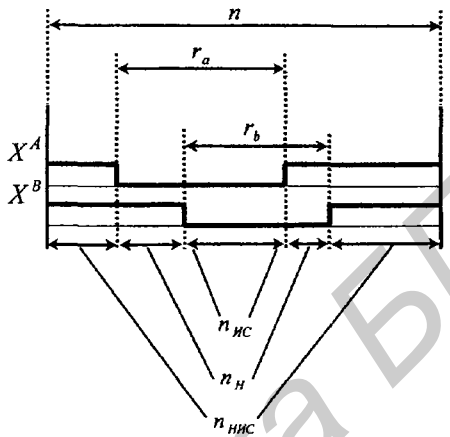

Рисунок 5 – Структура сравниваемых последовательностей после инвертирования

С другой стороны, необходимо обеспечить максимально возможную конфиденциальность формируемых последовательностей. Показано, что это обеспечивается при $n_{ИС} = n_{НИС}$. Последнее равенство выполняется только при $r_A + r_B = n$, но тогда не выполняется $e_H < 0,5$. Поэтому параметры r_A, r_B должны определяться компромиссно с учетом указанных условий.

Предложена методика численного решения этой задачи для общего случая. Для последовательностей большой длины получены аналитические решения:

$$r_A = \frac{e_H\, n^2 - n\, r_B}{n - 2 r_B}, \qquad (10)$$

$$r_B = \frac{n}{2}[2 e_{ИС} + e_H - 2\, e_{ИС} \cdot e_H \pm \sqrt{(2 e_{ИС} + e_H - 2\, e_{ИС} \cdot e_H)^2 - 4\, e_{ИС}(1 - e_H)}]. \qquad (11)$$

Например, для $n = 100000, e_H = 0,486, e_{ИС} = 0,33$ получаем: $r_A = 43800$, $r_B = 38700$ или $r_A = 38700, r_B = 43800$. Наличие двух решений обусловлено симметрией пары значений r_A и r_B.

Конфиденциальность сформированной итоговой последовательности, состоящей из n_C совпадающих битов, определяется соотношением в ней совпадающих инвертированных битов и совпадающих неинвертированных битов. Долю инвертированных совпадающих бит можно интерпретировать как вероятность того, что в совпадающих битах извлеченный бит окажется инвертированным, т.е. для БП, очищенной от не совпадающих битов, справедливо

$$P_{ИС} = e_{ИС},\ P_{НИС} = e_{НИС},\ P_{ИС} + P_{НИС} = 1, \qquad (12)$$

где $P_{ИС}, P_{НИС}$ – вероятности совпадения и. Энтропия такой последовательности равна

$$H = -n_C (P_{ИС} \log_2 P_{ИС} + P_{НИС} \log_2 P_{НИС}). \qquad (13)$$

Поскольку вероятности $P_{ИС}$, $P_{НИС}$ отличаются от 0,5, то это свойство может быть использовано для криптоанализа. Для повышения конфиденциальности итоговой последовательности предложены две процедуры. Во-первых, абонентам A и B известны позиции в итоговой последовательности инвертированных и неинвертированных битов базовой последовательности, поскольку каждый из абонентов знает номера битов в X_0, которые он инвертировал и может проследить их путь в итоговую последовательность. Криптоаналитику такая информация неизвестна. Зная расположения и число, например, инвертированных битов, A и B договариваются о некоторых согласованных секретных от криптоаналитика преобразованиях в итоговой последовательности. В качестве простейшего преобразования можно использовать выравнивание числа инвертированных и неинвертированных битов. Во-вторых, если на этапе устранения ошибок вместо согласованного удаления одного бита из пары, содержащей ноль или две ошибки, абоненты выбирают его случайно, независимо друг от друга, то не раскрывается номер оставшегося бита для криптоаналитика. Показано, что эту процедуру необходимо проводить только во время первой итерации, пока $e_C \approx e_H$.

Четвёртая глава посвящена разработке компьютерной имитационной модели для подтверждения работоспособности метода в пределах поставленных в диссертации задач исследования, а также экспериментальной отработки, уточнении и корректировки параметров отдельных процедур для получения результатов, в наибольшей мере отвечающих задачам формирования идентичных бинарных последовательностей у абонентов сети для использования их в качестве ключевой информации в алгоритмах аутентификации или шифрования.

Разработанная модель включает в себя следующие взаимосвязанные модули:

– модуль генерации исходных последовательностей;

– модуль устранения несовпадающих битов;

– модуль статистики и отслеживания номеров битов.

Данные программные модули разработаны и реализованы с использованием Borland Delphi 10.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Диссертационная работа посвящена исследованию формирования идентичных бинарных последовательностей у абонентов сети для использования их в качестве ключевой информации в алгоритмах аутентификации или шифрования без использования односторонних функций. Получены следующие результаты:

1. Получена обобщенная модель формирования идентичных бинарных последовательностей на базе открытого канала связи, позволяющая выявить возможность и общие закономерности формирования конфиденциальных ключевых последовательностей. Показано, что известные в настоящее время методы решения этой задачи включают одинаковую последовательность действий: формирование секретных индивидуальных исходных чисел (последовательностей) с некоторой долей подобия; устранение различий путем обмена информацией об ошибках по открытом каналу связи [1–А, 4–А, 6–А, 7–А, 8–А, 10–А].

2. Установлено, что при статистически независимом формировании бинарных последовательностей у абонентов сети доля несовпадающих битов является случайной и с равной вероятностью отклоняется от ½ в большую или меньшую сторону, что не позволяет в дальнейшем провести процедуру удаления ошибок с требуемой вероятностью [2–А, 5–А].

3. Предложен способ формирования исходных бинарных последовательностей у абонентов сети, обеспечивающий долю несовпадающих битов меньше ½ с заданной вероятностью и с приемлемым уровнем неопределенности сформированных последовательностей. Способ включает формирование открытой случайной базовой бинарной последовательности, независимое секретное случайное инвертирование битов базовой последовательности абонентами в количестве, рассчитанном по разработанной методике [1–А, 6–А, 12–А].

4. Предложен модифицированный итерационный метод отыскания и устранения несовпадающих битов в согласовываемых слабосовпадающих бинарных последовательностях, позволяющий эффективно устранять ошибки при проценте несовпадений, близком к 50. Метод основан на сравнении четностей пар битов, выбранных случайно и согласованно в обеих последовательностях, с

последующим удалением пар, содержащих одно несовпадение, а также согласованным удалением по одному биту из каждой оставляемой пары, причем для первой итерации этот бит может выбираться каждым абонентом случайно, что обеспечивает повышение неопределенности итоговой согласованной последовательности [2–А, 5–А, 13–А].

5. Предложен метод формирования идентичных бинарных последовательностей на базе открытого канала связи, включающий генерацию бинарных последовательностей с управляемым уровнем несовпадений и конфиденциальности битов, отыскание и устранение несовпадающих битов в сформированной слабосовпадающей последовательности, усиление конфиденциальности итоговой последовательности до приемлемого уровня, позволяющий сравнительно просто и без использования односторонних функций решать задачу распределения ключевой информации [3–А, 6–А, 8–А, 10–А].

6. Разработана компьютерная имитационная модель взаимодействия абонентов сети при формировании ключевой информации в соответствии с разработанным методом, позволяющая экспериментально выбирать параметры используемых процедур и оценивать работоспособность и эффективность предложенных решений [3–А, 9–А, 11–А].

Рекомендации по практическому использованию результатов

Полученные в диссертационной работе результаты могут быть использованы для создания действующих протоколов в задачах защиты информации и повышения эффективности известных методов.

В частности, способ формирования идентичных бинарных последовательностей у абонентов компьютерных сетей применим в протоколах распределения ключевой информации в задачах аутентификации или шифрования.

Метод удаления ошибок в слабосовпадающих последовательностях позволяет модифицировать протоколы, использующие квантовый канал. Возможность согласования последовательностей с большой долей ошибок открывает перспективу формирования согласованных БП при прослушивании квантового канала криптоаналитиком. Кроме того, этот метод применим в способе, использующем синхронизируемые ИНС. Предлагается комбинированное использование методов: на первом этапе использовать синхронизируемые ИНС для формирования последовательностей с некоторой долей ошибок, на втором этапе устранить ошибки с применением разработанного метода. Это позволит не доводить процесс до полной синхронизации и тем самым повысить конфиденциальность итоговой последовательности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных журналах

1–А. Абдольванд, Ф. Конфиденциальная идентификация двоичных последовательностей / В.Ф. Голиков, Ф. Абдольванд // Вестник БНТУ. – 2010. – № 2. – С. 29–32.

2–А. Абдольванд, Ф. Эффективность устранения ошибок в бинарных последовательностях при разнесенном формировании криптографического ключа / В.Ф. Голиков, Ф. Абдольванд // Доклады БГУИР. – 2010. – № 6 (52). – С. 107–112.

3–А. Абдольванд, Ф. Оценка потерь конфиденциальности при неклассических способах формирования криптографического ключа / В.Ф. Голиков, Ф. Абдольванд // Информатика. – 2011. – № 2 (30). – С. 104–110.

Статьи в сборниках материалов конференций

4–А. Голиков, В.Ф. О распределении ключевой информации в современных информационных системах / В.Ф. Голиков, Ф. Абдольванд // Комплексная защита информации: Материалы XIV междунар. конф., Могилев, 19–22 мая 2009 г. / редкол.: А.П. Леонов [и др.]. – Могилев, 2009. – С. 77–79.

5–А. Голиков, В.Ф. Устранение ошибок в бинарных последовательностях при формировании криптографического ключа без использования однонаправленных функций / В.Ф. Голиков, Ф. Абдольванд // Информационные системы и технологии: Материалы VI Междунар. конф., Минск, 24–25 нояб. 2010 г. / БГУИР; редкол.: А.Н. Курбацкий [и др.]. – Минск, 2010. – С. 34–37.

6–А. Голиков, В.Ф. Конфиденциальное формирование идентичных бинарных последовательностей в задачах защиты информации / В.Ф. Голиков, Ф. Абдольванд // Комплексная защита информации: Материалы XVI науч.-практ. конф., Гродно, 17–20 мая 2011 г. / редкол.: А.Н. Курбацкий [и др.]. – Гродно, 2011. – С. 123–126.

Тезисы докладов на научных конференциях

7–А. Абдольванд, Ф. Предисловие к квантовой криптографии / Ф. Абдольванд // Вторая научная конференция иранских студентов, проживающих в Беларуси, Минск, 17 апр. 2009 г. / БГМУ; редкол.: А. Бакуи [и др.]. – Минск, 2009. – С. 18–20.

8–А. Голиков, В.Ф. Об одной модели формирования ключевой информации для перспективных информационных технологий / В.Ф. Голиков, Ф. Абдольванд // Наука – образованию, производству, экономике: Материалы Седьмой междунар. научно-техн. конф., Минск, 15 мая 2009 г. / БНТУ, редкол.: Б.М. Хрусталев [и др.]. – Минск, 2009. – С. 156.

9–А. Абдольванд, Ф. Моделирование процесса идентификации бинарных последовательностей по выборкам ограниченного объема / Ф. Абдольванд, В.Ф. Голиков // Наука – образованию, производству, экономике: Материалы Седьмой междунар. науч.-техн. конф., Минск, 15 мая 2009 г. / БНТУ; редкол.: Б.М. Хрусталев [и др.]. – Минск, 2009. – С. 157.

10–А. Абдольванд, Ф. Об одном способе идентификации ключевых бинарных последовательностей / В.Ф. Голиков, Ф. Абдольванд // Технические средства защиты информации: Материалы VII Белорус.-российск. науч.-техн. конф., Минск, 23–24 июня 2009 г. / БГУИР; редкол.: Л.М. Лыньков [и др.]. – Минск, 2009. – С. 35.

11–А. Абдольванд, Ф. Моделирование процесса формирования идентичных бинарных последовательностей / Ф. Абдольванд // Наука – образованию, производству, экономике: Материалы Восьмой междунар. науч.-техн. конф., Минск, 25 апр. 2010 г. / БНТУ; редкол.: Б.М. Хрусталев [и др.]. – Минск, 2010. – С. 227.

12–А. Голиков, В.Ф. Алгоритм формирования идентичных бинарных последовательностей / В.Ф. Голиков, Ф. Абдольванд // Наука – образованию, производству, экономике: Материалы Восьмой междунар. науч.-техн. конф., Минск, 25 апр. 2010 г. / БНТУ; редкол.: Б.М. Хрусталев [и др.]. – Минск, 2010. – С. 232.

13–А. Голиков, В.Ф. Устранение ошибок в бинарных ключевых последовательностях при разнесенном формировании ключа / В.Ф. Голиков, Ф. Абдольванд // Технические средства защиты информации: тез. докл. и кратк. сообщ. VIII Белорус.-российск. науч.-техн. конф., Браслав, 24–28 мая 2010 г. / БГУИР; редкол.: Л.М. Лыньков [и др.]. – Минск, 2010. – С. 43.

РЭЗЮМЭ

Абдальванд Фарид

Открытае фарміраванне канфідэнцыйных ідэнтычных бінарных паслядоўнасцяў у задачах абароны інфармацыі

Ключавыя словы: крыптаграфічная сістэма, бінарная паслядоўнасць, ключавая інфармацыя.

Мэтай работы: з'яўляецца распрацоўка тэарэтычных палажэнняў і практычных рэкамендацый, накіраваных на распрацоўку метада фарміравання ідэнтычных бінарных паслядоўнасцяў у абанентаў сеткі для выкарыстання іх ў якасці ключавой інфармацыі ў алгарытмах аўтэнтыфікацыі ці шыфравання.

Аб'ектам даследвання з'яўляюцца заканамернасці фарміравання ключавой інфармацыі ў компьютэрных сетках. Прадметам даследвання з'яўляецца спосаб фарміравання ідэнтычных бінарных паслядоўнасцяў у абанентаў сеткі без выкарыстання аднабаковых функцый.

Атрыманыя вынікі і іх навіна: прапанаваны спосаб прамога размеркавання ключавой інфармацыі, заснаваны на выяўленых заканамернасцях, уключаючых фармірованне бінарных паследоўнасцей з лімітна дапустимым узроўнем подабенства пры приймальным узроўнем канфідэнцыйнасці, скасавання несупадзення ўзроўнем шляхам абмена інфармацияй об нессупадзеннях по адкрытаму каналу сувязі, повышэння канфідэнцыйнасці падагульняльнай паслядоўнасці за кошт дададковай інфармацыі аб структуры, сфарміраванай паслядоўнасці, невядомай крыптааналітыку.

Ступень выкарыстання: распрацавана методыка разліка параметраў унясення патрабуемага узгаднення, праведзены аналіз структуры сфарміраваных зыходных паслядоўнасцяў. Праведзеная ацэнка ўзроўня недакладнасцяў сфарміраваных выніковых бінарных паслядоўнасцяў паказвае, што прапанаваны метад дазваляе фарміраваць абанентам агульную бінарную паследоўнасць, прыстасаваную да выкарыстання ў якасці ключавой інфармацыі. Прапанаваны спосабы яе павышэння, дазваляючыя абанентам зрабіць узгодненыя сакрэтныя ад крыптааналітыка пераўтварэнні выніковай паслядоўнасці.

Комп'ютарная імітацыйная мадэль працэса фарміравання ідэнтычных бінарных паследоўнасцей падцьвердзіла тэарэтычныя меркаванні и дазволіла вызначыць асноўныя параметры пераўтварэнняў.

Галіна ўжывання: спосаб дае магчымасць абанентам сеткі сфарміраваць агульную канфідэнцыйную бінарную паслядоўнасць, але не праводзіць іх аўтэнтыфікацыі, значыць для яго практычнага выкарыстання ў такім выглядзе неабходна мець аўтэнтыфіцыраваны канал ці канал, дазваляючы толькі праслухоўваць інфармацыю.

РЕЗЮМЕ

Абдольванд Фарид

Открытое формирование конфиденциальных идентичных бинарных последовательностей в задачах защиты информации

Ключевые слова: криптографическая система, бинарная последовательность, ключевая информация.

Цель работы: разработка теоретических положений и практических рекомендаций, направленных на разработку метода формирования идентичных бинарных последовательностей у абонентов сети для использования их в качестве ключевой информации в алгоритмах аутентификации или шифрования. Объектом исследования являются закономерности формирования ключевой информации в компьютерных сетях. Предметом исследования является способ формирования идентичных бинарных последовательностей у абонентов сети без использования односторонних функций.

Полученные результаты и их новизна: предложен способ прямого распределения ключевой информации, основывающийся на выявленных закономерностях, включающий формирование бинарных последовательностей с предельно допустимым уровнем подобия при приемлемом уровне конфиденциальности, устранение несовпадений путем обмена информацией о несовпадениях по открытому каналу связи, повышение конфиденциальности итоговой последовательности за счет дополнительной информации о структуре, сформированной последовательности, неизвестной криптоаналитику.

Степень использования: разработана методика расчета параметров внесения требуемого рассогласования, проведен анализ структуры сформированных исходных последовательностей. Проведенная оценка уровня неопределенности сформированных итоговых бинарных последовательностей показывает, что предложенный метод позволяет формировать абонентам общую БП, пригодную для использования в качестве ключевой информации. Предложены способы ее повышения, позволяющие абонентам производить согласованные секретные от криптоаналитика преобразования итоговой последовательности.

Компьютерная имитационная модель процесса формирования идентичных бинарных последовательностей подтвердила теоретические предположения и позволила определить основные параметры преобразований.

Область применения: способ дает возможность абонентам сети сформировать общую конфиденциальную бинарную последовательность, но не производит её аутентификации, следовательно, для его практического использования в таком виде необходимо иметь аутентифицированный канал или канал, позволяющий только прослушивать информацию.

SUMMARY

Abdolvand Farid

Open formation of confidential identical binary sequences to solve information protection problems

Key words: cryptographic system, binary sequence, key information.

This work is aimed at elaborating theoretical provisions and practical recommendations to develop identical binary sequence formation techniques for network users to use the same as the key information in authentication or enciphering algorithms.

Aim of work: is the formation regulations of computer network key information. The study focuses on research of identical binary sequence techniques application by network users with no single-way function used.

Obtained results and their originality: the author has suggested the method of key information direct distribution, based on regularities revealed, including binary sequence formation with maximum similarity at acceptable confidentiality level, distortion removal by exchange of distortion-related information at open com channels, final sequence confidentiality increase due to additional structural information availability and generation of sequences unknown to cryptanalyst.

Usage degree: the study has elaborated the calculation method for required misbalance parameters, while analyzing the initial sequence structural framework. The assessment made to analyze the final binary sequence indeterminacy level proves that the suggested method enables users to form the overall binary sequence organization to be further used as the key information. The binary sequence organization upgrade methods have been suggested to avail coordinated cryptanalyst-concealed transformations of the final sequences to users.

The computer simulation of the identical binary sequence formation process has confirmed the theoretical assumptions and allowed to determine the major transformation parameters.

Application area: the method developed provides overall confidentiality of binary sequences when applied by network users, with no authentication feasible. For this purpose, an authenticated channel or overhearing channel should be used for this method practical implementation.

Научное издание

АБДОЛЬВАНД ФАРИД

ОТКРЫТОЕ ФОРМИРОВАНИЕ КОНФИДЕНЦИАЛЬНЫХ ИДЕНТИЧНЫХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание учёной степени кандидата технических наук

Подписано в печать 14.02.2012. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Отпечатано на ризографе. Усл. печ. л. 1,63.
Уч.-изд. л. 1,4. Тираж 60 экз. Заказ 88.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6