На правах рукописи

Косолапов Дмитрий Олегович

ПОСТРОЕНИЕ МНОГОСТОРОННИХ МУЛЬТИЛИНЕЙНЫХ АЛГОРИТМОВ В УСЛОВИЯХ РАЗЛИЧНЫХ МОДЕЛЕЙ БЕЗОПАСНОСТИ

05.13.18 - математическое моделирование, численные методы и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Владивосток
2010

Работа выполнена на кафедре информационной безопасности Дальневосточного государственного университета

Научный руководитель: доктор физико-математических наук, профессор КОРНЮШИН Павел Николаевич

Официальные оппоненты: доктор физико-математических наук, профессор НУРМИНСКИЙ Евгений Алексеевич

доктор физико-математических наук, профессор СТЕПАНОВА Алёна Андреевна

Ведущая организация: Морской государственный университет имени адмирала Г.И. Невельского (г. Владивосток)

Защита состоится « 10 » декабря 2010 г. в 10:00 часов на заседании диссертационного совета Д 005.007.01 в Институте автоматики и процессов управления ДВО РАН по адресу: 690041, г. Владивосток, ул. Радио, 5.

С диссертацией можно ознакомиться в библиотеке Института автоматики и процессов управления ДВО РАН по адресу: 690041, г. Владивосток, ул. Радио, 5.

Автореферат разослан « 2 » ноября 2010 г.

Ученый секретарь
диссертационного совета Д 005.007.01,
к.т.н. А.В. Лебедев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Развитие информационных технологий и средств обработки, хранения и передачи информации привело к необходимости защищать данные на всех этапах информационного обмена. Криптографический уровень защиты информации является своего рода «последней линией обороны», т.к. позволяет защищать информацию даже после получения к ней доступа злоумышленником. При этом обеспечивается определенный уровень криптографической стойкости, т.е. способности криптографического алгоритма противостоять возможным атакам на него. Стойким считается алгоритм, для успешной атаки на который злоумышленнику необходимы недостижимые вычислительные ресурсы, недостижимый объём перехваченных открытых и зашифрованных сообщений или же такое время раскрытия, что по его истечению защищенная информация будет уже не актуальна. Стойкость криптографических алгоритмов доказывается в условиях определенных математических моделей безопасности.

Известны различные виды моделей безопасности, классифицирующиеся по ряду критериев, например, по защищаемому объекту (модели безопасности доступа). Под моделями безопасности криптографических примитивов понимаются формализованные модели поведения вероятного злоумышленника при попытке нарушения стойкости криптографических алгоритмов.

Появление в 1976 г. асимметричной криптографии (У. Диффи и М. Хеллман) значительно расширило возможности криптографии и положило начало разработке большого количества криптографических алгоритмов. С математической точки зрения стойкость асимметричных криптоалгоритмов основана на сложности решения известных математических задач, таких как, например, задач факторизации целого числа и дискретного логарифмирования в конечном поле. Алгоритмы решения данных задач имеют субэкспоненциальную сложность, поэтому при определенных размерах ключей их решение полагается невозможным на современном этапе развития вычислительной техники.

В 90-е гг. XX в. получили распространение асимметричные криптоалгоритмы на основе эллиптических кривых. Данные алгоритмы строятся с помощью преобразования семейства алгоритмов Эль-Гамаля, а их стойкость основана на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой. Известно, что задача дискретного логарифмирования в конечном поле не сложнее задачи дискретного логарифмирования в группе точек эллиптической кривой, заданной над конечным полем.

В 2000 г. А. Жу был предложен первый билинейный алгоритм – асимметричный криптоалгоритм ключевого соглашения на основе билинейных спариваний в группе точек эллиптической кривой. Стойкость билинейных

алгоритмов основана на сложности решения билинейных проблем Диффи-Хеллмана. В настоящее время не существует эффективных математических алгоритмов решения данных проблем. С помощью билинейного спаривания также были построены эффективные алгоритмы на основе идентификационных данных – криптоалгоритмы, в которых открытый ключ абонента получается явным образом из его идентификатора.

К настоящему времени разработан ряд билинейных криптографических алгоритмов, таких как: алгоритм шифрования на основе идентификационных данных (Д. Боне, М. Франклин), алгоритм избирательного шифрования (Д. Боне, Г. Крещенцо, Р. Островски, Г. Персиано), алгоритм подписи (Д. Боне, Б. Линн, Х. Шахем), алгоритм слепой подписи (А. Болдырева), алгоритм мультиподписи (А. Болдырева), алгоритм короткой подписи (Ф. Занг, Р. Сафави-Наини, В. Сусило), алгоритм распределения ключа (Р. Сакаи, К. Огиши, М. Казахара), алгоритмы шифроподписи на основе идентификационных данных (Д. Мэлони-Ли и Б. Либерт, Д. Квисквотер). Данные алгоритмы обеспечивают безопасность информации при её обмене несколькими абонентами.

В случае группового обмена информацией билинейные криптоалгоритмы могут быть использованы при условии разбиения группы абонентов на подгруппы из нескольких абонентов и последовательного применения данных алгоритмов к каждой подгруппе. Данный метод приводит к повышению вычислительной и связной сложности обеспечения безопасности информации для всей группы.

Для решения задачи обеспечения безопасного группового информационного обмена в 2002 г. Д. Боне и А. Сильверберг были предложены первые мультилинейные алгоритмы – алгоритм ключевого соглашения и алгоритм широковещательного шифрования. В данных алгоритмах было использовано мультилинейное отображение, являющееся обобщением билинейного спаривания до случая n аргументов. Также в 2002 г. Х.К. Ли, Х.С. Ли, Я.Р. Ли было предложено семейство мультилинейных алгоритмов ключевого соглашения. Стойкость данных алгоритмов основана на сложности решения мультилинейных проблем Диффи-Хеллмана.

Предложенные мультилинейные алгоритмы имеют ряд недостатков, связанных со стойкостью, а именно: для алгоритма широковещательного шифрования Д. Боне и А. Сильверберг не показана стойкость к адаптивным атакам с выбором шифротекста, для алгоритмов ключевого соглашения Х.К. Ли, Х.С. Ли, Я.Р. Ли не предусмотрена возможность выявления злоумышленника. Также, для ряда криптографических примитивов (таких, как шифрование на основе идентификационных данных, избирательное шифрование и шифроподпись) до настоящего времени не было предложено групповых (многосторонних) алгоритмов, что усложняет использование данных примитивов для групп абонентов.

Поэтому в настоящее время возникла трудность построения многосторонних алгоритмов, являющихся более эффективными для группы абонентов, чем многократное применение алгоритмов для подгрупп из нескольких абонентов. При этом стойкость данных алгоритмов не должна быть ниже, чем стойкость схемы многократного применения алгоритмов для подгрупп из нескольких абонентов.

Таким образом, тема проводимого в данной работе исследования является актуальной. Из актуальности темы работы следует ее цель.

Целью работы является разработка семейства многосторонних мультилинейных алгоритмов, являющихся доказуемо стойкими в условиях различных моделей безопасности.

Задачи исследования. Для достижения поставленной цели решались следующие задачи:

1) построение математических моделей безопасности многосторонних криптографических примитивов;

2) разработка многосторонних алгоритмов широковещательного шифрования, избирательного шифрования, подписи, слепой подписи, распределения ключа, шифроподписи и ключевого соглашения;

3) доказательство стойкости и оценка сложности разработанных многосторонних алгоритмов.

Научная новизна полученных результатов заключается в следующем.

1) Разработаны более сильные математические модели безопасности для многосторонних криптографических примитивов;

2) Предложены многосторонние мультилинейные алгоритмы, позволяющие использовать билинейные криптографические примитивы в случае большого количества абонентов;

3) Доказаны стойкость к адаптивной атаке с выбранным открытым текстом базового алгоритма широковещательного шифрования на основе идентификационных данных, стойкость к адаптивной атаке с выбранным шифротекстом полного алгоритма широковещательного шифрования на основе идентификационных данных и стойкость алгоритма ключевого соглашения на основе идентификационных данных с выявлением злоумышленника в расширенной модели безопасности ключевого соглашения;

4) Разработаны математические проблемы, обеспечивающие приемлемый уровень сложности для обеспечения стойкости многосторонних алгоритмов.

Методы исследования. В диссертации применяются методы современной алгебры конечных полей, теория вероятностей, теория сложности алгоритмов, математические модели безопасности криптографических примитивов.

Теоретическая и практическая значимость работы. В работе предложены математические модели безопасности широковещательного

шифрования при адаптивной атаке с выбором шифротекста и открытого текста, расширенная модель безопасности ключевого соглашения, многосторонние математические проблемы, проведено строгое доказательство стойкости предложенных криптографических алгоритмов в условиях разработанных математических моделей безопасности.

Использование мультилинейных отображений позволит снизить связную и вычислительную сложность многосторонних алгоритмов, усилив их стойкость. Предложенные мультилинейные алгоритмы могут быть использованы при построении многосторонних криптосистем для обеспечения конфиденциальности и аутентичности информационного обмена группы абонентов.

Апробация результатов. Полученные результаты докладывались на региональной научно-технической конференции «Знание, творчество, профессионализм» (Владивосток, 2005), 3-й и 4-й Международных научно-практических конференциях «Интеллектуальные технологии в образовании, экономике и управлении» (Воронеж, 2006-2007), Региональной конференции студентов, аспирантов и молодых ученых по физике (Владивосток, 2006), конференции «Информационная безопасность в открытом образовании» (Магнитогорск, 2007), 48-й, 50-й и 51-й Всероссийских научных конференциях ТОВМИ (Владивосток, 2005, 2007-2008), Российской школе-семинаре «Синтаксис и семантика логических систем» (Владивосток, 2008), Всероссийских конференциях студентов, аспирантов и молодых ученых по физике ДВГУ (Владивосток, 2007, 2009), XXXIII Дальневосточной математической школе-семинаре имени академика Е.В. Золотова (Владивосток, 2008), Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых (Томск, 2009), семинаре кафедры информационной безопасности ДВГУ (Владивосток, 2009), семинаре Института автоматики и процессов управления ДВО РАН (Владивосток, 2009).

Публикации. По материалам диссертации опубликовано 18 работ, в том числе 2 в журналах, рекомендуемых ВАК.

Структура и объем работы. Диссертационная работа состоит из введения, четырех глав, заключения и списка литературы, включающего 67 наименований. Содержание работы изложено на 138 страницах текста. Работа содержит 2 таблицы и 2 рисунка.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассматривается состояние проблемы на сегодняшний день и актуальность темы исследования, формулируется цель и задачи диссертационной работы, приводится ее краткое содержание.

В **первой главе** исследуются математические основы билинейных и мультилинейных криптографических алгоритмов, рассматриваются

билинейные и мультилинейные криптографические алгоритмы, предложенные к настоящему времени. Первая глава состоит из 3 разделов.

В первом разделе описываются математические аспекты билинейной криптографии, история билинейных алгоритмов и математические проблемы, на сложности решения которых основана стойкость билинейных алгоритмов.

Во втором разделе рассматриваются базовый и полный билинейные алгоритмы шифрования Боне и Франклина на основе идентификационных данных, алгоритм избирательного шифрования, алгоритм подписи Боне, Линна и Шахема, алгоритм слепой подписи, алгоритм мультиподписи, алгоритм подписи Занга, Сафави-Наини и Сусило, однораундовый алгоритм выработки общего ключа А. Жу, алгоритм распределения ключа Сакаи, Огиши и Казахара, алгоритм шифроподписи Мэлони-Ли и алгоритм шифроподписи Либерта и Квисквотера.

В третьем разделе рассматривается обобщение билинейного спаривания – мультилинейное отображение и предложенные к настоящему времени мультилинейные алгоритмы. Стойкость данных алгоритмов в соответствующих моделях безопасности основана на сложности решения многосторонних мультилинейных математических проблем.

Сформулированы следующие n-сторонние математические проблемы, на сложности решения которых основана стойкость многосторонних алгоритмов: n-сторонняя проблема распознавания Диффи-Хеллмана, n-сторонняя вычислительная проблема Диффи-Хеллмана, мультилинейная проблема Диффи-Хеллмана (MDH), проблема инверсии Диффи-Хеллмана и общая проблема Диффи-Хеллмана.

Предложены следующие n-сторонние математические проблемы, на сложности решения которых может быть основана стойкость будущих многосторонних алгоритмов: n-сторонняя слабая проблема Диффи-Хеллмана, обратная n-сторонняя вычислительная проблема Диффи-Хеллмана, обобщенная мультилинейная проблема Диффи-Хеллмана, мультилинейная проблема распознавания Диффи-Хеллмана и мультилинейная проблема распознавания Диффи-Хеллмана для случая хеширования.

n-сторонняя слабая проблема Диффи-Хеллмана заключается в сложности получения набора $\langle s_1 Q,...,s_n Q\rangle$ по заданному набору $\langle P,Q,s_1 P,...,s_n P\rangle$, где $P,Q \in G$, P - образующий элемент аддитивной циклической группы G простого порядка q, а $s_1,...,s_n \in \mathbb{Z}_q^*$.

Обратная n-сторонняя вычислительная проблема Диффи-Хеллмана заключается в сложности нахождения bP, $b \in Z_q^*$, удовлетворяющего равенству $a_1...a_n = rb \bmod q$ по заданному набору $\langle P,a_1 P,...,a_n P,rP\rangle$, где $a_1,...,a_n,r \in \mathbb{Z}_q^*$, а P - образующий элемент аддитивной циклической группы G простого порядка q.

Обобщенная мультилинейная проблема Диффи-Хеллмана (GMDH – General Multilinear Diffie-Hellman problem) заключается в сложности получения

набора $\langle Q, \mu(Q, P_2, ..., P_{n+1})^{a_2 \cdots a_{n+1}} \rangle$ по заданному набору $\langle P, a_2 P, a_3 P, ..., a_{n+1} P \rangle$, где элементы $a_2, a_3, ..., a_{n+1} \in \mathbb{Z}_q^*$ выбираются случайно, $Q, P_2, ..., P_{n+1}$ - произвольные элементы аддитивной циклической группы G простого порядка q, P - образующий элемент группы G_1, а μ - n-мультилинейное отображение.

Мультилинейная проблема распознавания Диффи-Хеллмана (DMDH – Decisional Multilinear Diffie-Hellman problem) заключается в сложности проверки равенства $r = \mu(P, P, ..., P)^{a_1 a_2 \cdots a_{n+1}}$ по заданному набору $\langle P, a_1 P, a_2 P, ..., a_{n+1} P, r \rangle$, где элементы $a_1, a_2, ..., a_{n+1}, r \in \mathbb{Z}_q^*$ выбираются случайно, P - образующий элемент аддитивной циклической группы G простого порядка q, а μ - n-мультилинейное отображение.

Мультилинейная проблема распознавания Диффи-Хеллмана для случая хеширования (DHMDH – Decisional Hash Multilinear Diffie-Hellman problem) заключается в сложности проверки равенства $r = H(\mu(P, P, ..., P)^{a_1 a_2 \cdots a_{n+1}})$ по заданному набору $\langle P, a_1 P, a_2 P, ..., a_{n+1} P, r \rangle$, где $a_1, a_2, ..., a_{n+1}, r \in \mathbb{Z}_q^*$ выбираются случайно, задана хеш-функция $H : G_2 \to \mathbb{Z}_q^*$, G_2 - мультипликативная циклическая группа простого порядка q, P - образующий элемент аддитивной циклической группы G_1 простого порядка q, а μ - n-мультилинейное отображение.

Во **второй главе** предложены мультилинейные алгоритмы, полученные с помощью обобщения соответствующих билинейных алгоритмов на мультилинейный случай, рассмотрены возможности построения данных алгоритмов в модели k-ичного дерева и возможности их использования в случае отсутствия мультилинейных отображений для всех значений n. Вторая глава состоит из 3-х разделов.

В первом разделе построены многосторонние мультилинейные алгоритмы.

Построен базовый мультилинейный алгоритм широковещательного шифрования на основе идентификационных данных (MulBasicIdent). Данный алгоритм решает задачу шифрования сообщения для n абонентов с идентификаторами $ID_1, ..., ID_n$. Алгоритм представлен этапами инициализации, получения закрытого ключа, шифрования и расшифрования.

Пусть $k \in \mathbb{Z}$ - принимаемый алгоритмом на этапе инициализации параметр стойкости. Этап *инициализации* представлен следующими процедурами.

1. На основе k Центром генерации закрытых ключей (PKG) генерируется простой порядок q групп G_1 и G_2, $2n$-мультилинейное отображение $\mu : \underbrace{G_1 \times G_1 \times ... \times G_1}_{2n} \to G_2$ и произвольный образующий элемент группы $P \in G_1$, где G_1 - аддитивная циклическая группа, а G_2 - мультипликативная циклическая группа.

2. Центром PKG случайным образом выбираются элементы $s_1,...,s_n \in \mathbb{Z}_q^*$ и вычисляется набор открытых ключей $P_{pub_1} = s_1 P,...,P_{pub_n} = s_n P$.

3. Центром PKG выбираются криптографические хеш-функции $H_1 : \{0,1\}^* \to G_1^*$ и $H_2 : G_2 \to \{0,1\}^l$ для некоторого $l \in \mathbb{Z}$, где $\{0,1\}^*$ - множество двоичных векторов произвольной длины, а $\{0,1\}^l$ - множество двоичных векторов длины l.

В данном алгоритме пространства сообщений и шифротекстов представляют собой множества $\vartheta = \{0,1\}^l$ и $C = G_1^* \times \{0,1\}^l$ соответственно, элементы $s_1,...,s_n \in \mathbb{Z}_q^*$ являются мастер-ключами абонентов, а системными параметрами является набор $\langle G_1, G_2, \mu, l, P, P_{pub_1},...,P_{pub_n}, H_1, H_2 \rangle$.

Особенностью алгоритмов на основе идентификационных данных является необходимость получения абонентом закрытого ключа у Центра PKG. На этапе *получения закрытого ключа* проводятся следующие вычисления:

1) для идентификаторов абонентов $ID_1,...,ID_n \in \{0,1\}^*$ Центром PKG вычисляются $Q_{ID_1} = H_1(ID_1) \in G_1^*,...,Q_{ID_n} = H_1(ID_n) \in G_1^*$;

2) Центром PKG вычисляются и передаются абонентам по защищенному каналу закрытые ключи $d_{ID_1} = s_1 Q_{ID_1},...,d_{ID_n} = s_n Q_{ID_n}$, $d_{ID_i} \in G_1$, где $s_1,...,s_n$ - мастер-ключи.

На этапе *шифрования* сообщения M с помощью идентификаторов $ID_1,...,ID_n \in \{0,1\}^*$ абонентом выполняются следующие операции:

1) вычисляются $Q_{ID_1} = H_1(ID_1) \in G_1^*,...,Q_{ID_n} = H_1(ID_n) \in G_1^*$;

2) выбирается случайный элемент $r \in \mathbb{Z}_q^*$;

3) вычисляется шифротекст $C = \langle rP, M \oplus H_2(g^r) \rangle$, где $g = \mu(Q_{ID_1},...,Q_{ID_n}, P_{pub_1},...,P_{pub_n}) \in G_2^*$.

Для *расшифрования* шифротекста $C = \langle U, V \rangle$ абонентом с идентификатором ID_i с помощью закрытого ключа $d_{ID_i} \in G_1^*$ вычисляется открытый текст следующим образом:

$$V \oplus H_2(\mu(Q_{ID_1},...,Q_{ID_{i-1}}, d_{ID_i}, Q_{ID_{i+1}},...,Q_{ID_n}, P_{pub_1},...,P_{pub_{i-1}}, U, P_{pub_{i+1}},...,P_{pub_n})) = M.$$

Корректность алгоритма подтверждается выполнением следующего равенства, смысл которого сводится к подстановке в аргумент функции H_2 на этапе расшифрования выражений для закрытого ключа $d_{ID_i} = s_i Q_{ID_i}$ и элемента $U = rP$:

$$\mu(Q_{ID_1},...,Q_{ID_{i-1}}, d_{ID_i}, Q_{ID_{i+1}},...,Q_{ID_n}, P_{pub_1},...,P_{pub_{i-1}}, U, P_{pub_{i+1}},...,P_{pub_n}) =$$
$$= \mu(Q_{ID_1},...,Q_{ID_n}, P_{pub_1},...,P,...,P_{pub_n})^{s_i r} = \mu(Q_{ID_1},...,Q_{ID_n}, P_{pub_1},...,P_{pub_n})^r = g^r.$$

Так как $V = M \oplus H_2(g^r)$, то на этапе расшифрования получаем $M \oplus H_2(g^r) \oplus H_2(g^r) = M$.

На основе алгоритма MulBasicIdent с помощью метода Фуджисаки-Окамото построен полный алгоритм широковещательного шифрования на основе идентификационных данных (MulFullIdent, МКШОИД).

МКШОИД также представлен этапами инициализации, получения закрытого ключа, шифрования и расшифрования.

Пусть $k \in \mathbb{Z}$ - принимаемый алгоритмом на этапе инициализации параметр стойкости. Этап *инициализации* представлен следующими процедурами.

1. На основе k Центром PKG генерируется простой порядок q групп G_1 и G_2, $2n$-мультилинейное отображение $\mu : \underbrace{G_1 \times G_1 \times ... \times G_1}_{2n} \to G_2$ и произвольный образующий элемент группы $P \in G_1$, где G_1 - аддитивная циклическая группа, а G_2 - мультипликативная циклическая группа.

2. Центром PKG случайным образом выбираются элементы $s_1, ..., s_n \in \mathbb{Z}_q^*$ и вычисляется набор открытых ключей $P_{pub_1} = s_1 P, ..., P_{pub_n} = s_n P$, $P_{pub_i} \in G_1$.

3. Центром PKG выбираются криптографические хеш-функции $H_1 : \{0,1\}^* \to G_1^*$, $H_2 : G_2 \to \{0,1\}^l$ для некоторого $l \in \mathbb{Z}$, $H_3 : \{0,1\}^l \times \{0,1\}^l \to \mathbb{Z}_q^*$ и $H_4 : \{0,1\}^l \to \{0,1\}^l$.

В данном алгоритме пространства сообщений и шифротекстов представляют собой множества $\vartheta = \{0,1\}^l$ и $C = G_1^* \times \{0,1\}^l \times \{0,1\}^l$ соответственно, элементы $s_1, ..., s_n \in \mathbb{Z}_q^*$ являются мастер-ключами абонентов, а системными параметрами является набор $\langle G_1, G_2, \mu, l, P, P_{pub_1}, ..., P_{pub_n}, H_1, H_2, H_3, H_4 \rangle$.

На этапе *получения закрытого ключа* проводятся следующие вычисления:

1) для идентификаторов абонентов $ID_1, ..., ID_n \in \{0,1\}^*$ Центром PKG вычисляются $Q_{ID_1} = H_1(ID_1) \in G_1^*, ..., Q_{ID_n} = H_1(ID_n) \in G_1^*$;

2) Центром PKG вычисляются и передаются абонентам по защищенному каналу закрытые ключи $d_{ID_1} = s_1 Q_{ID_1}, ..., d_{ID_n} = s_n Q_{ID_n}$, $d_{ID_i} \in G_1$, где $s_1, ..., s_n$ - мастер-ключи.

На этапе *шифрования* сообщения M с помощью идентификаторов $ID_1, ..., ID_n \in \{0,1\}^*$ абонентом выполняются следующие операции:

1) вычисляются $Q_{ID_1} = H_1(ID_1) \in G_1^*, ..., Q_{ID_n} = H_1(ID_n) \in G_1^*$;

2) выбирается случайный вектор $\sigma \in \{0,1\}^l$, $l \in \mathbb{Z}$;

3) вычисляется $r = H_3(\sigma, M)$, $r \in \mathbb{Z}_q^*$;

4) вычисляется шифротекст $C = \langle rP, \sigma \oplus H_2(g^r), M \oplus H_4(\sigma) \rangle$, где $g = \mu(Q_{ID_1}, ..., Q_{ID_n}, P_{pub_1}, ..., P_{pub_n}) \in G_2^*$.

Для *расшифрования* шифротекста $C = \langle U, V, W \rangle$ абонентом с идентификатором ID_i выполняются следующие процедуры.

1. Если $U \notin G_1^*$, то шифротекст не принимается. В противном случае, с помощью закрытого ключа $d_{ID_i} \in G_1^*$ вычисляется:

$$V \oplus H_2(\mu(Q_{ID_1},...,Q_{ID_{i-1}},d_{ID_i},Q_{ID_{i+1}},...,Q_{ID_n},P_{pub_1},...,P_{pub_{i-1}},U,P_{pub_{i+1}},...,P_{pub_n})) = \sigma .$$

2. Абонентом вычисляется $W \oplus H_4(\sigma) = M$.

3. Абонентом вычисляется $r = H_3(\sigma, M)$, $r \in \mathbb{Z}_q^*$ и проверяется $U = rP$. Если равенство не выполняется, то шифротекст не принимается, в противном случае полагается, что M - открытый текст.

Корректность алгоритма подтверждается аналогично MulBasicIdent.

Помимо алгоритмов широковещательного шифрования на основе идентификационных данных также предложены многосторонние мультилинейные алгоритмы избирательного шифрования, подписи, слепой подписи, распределения ключа и шифроподписи.

Во втором разделе мультилинейный алгоритм подписи построен в модели k-ичного дерева.

В третьем разделе исследована возможность использования мультилинейных алгоритмов в случае отсутствия мультилинейных отображений для всех значений n. В данном случае возможна модификация алгоритмов добавлением фиктивных абонентов до ближайшего возможного значения n. После этапа инициализации алгоритма первые $n-r$ абонентов берут на себя функции эмуляции недостающих абонентов, где n - ближайшее допустимое количество абонентов, а r - реальное количество абонентов, $n \geq r$.

В **третьей главе** построены математические модели безопасности широковещательного шифрования, доказана стойкость предложенных алгоритмов MulBasicIdent и MulFullIdent (МКШОИД) в условиях данных моделей и проведена оценка вычислительной сложности всех предложенных в главе 2 криптографических алгоритмов. Третья глава состоит из 3-х разделов.

В первом разделе рассмотрены существующие модели безопасности, вычислительные модели, модели злоумышленников и типы проводимых атак.

Во втором разделе построены математические модели безопасности, в условиях которых проводится доказательство стойкости алгоритмов широковещательного шифрования. Модели безопасности широковещательного шифрования основаны на играх, проводимых злоумышленником (атакующим алгоритмом) с запросчиком (challenger).

Игра злоумышленника, проводящего атаку на алгоритм широковещательного шифрования, состоит из процедуры инициализации, 2-х этапов проведения запросов, постановки задачи и вывода результата.

Во время *инициализации* запросчик принимает параметр стойкости $k \in \mathbb{N}$, запускает процедуру инициализации алгоритма, передает атакующему алгоритму параметры $params$ и сохраняет мастер-ключи $master-keys$ в секрете. Определены G_1 - аддитивная циклическая группа простого порядка q с

образующим элементом P, и G_2 - мультипликативная циклическая группа простого порядка q.

На *этапе 1* атакующий алгоритм генерирует запросы $q_1,...,q_m$ и отправляет их запросчику, где q_i является:

1) запросом закрытого ключа $\langle ID_i' \rangle$. В данном случае запросчик запускает процедуру генерации закрытого ключа $d_i' \in G_1$, соответствующего открытому ключу $\langle ID_i' \rangle$, и передает d_i' атакующему алгоритму.

2) запросом расшифрования $\langle ID_i', C_i' \rangle$. В данном случае запросчик запускает процедуру генерации закрытого ключа d_i', соответствующего открытому ключу $\langle ID_i' \rangle$. Далее запускает процедуру расшифрования шифротекста C_i' с помощью d_i' и передает полученный открытый текст атакующему алгоритму.

Данные запросы проводятся адаптивно, т.е. каждый запрос q_i может зависеть от ответов на запросы $q_1,...,q_{i-1}$.

После завершения этапа 1 атакующий алгоритм генерирует 2 открытых текста $M_0, M_1 \in \vartheta$ равной длины и набор идентификаторов абонентов $ID_1,...,ID_n$, для которых он проводит атаку, где ϑ - множество открытых текстов произвольной длины. Единственным ограничением является тот факт, что $ID_i \neq ID_j'$ при $i = 1,...,n, j = 1,...,m$ во время этапа 1.

Постановка задачи запросчика атакующему алгоритму имеет следующий вид. Запросчик случайно выбирает бит $b \in \{0,1\}$ и отправляет $C_b = Encrypt(params, ID_1,...,ID_n, M_b)$ алгоритму.

На *этапе 2* атакующий алгоритм генерирует и отправляет запросчику дополнительные запросы $q_{m+1},...,q_l$, где q_i является:

1) запросом закрытого ключа $\langle ID_j' \rangle$, где $ID_i \neq ID_j'$ для $i = 1,...,n, j = m+1,...,l$. Запросчик отвечает так же, как и во время этапа 1.

2) запросом расшифрования $\langle ID_j', C_j' \rangle$, где $\langle ID_j', C_j' \rangle \neq \langle ID_i, C_i \rangle$ для $i = 1,...,n, j = m+1,...,l$. Запросчик отвечает так же, как и во время этапа 1.

Данные запросы могут проводиться адаптивно, как и во время этапа 1.

В качестве *результата* атакующий алгоритм возвращает бит $b' \in \{0,1\}$ и выигрывает игру, если $b = b'$.

Выигрышем при проведении атаки злоумышленника A на алгоритм E называется следующая функция параметра стойкости $k \in \mathbb{N}$: $Adv_{E,A}(k) = \left| \Pr[b = b'] - \frac{1}{2} \right|$, где $\Pr[b = b']$ - вероятность события, состоящего в совпадении значений битов b и b'.

Атакующий алгоритм в определенной выше игре называется IND-IDB-CCA злоумышленником. Если для всех полиномиальных во времени IND-IDB-

CCA злоумышленников A, способных проводить запросы закрытого ключа и расшифрования на алгоритм E, функция $Adv_{E,A}(k)$ является пренебрежимо малой, то определенная выше игра является *математической моделью безопасности широковещательного шифрования при адаптивной атаке с выбором шифротекста*, а алгоритм E в условиях данной модели является IND-IDB-CCA стойким (семантически стойким к адаптивной атаке с выбором шифротекста). В современной криптографии при построении алгоритмов шифрования проводится доказательство их стойкости в модели безопасности при адаптивной атаке с выбором шифротекста. Данная атака является самой сильной среди существующих атак на алгоритмы шифрования.

Злоумышленник A, способный проводить только запросы закрытого ключа, называется IND-IDB-CPA злоумышленником. Если для всех полиномиальных во времени IND-IDB-CPA злоумышленников A, способных проводить запросы закрытого ключа на алгоритм E, функция $Adv_{E,A}(k)$ является пренебрежимо малой, то игра атакующего алгоритма и запросчика является *математической моделью безопасности широковещательного шифрования при адаптивной атаке с выбором открытого текста*, а алгоритм E в условиях данной модели является IND-IDB-CPA стойким (семантически стойким к адаптивной атаке с выбором открытого текста).

Автором работы доказана стойкость алгоритма MulBasicIdent в условиях математической модели безопасности широковещательного шифрования при адаптивной атаке с выбором открытого текста и предположении сложности мультилинейной проблемы Диффи-Хеллмана (MDH).

Для доказательства IND-IDB-CCA стойкости алгоритма MulFullIdent доказана IND-CPA стойкость связанного алгоритма MulBasicPub - алгоритма широковещательного шифрования с открытым ключом (не использующего идентификационных данных). MulBasicPub состоит из 3-х процедур – генерации ключа, шифрования и расшифрования.

На этапе *генерации ключа* по заданному параметру стойкости $k \in \mathbb{Z}^+$ алгоритмом выполняется:

1) запускается генератор G и на основе k генерируются 2 группы G_1, G_2 простого порядка q и $2n$-мультилинейное отображение $\mu : \underbrace{G_1 \times G_1 \times ... \times G_1}_{2n} \to G_2$, выбирается произвольный образующий элемент группы $P \in G_1$;

2) случайным образом выбираются элементы $s_1, ..., s_n \in \mathbb{Z}_q^*$ и вычисляются $P_{pub_1} = s_1 P, ..., P_{pub_n} = s_n P$, далее случайным образом выбираются $Q_{ID_1}, ..., Q_{ID_n} \in G_1^*$;

3) выбирается криптографическая хеш-функция $H_2 : G_2 \to \{0,1\}^w$ для некоторого $w \in \mathbb{N}$;

4) возвращается открытый ключ абонента с индексом i - набор $\langle q, G_1, G_2, \mu, w, P, P_{pub_i}, Q_{ID_i}, H_2 \rangle$ и закрытый ключ $d_{ID_i} = s_i Q_{ID_i} \in G_1^*$.

Для *шифрования* сообщения $M \in \{0,1\}^*$ выбирается случайный элемент $r \in \mathbb{Z}_q^*$ и вычисляется шифротекст $C = \langle rP, M \oplus H_2(g^r) \rangle$, где $g = \mu(Q_{ID_1}, ..., Q_{ID_n}, P_{pub_1}, ..., P_{pub_n}) \in G_2^*$.

Для *расшифрования* шифротекста $C = \langle U, V \rangle$ i-м абонентом с помощью закрытого ключа $d_{ID_i} \in G_1^*$ вычисляется:

$$V \oplus H_2(\mu(Q_{ID_1}, ..., Q_{ID_{i-1}}, d_{ID_i}, Q_{ID_{i+1}}, ..., Q_{ID_n}, P_{pub_1}, ..., P_{pub_{i-1}}, U, P_{pub_{i+1}}, ..., P_{pub_n})) = M .$$

Доказательство стойкости алгоритма MulBasicPub следует из следующей леммы.

Лемма 3.4 Пусть $H_2 : G_2 \to \{0,1\}^w$ - случайный оракул, где $w \in \mathbb{N}$, а A - IND-CPA злоумышленник, имеющий выигрыш $\varepsilon(k)$ при атаке на MulBasicPub. Предположим, что A выполняет в общем $q_{H_2} > 0$ запросов к H_2 для каждого абонента, $q_{H_2} \in \mathbb{N}$. Тогда существует алгоритм B, решающий проблему MDH для генератора G с выигрышем не менее $2n\varepsilon(k)/q_{H_2}$ и временем работы не более $O(n*time(A))$, где n - количество абонентов, а $time(A)$ - время работы злоумышленника A.

С помощью данной леммы и ряда утверждений доказана стойкость алгоритма MulFullIdent (МКШОИД) в условиях математической модели безопасности широковещательного шифрования при адаптивной атаке с выбором шифротекста и предположении сложности MDH. Следующая теорема представляет собой один из основных результатов диссертации.

Теорема 3.7 В предположении, что хеш-функции H_1, H_2, H_3, H_4 являются случайными оракулами, алгоритм MulFullIdent является IND-IDB-CCA стойким при предположении сложности проблемы MDH в генерируемых генератором G группах. Пусть существует IND-IDB-CCA злоумышленник A, имеющий для каждого абонента выигрыш $\varepsilon(k) \in \mathbb{R}$ при атаке на MulFullIdent, и A проводит атаку за время, не превышающее $t(k) \in \mathbb{R}$, где $k \in \mathbb{N}$ - параметр стойкости. Пусть A выполняет не более $q_E \in \mathbb{N}$ запросов закрытого ключа, не более $q_D \in \mathbb{N}$ запросов расшифрования и не более $q_{H_2}, q_{H_3}, q_{H_4} \in \mathbb{N}$ запросов к оракулам H_2, H_3, H_4 соответственно. Тогда существует алгоритм B, решающий MDH для генератора G, со временем выполнения $t_1(k) \in \mathbb{R}$, при этом для его выигрыша и времени выполнения справедливы следующие неравенства:

$$Adv_{G,B}(k) \geq 2nFO_{adv}\left(\frac{\varepsilon(k)}{e(1+q_E+q_D)}, q_{H_4}, q_{H_3}, q_D\right)/q_{H_2},\ t_1(k) \leq nFO_{time}(t(k), q_{H_4}, q_{H_3}),$$

где

$$FO_{adv}(\varepsilon(k), q_{H_4}, q_{H_3}, q_D) = \frac{1}{2(q_{H_4}+q_{H_3})}((\varepsilon(k)+1)(1-2/q)^{q_D}-1),$$

$FO_{time}(t(k), q_{H_4}, q_{H_3}) = t(k) + O((q_{H_4} + q_{H_3})w)$,

n - количество абонентов, $w \in \mathbb{N}$ - длина σ.

Доказательство теоремы основано на последовательном применении доказанных утверждений и леммы. Возможность проведения атаки IND-IDB-CCA злоумышленником на алгоритм MulFullIdent с выигрышем $\varepsilon(k)$ и временем $t(k)$ приводит к возможности проведения атаки IND-CCA злоумышленником на алгоритм MulBasicPub^{hy} с выигрышем $\varepsilon' \geq \frac{\varepsilon(k)}{e(1+q_E+q_D)}$ и временем $t' \leq O(t)$ (утверждение 3.9). В свою очередь, возможность проведения атаки IND-CCA злоумышленником на алгоритм MulBasicPub^{hy} с выигрышем ε' и временем t' приводит к возможности проведения атаки IND-CPA злоумышленником на алгоритм MulBasicPub с выигрышем $\varepsilon'' \geq FO_{adv}(\varepsilon', q_{H_4}, q_{H_3}, q_D)$ и временем $t'' \leq FO_{time}(t', q_{H_4}, q_{H_3})$ (утверждение 3.8). Возможность проведения атаки IND-CPA злоумышленником на алгоритм MulBasicPub с выигрышем ε'' и временем t'' приводит к возможности решения мультилинейной проблемы Диффи-Хеллмана с выигрышем $\varepsilon''' \geq 2n\varepsilon'' / q_{H_2}$ и временем $t''' \leq O(nt'')$ (лемма 3.4).

Из приведенных выше утверждений получена оценка выигрыша злоумышленника при решении проблемы MDH и его времени работы:

$$\varepsilon''' \geq 2n\varepsilon'' / q_{H_2} \geq 2nFO_{adv}(\varepsilon', q_{H_4}, q_{H_3}, q_D) / q_{H_2} \geq 2nFO_{adv}(\frac{\varepsilon(k)}{e(1+q_E+q_D)}, q_{H_4}, q_{H_3}, q_D) / q_{H_2},$$

$$t''' \leq O(nt'') \leq nFO_{time}(t', q_{H_4}, q_{H_3}) \leq nFO_{time}(t(k), q_{H_4}, q_{H_3}).$$

Теорема доказана.

В сравнении с предложенным Боне и Сильверберг алгоритмом мультилинейного широковещательного шифрования предложенный алгоритм МКШОИД является более безопасным, т.к. обладает стойкостью к самому сильному типу атак злоумышленника.

В третьем разделе проведена оценка вычислительной эффективности предложенных в главе 2 мультилинейных алгоритмов. Показано, что МКШОИД является вычислительно и связно более эффективным, чем последовательное применение аналогичного по стойкости билинейного алгоритма Боне и Франклина.

В **четвертой главе** предложен алгоритм аутентифицированного ключевого соглашения на основе идентификационных данных и проведено доказательство стойкости алгоритма в расширенной модели безопасности ключевого соглашения.

В первом разделе рассмотрены результаты Х.К. Ли, Х.С. Ли, Я.Р. Ли, полученные в 2002 г.

Во втором разделе построен алгоритм ключевого соглашения. Алгоритм представлен процедурами инициализации, генерации и рассылки закрытых ключей, публикации, выработки ключа и верификации.

На этапе *инициализации* проводится генерация параметров алгоритма. Пусть G_1 и G_2 - мультипликативные циклические группы одинакового простого порядка p, а g - образующий элемент группы G_1. Пусть заданы 2 хеш-функции $H_1 : \{0,1\}^* \to G_1^*$ и $H_2 : G_1^* \to \mathbb{Z}_p^*$. Пусть $ID_1,...,ID_n$ - идентификаторы n абонентов $A_1,...,A_n$, вырабатывающих общий секретный ключ. Пусть $e_{n-1} : G_1^{n-1} \to G_2$ - $(n-1)$-мультилинейное отображение.

На этапе *генерации и рассылки закрытых ключей* для каждого абонента с идентификатором ID_i $(1 \le i \le n)$ Центром PKG вычисляется открытый ключ $Q_{ID_i} = H_1(ID_i) \in G_1$. Далее Центром PKG генерируется набор случайных целых чисел $s_1,...,s_n \in [1, p-1]$, являющихся мастер-ключами абонентов. По данным мастер-ключам Центром PKG вычисляется набор открытых ключей $P_{pub_1} = g^{H_2(H_1(ID_1)^{s_1})},...,P_{pub_n} = g^{H_2(H_1(ID_n)^{s_n})} \in G_1$, набор долгосрочных закрытых ключей $d_{ID_1} = H_1(ID_1)^{s_1},...,d_{ID_n} = H_1(ID_n)^{s_n} \in G_1$ и каждому абоненту передается его долгосрочный закрытый ключ по защищенному каналу.

На этапе *публикации* каждым абонентом A_i выбирается случайное целое число $a_i \in [1, p-1]$ и вычисляется $g^{a_i} \in G_1$. A_i рассылает всем остальным абонентам краткосрочный открытый ключ g^{a_i}, а a_i сохраняет в секрете.

На этапе *выработки ключа* по полученным значениям и идентификаторам i-м абонентом вычисляется набор открытых ключей $Q_{ID_i} = H_1(ID_i) \in G_1$ $(1 \le i \le n)$. Далее вычисляется ключ следующего вида

$$K_{A_i} = e_{n-1}(g^{a_1 + H_2(g^{a_1} \| Q_{ID_1})} P_{pub_1},...,g^{a_{i-1} + H_2(g^{a_{i-1}} \| Q_{ID_{i-1}})} P_{pub_{i-1}}, g^{a_{i+1} + H_2(g^{a_{i+1}} \| Q_{ID_{i+1}})} P_{pub_{i+1}},...,$$
$$,...,g^{a_n + H_2(g^{a_n} \| Q_{ID_n})} P_{pub_n})^{a_i + H_2(g^{a_i} \| Q_{ID_i}) H_2(d_{ID_i})} = e_{n-1}(g,...,g)^{[a_1 + H_2(g^{a_1} \| H_1(ID_1)) H_2(H_1(ID_1)^{s_1})]...[a_n + H_2(g^{a_n} \| H_1(ID_n)) H_2(H_1(ID_n)^{s_n})]}$$

Процедура *верификации* заключается в следующем. Выработанный ключ каждый абонент зашифровывает с помощью своего идентификатора (например, билинейным алгоритмом шифрования Боне и Франклина) и отправляет полученное значение Центру генерации закрытых ключей PKG. Центр PKG расшифровывает полученные значения и проверяет равенство всех выработанных ключей. В случае равенства Центр PKG широковещательно рассылает всем абонентам сигнальное сообщение одобрения передачи. В случае обнаружения одного или более ключей, не совпадающих с другими ключами, Центр PKG широковещательно рассылает сообщение отказа передачи и идентификаторы абонентов, являющихся злоумышленниками.

Автором работы предложена расширенная модель безопасности ключевого соглашения и доказана стойкость построенного алгоритма ключевого соглашения в условиях данной модели.

Теорема 4.1 Предложенный алгоритм ключевого соглашения является стойким к атакам активного злоумышленника в расширенной модели

безопасности ключевого соглашения при предположении сложности мультилинейной проблемы Диффи-Хеллмана и доверия к Центру генерации закрытых ключей.

В **заключении** диссертационной работы приводятся основные и дополнительные результаты исследований, проводится обоснование целесообразности использования математического аппарата мультилинейных отображений при построении многосторонних криптосистем будущего.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Построено семейство многосторонних алгоритмов с применением математического аппарата мультилинейных отображений, а именно, алгоритмы широковещательного шифрования на основе идентификационных данных, избирательного шифрования, подписи, слепой подписи, шифроподписи, ключевого соглашения на основе идентификационных данных с возможностью выявления злоумышленника.
2. Разработаны математические модели безопасности и математические проблемы, на сложности решения которых может быть основана стойкость многосторонних алгоритмов будущего.
3. Доказано, что алгоритм МКШОИД обладает стойкостью к адаптивным атакам с выбором шифротекста при предположении сложности проблемы MDH. Для обеспечения безопасного группового обмена информацией алгоритм МКШОИД является вычислительно и связно более эффективным, чем многократное применение билинейного алгоритма Боне и Франклина.
4. Предложен алгоритм ключевого соглашения на основе идентификационных данных. Преимуществом данного алгоритма является использование идентификационных данных абонентов и возможность выявления злоумышленника во время выполнения алгоритма. Показана стойкость предложенного алгоритма ключевого соглашения в расширенной модели безопасности ключевого соглашения. Проведена программная реализация алгоритма для случая 3-х абонентов.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Гончаров С.М., Косолапов Д.О., Харин Е.А. Выработка уникальных псевдослучайных последовательностей на основе клавиатурного почерка // Научно-практическая конференция «Информационная безопасность в открытом образовании». Тезисы докладов. - Магнитогорск: МаГУ, 2007. – С. 65-66.

2. Гончаров С.М., Косолапов Д.О., Харин Е.А. Мультилинейная схема шифрования Боне-Франклина на основе идентификационных данных // Научно-

практическая конференция «Информационная безопасность в открытом образовании». Тезисы докладов. - Магнитогорск: МаГУ, 2007. – С. 67-69.

3. Гончаров С.М., Косолапов Д.О. Использование мультилинейных отображений для построения безопасных систем группового обмена данными // Российская школа-семинар «Синтаксис и семантика логических систем». Тезисы докладов. - Владивосток: Изд-во Дальнаука, 2008. – С. 13-16.

4. Корнюшин П.Н., Гончаров С.М., Косолапов Д.О. Схема короткой групповой подписи в модели k-ичного дерева // Материалы 51-й всероссийской научной конференции. - Владивосток: ТОВМИ, 2008. - С. 79-81.

5. Косолапов Д.О., Гончаров С.М., Корнюшин П.Н. Хеш-цепи в многосторонних платежах // Материалы XLVIII Всероссийской межвузовской научно-технической конференции. - Владивосток: ТОВМИ, 2005. - С. 75-76.

6. Косолапов Д.О. Многосторонние микроплатежи и ведение счета клиента в мобильной сети // Сборник докладов региональной научно-технической конференции «Знание, творчество, профессионализм». - Владивосток: МГУ им. адм. Г.И. Невельского, 2005. - С. 418-422.

7. Косолапов Д.О., Гончаров С.М., Корнюшин П.Н. Криптосистемы на основе идентификационных данных для обеспечения безопасности информационного обмена в мобильной телефонии // Материалы 3-й Международной Научно-практической конференции «Интеллектуальные технологии в образовании, экономике и управлении». - Воронеж: ВИЭСУ, 2006. - С. 271-273.

8. Косолапов Д.О., Гончаров С.М. Оптимизация билинейного Тейт-спаривания в группе точек эллиптической кривой на базе алгоритма Миллера // Региональная конференция студентов, аспирантов и молодых ученых по физике. Тезисы докладов. - Владивосток: ДВГУ, 2006. - С. 168-169.

9. Косолапов Д.О. Возможности построения криптосистем на основе мультилинейных форм // Всероссийская конференция студентов, аспирантов и молодых ученых по физике. 14-16 ноября 2007. Материалы конференции. - Владивосток: ДВГУ, 2007. – С. 120-121.

10. Косолапов Д.О., Гончаров С.М., Корнюшин П.Н. Мультилинейные отображения и возможности построения новых криптосистем // Материалы 50-й Всероссийской научной конференции. Т. 2. - Владивосток: ТОВМИ, 2007. – С. 39-40.

11. Косолапов Д.О., Корнюшин П.Н. Обобщение билинейных криптосистем шифрования и подписи // Материалы IV международной научно-практической конференции «Интеллектуальные технологии в образовании, экономике и управлении 2007». - Воронеж: ВИЭСУ, 2007. - С. 285-288.

12. Косолапов Д.О., Гончаров С.М. Групповая мультилинейная схема электронно-цифровой подписи // XXXIII Дальневосточная математическая школа-семинар имени академика Е.В. Золотова: тезисы докладов. - Владивосток: Изд-во Дальнаука, 2008. – С. 18.

13. Косолапов Д.О., Харин Е.А., Гончаров С.М., Корнюшин П.Н. Генерация ключевых последовательностей на основе рисунка радужной оболочки глаза // Проблемы правовой и технической защиты информации: сб. научных статей. - Барнаул: Изд-во Алт. Ун-та, 2008. - С. 145-150.

14. Косолапов Д.О., Харин Е.А., Гончаров С.М., Корнюшин П.Н. Использование рисунка радужной оболочки глаза для генерации ключевой пары // Доклады Томского государственного университета систем управления и радиоэлектроники, 2(18), часть 1. - Томск: Изд-во ТГУСУР, 2008. - С. 30-31.

15. Косолапов Д.О., Харин Е.А., Гончаров С.М., Корнюшин П.Н. Мультилинейные протоколы в асимметричной криптографии // Доклады Томского государственного университета систем управления и радиоэлектроники, 2(18), часть 1. - Томск: Изд-во ТГУСУР, 2008. - С. 51-53.

16. Косолапов Д.О., Харин Е.А., Корнюшин П.Н. Мультилинейные криптосистемы шифрования, подписи и распределения ключей // Проблемы правовой и технической защиты информации: сб. научных статей. - Барнаул: Изд-во Алт. Ун-та, 2008. - С. 116-120.

17. Косолапов Д.О., Гончаров С.М., Корнюшин П.Н. Протокол ключевого соглашения на основе идентификационных данных с возможностью выявления злоумышленника // Всероссийская конференция студентов, аспирантов и молодых ученых по физике. 27-29 апреля 2009. Материалы конференции. – Владивосток: ДВГУ, 2009. – С. 109-111.

18. Косолапов Д.О. Протокол ключевого соглашения на основе идентификационных данных с возможностью выявления злоумышленника // Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых 12-15 мая 2009 г, Тематический выпуск «Системная интеграция и безопасность», ч. 3. – Томск: В-Спектр, 2009. - С. 277-283.

Личный вклад автора. Все основные результаты, представленные в диссертационной работе, получены автором самостоятельно. Работы [6, 9, 18] выполнены автором самостоятельно. В работах [2-5, 7, 8, 10-12, 15-17] автор участвовал в постановке проблемы, провел необходимые теоретические исследования, связанные с построением математических моделей безопасности и разработкой мультилинейных алгоритмов, и соответствующие вычисления, связанные с доказательством стойкости предложенных алгоритмов для решения задачи обеспечения безопасности группового информационного обмена. В работах [1, 13, 14] автор сформулировал возможность использования в многосторонних алгоритмах ключевых последовательностей на основе клавиатурного почерка и рисунка радужной оболочки глаза.

Косолапов Дмитрий Олегович

ПОСТРОЕНИЕ МНОГОСТОРОННИХ МУЛЬТИЛИНЕЙНЫХ АЛГОРИТМОВ В УСЛОВИЯХ РАЗЛИЧНЫХ МОДЕЛЕЙ БЕЗОПАСНОСТИ

Автореферат

Подписано в печать Усл. печ. л. 1,0. Уч.-изд. л. 0,83
Формат 60x84/16 Тираж 100 экз. Заказ 32.

Издано ИАПУ ДВО РАН, г. Владивосток ул. Радио, 5
Отпечатано участком оперативной печати ИАПУ ДВО РАН
г. Владивосток ул. Радио, 5