УДК 004.056.55

На правах рукописи

ОТАР ЕРЛАН ХАСЕНҰЛЫ

Разработка эффективных алгоритмов в асимметричных криптосистемах

05.13.01 – Системный анализ, управление и обработка информации

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Республика Казахстан
Алматы, 2010

Работа выполнена в Институте проблем информатики и управления Министерства образования и науки Республики Казахстан

Научные руководители: доктор технических наук,
профессор Айтчанов Б.Х.,
доктор технических наук
профессор Абдикаликов К.А.

Официальные оппоненты: доктор технических наук,
профессор Бейсенби М.А.

кандидат технических наук
доцент Буранбаева А.И.

Ведущая организация: Институт математики МОН РК

Защита диссертации состоится 18 ноября 2010г. в 14.30 часов на заседании объединенного диссертационного совета ОД 14.13.03 при Казахском Национальном техническом университете имени К.И.Сатпаева Министерства образования и науки Республики Казахстан по адресу:

050013, Республика Казахстан, г.Алматы, ул.Сатпаева, 22, нефтяной корпус, конференц-зал.

С диссертацией можно ознакомиться в библиотеке Казахского национального технического университета имени К.И.Сатпаева.

Автореферат разослан «__» октября 2010 года.

Ученый секретарь объединенного
диссертационного совета ОД 14.13.03
доктор технических наук, профессор Г.З.Казиев

ВВЕДЕНИЕ

Актуальность темы исследования. В настоящее время в связи с широким использованием компьютерных технологий во всех отраслях экономики, науки и техники перед разработчиками криптографических алгоритмов постоянно ставятся новые задачи. При этом потребности развивающихся телекоммуникационных сетей самого разнообразного применения, потребности обеспечения информационной безопасности в глобальной сети Internet, потребности банковских и других систем являются основными побудительными мотивами развития асимметричной криптографии.

Вопросам построения оптимальных по быстродействию алгоритмов и оптимизации алгоритмов, реализующих компьютерные технологии решения задач обработки и защиты информации, уделяется большое внимание зарубежных и отечественных ученых и специалистов. В этой связи нужно отметить работы Кули, Тьюки, Рабинера, Винограда, В.М.Амербаева, С.С.Агаяна, А.В.Воеводина, В.К.Задираки, С.С.Мельниковой, А.В.Ефимова, И.Е.Капорина, Шеннона, Диффи, Хеллмана, Райвеста, Шамира, Адельмана, В.В.Кульбы, Р.Г.Бияшева, И.А.Самаева, О.С.Олексюка, К.А.Абдикаликова и др.

Актуальность указанных вопросов обуславливается и тем, что с каждым годом усиливается поток задач с большим объемом обрабатываемой информации, требующих зачастую решение в реальном масштабе времени. Информационная безопасность является одним из основных элементов национальной безопасности, которая указана в качестве долгосрочного приоритета в Послании Президента страны народу Казахстана «Стратегия развития республики до 2030 года». Известно, что проблема обеспечения информационной безопасности носит комплексный характер и сочетает в себе нормативно-законодательные, организационные, программные, технические и другие меры. Кроме того, в Концепции информационной безопасности Республики Казахстан, принятой Советом безопасности Республики Казахстан, указывается на необходимость создания отечественной системы обеспечения информационной безопасности, разработки и оптимизации методов, моделей и алгоритмов защиты информации для различных уровней ее секретности с последующей их аппаратно-программной реализацией. При этом важными остаются и задачи выявления резервов оптимизации алгоритмов с требуемыми характеристиками качества решений и задачи выбора оптимальных алгоритмов, обеспечение качества их программной и аппаратурной реализаций.

В связи с вышеуказанным, соискателем были рассмотрены задачи по созданию, исследованию, оптимизации и реализации алгоритмов и методов шифрования, схем формирования электронной цифровой подписи, повышающих криптостойкость и эффективность алгоритмов.

Целью работы является разработка новых модификаций алгоритмов быстрого умножения многоразрядных чисел на основе ортогональных преобразований и алгоритмов вычисления остатка с подтверждением их эффективности по быстродействию, новых модификаций эффективных алгоритмов решения задач защиты информации и электронной цифровой подписи с описаниями их компьютерных технологий, выявление резервов оптимизации реализаций алгоритмов при соответствующих компьютерных технологиях решения основных задач обработки данных с учетом моделей вычислений, получение оценок основных характеристик рассмотренных алгоритмов и разработка их математического обеспечения с проверкой эффективности на практике.

Задачами исследования являются:

- разработка новых быстрых алгоритмов умножения многоразрядных чисел с соответствующими обоснованиями их оптимальности;
- исследование резервов выбора эллиптических кривых для оптимизации шифрования с открытым ключом и для построения криптографических алгоритмов и протоколов подписи «вслепую»;
- рассмотрение модификаций эффективных алгоритмов решения задач защиты информации на базе алгоритма RSA;
- исследование практических аспектов вопросов обеспечения безопасности конфиденциальной информации в различных объектах;
- получение оценок основных характеристик рассмотренных алгоритмов и разработка соответствующих программных обеспечений.

Объект исследования: алгоритмы умножения многоразрядных чисел на основе ортогональных преобразований; алгоритмы шифрования с открытым ключом и подписи «вслепую» на основе эллиптических кривых; системы защиты конфиденциальной информации в организациях.

Предмет исследования:

- модифицированные алгоритмы умножения многоразрядных чисел на основе быстрых преобразований Фурье и быстрых вейвлет-преобразований;
- схемы использования подхода на основе эллиптических кривых для оптимизации шифрования с открытым ключом и подписи «вслепую»;
- модификации эффективных алгоритмов решения задач защиты информации на базе алгоритма RSA.

Методы исследования. При выполнении исследований по данной диссертационной работе были использованы положения теории вероятностей, конечных полей, модулярной арифметики и высшей алгебры.

Научная новизна работы заключается в следующем:

– разработаны новые модификации алгоритмов умножения многоразрядных чисел на основе быстрых преобразований Фурье и быстрых

вейвлет-преобразований с обоснованием их оптимальности по порядку по быстродействию;

– предложены способы оптимизации некоторых быстрых алгоритмов вычисления остатка, отличающихся своими предвычислениями, поствычислениями и временными показателями по реализации;

– рассмотрена возможность использования подхода на основе эллиптических кривых для оптимизации шифрования с открытым ключом и подписи «вслепую», обеспечивающей подписание сообщения, текст которого неизвестен подписывающему;

– разработан многопользовательский вариант системы защиты алгоритма RSA с модулем, равным произведению трех простых чисел;

– предложена эффективная система защиты информации для достижения целенаправленного предотвращения потенциального ущерба интересам организации, основанная на системном подходе к защите конфиденциальной информации;

– разработаны библиотеки программ, реализующих рассмотренные алгоритмы решения задач и подтверждающих оптимальность разработанных компьютерных технологий.

Положения, выносимые на защиту:

- модификации алгоритмов умножения многоразрядных чисел с помощью быстрых преобразований Фурье и вейвлет-преобразований;
- способы использования подхода на основе эллиптических кривых в алгоритмах шифрования и подписи «вслепую»;
- многопользовательский вариант схемы RSA-защиты для обмена информацией между тремя пользователями;
- эффективная система защиты конфиденциальной информации в различных организациях, основанная на системном подходе к безопасности информации.

Теоретическая и практическая значимость полученных результатов.

Полученные в диссертации теоретические результаты развивают научные основы криптографии и расширяют теорию построения эффективных алгоритмов асимметричных криптосистем.

Практическая значимость полученных результатов заключается в:

– разработке программных комплексов для реализации предложенных новых модификаций умножения многоразрядных чисел, вычисления остатка, шифрования с открытым ключом на основе использования эллиптических кривых и возможности их использования для защиты данных при их хранении и передаче в информационно-телекоммуникационных системах электронного правительства, электронного голосования, дистанционного обучения;

– реализации полученных результатов работы в практике работы Управления Центра обеспечения правительственной связи Комитета национальной безопасности Республики Казахстан по Актюбинской области

и в учебном процессе на физико-математическом факультете Актюбинского государственного университета имени К.Жубанова (курс лекций и лабораторный практикум «Основы защиты информации»);

– выполнении научно-исследовательских работ по разделу «Комплексное обеспечение безопасности информационных космических технологий» по теме «Разработка технологических основ создания и применения спутниковых информационно-телекоммуникационных систем и обеспечения их безопасности» Государственной программы «Развитие космической деятельности в Республике Казахстан на 2005-2007 годы».

Апробация работы. Основные результаты диссертационной работы докладывались и обсуждались на научном семинаре ДГД «Институт проблем информатики и управления» МОН РК под руководством д.ф.-м.н., профессора Бияшева Р.Г., на объединенном семинаре физико-математического факультета АГУ имени К.Жубанова и Института кибернетики имени В.М.Глушкова НАН Украины под руководством д.ф.-м.н., профессора Задираки В.К. и д.т.н., профессора Абдикаликова К.А., на международных конференциях «Проблемы дифференциальных уравнений, анализа и алгебры» (г.Актобе, 2006г., 2009г.), «Современные проблемы математики, информатики и управления», посвященной 60-летию д.ф.-м.н., профессора, академика Международной академии информатизации М.Б.Айдарханова (г.Алматы, 2008г.), «Актуальные проблемы математики, информатики, механики и теории управления» (г.Алматы, 2009г.), на республиканской научной конференции молодых ученых «Жас ғалым» (г.Астана, 2009г.), на «II, III Ержановских чтениях» (г.Актобе, 2007г., 2010г.).

Связь темы с планами научно-исследовательских программ. Диссертационная работа выполнялась в соответствии с планами научных и прикладных работ лаборатории информационной безопасности Института проблем информатики и управления МОН РК в рамках тем следующих программ научных исследований МОН РК:

1. «Разработка технологических основ создания и применения спутниковых информационно-телекоммуникационных систем и обеспечения их безопасности» (№ госрегистрации 0105РК00189) Государственной программы «Развитие космической деятельности в Республике Казахстан на 2005-2007 годы»;
2. «Разработка и исследование технологий защиты информации, базирующихся на модулярной арифметике» (№ госрегистрации 0106РК00524) программы фундаментальных исследований «Разработка и исследование моделей, методов и алгоритмов создания защищенных и интеллектуальных информационных технологий» (ПФИ, 2006-2008г.г., шифр Ф.0369-8).

Публикации. По результатам исследований опубликовано 17 работ, в том числе 5 в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МОН РК, 10 статей в международных конференциях.

Структура работы. Работа изложена на 123 страницах, состоит из введения, трех разделов, заключения, списка использованных источников, который включает 81 наименований, и 2 приложений.

ОСНОВНАЯ ЧАСТЬ

Во введении обоснована актуальность темы исследования и ее важность при решении задач обработки информации и информационной безопасности, сформулированы цель и задачи работы, основные научные положения, выносимые на защиту, научная новизна и практическая ценность полученных результатов. Приведены сведения о реализации результатов работы, об их апробации, связи с планами научных работ, публикациях, структуре диссертации.

В первом разделе приводятся основные характеристики вычислительных алгоритмов решения задач обработки и защиты информации, к которым относятся время, необходимое для решения рассматриваемой задачи на компьютере и мера полной погрешности решения задачи при использовании соответствующего алгоритма, и формулировки основных задач оптимизации алгоритмов по различным критериям, заключающихся в минимизации одной из указанных характеристик при соблюдении определенных ограничений на другие.

Так как поддержание и обеспечение надежного функционирования механизмов системы защиты информации сопряжено с решением специфических задач, решения которых могут гарантировать надежность используемых алгоритмов и программных средств, реализующих функции защиты информации, то вопросы построения оптимальных по быстродействию алгоритмов, реализующих компьютерные технологии решения задач обработки информации и информационной безопасности, и оптимизации по быстродействию известных алгоритмов решения задач цифровой обработки сигналов постоянно сохраняют свою актуальность.

В связи с этим приведены обзор и анализ ряда моделей вычислений для их высокой производительности и указаны основные направления исследований, связанные с разработкой новых модификаций криптографических алгоритмов и выявлением резервов оптимизации вычислений.

Второй раздел работы посвящен вопросам оптимизации по быстродействию алгоритмов быстрого умножения многоразрядных чисел, которые используются при разработке криптографических методов защиты информации с открытым ключом и имеют свои области эффективного применения в зависимости от области значений длины слова.

Это связано, прежде всего, с тем, что необходимо быстро выполнять арифметические операции над числами, разрядность которых превышает длину разрядного слова и составляет 180-200 десятичных знаков, и, тем самым, повысить производительность двухключевой криптографии.

Так как произведение двух многоразрядных чисел является, без учета переносов, циклической сверткой двух сомножителей, то метод умножения многоразрядных чисел с помощью быстрых преобразований Фурье, предложенный Штрассеном, основываются на использовании теоремы о дискретной свертке двух функций.

Пусть A(x)– полином степени $l-1$, т.е. $A(x)=\sum_{i=0}^{l-1} A_i x^i$, и $\omega-$ примитивный l-й корень из единицы. Тогда, чтобы получить полиномиальные значения $A(\omega^i)$ для $i=0,1,...,l-1$ алгоритм БПФ вычисляет произведение матрицы на вектор:

$$\begin{bmatrix} A(1) \\ A(\omega) \\ \dots \\ A(\omega^{i-1}) \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{i-1} \\ \dots & \dots & \dots & \dots \\ 1 & \omega^{i-1} & \dots & \omega^{(i-1)(i-1)} \end{bmatrix} \begin{bmatrix} A_0 \\ A_1 \\ \dots \\ A_{i-1} \end{bmatrix}$$

Значения $A(\omega^i)$, i $=0,1,...,l$ -1, однозначно определяют полином A(x). По ним коэффициенты A_i могут быть найдены с помощью обратного преобразования Фурье.

После раскрытия основных деталей метода дано пошаговое описание алгоритма умножения целых чисел на основе БПФ, работающего над произвольным полем, в котором существует l-й корень из единицы. Даны априорные оценки количества операций умножения и сложения.

При этом для реализации шагов вычисления дискретного преобразования и обратного дискретного преобразования Фурье предлагается использование модификации алгоритма БПФ с предварительной заготовкой элементов матрицы преобразования, так как заготовка таблицы корней ДПФ, рассчитанной на N_{max} (например, с $N=512$), с q верными значащими цифрами значительно сокращает время реализации рассмотренного алгоритма умножения и уменьшает оценку округления.

В этом разделе рассмотрена и возможность применения вейвлет-преобразований к построению эффективных алгоритмов, в частности, алгоритма умножения многоразрядных чисел с целью сокращения количества необходимых вычислений.

Известно, что за последние десятилетия вейвлет-преобразования как математический инструмент усиленно начали конкурировать с преобразованиями Фурье, особенно в вопросах анализа и обработки нестационарных или неоднородных сигналов разных типов с характерными частотами и локальными координатами, при которых эти частоты проявляют себя. В вейвлет-анализе, так же как и в Фурье-анализе, исследуемый процесс представляется в виде линейной комбинации функций, образующих базис соответствующего преобразования. Вейвлет-преобразование одномерного сигнала состоит в его разложении по базису, сконструированному по обладающей определенными свойствами солитоноподобной функции (вейвлета) посредством масштабных изменений и переносов. Каждая из

функций этого базиса характеризует как определенную пространственную (временную) частоту, так и ее локализацию в физическом пространстве (времени). В результате появляется возможность анализировать свойства сигнала одновременно в физическом и в частотном пространствах. В этом заключается отличие вейвлет-преобразования от традиционно применяемого анализа сигналов преобразования Фурье.

Основная часть работ, касающихся практического использования вейвлет-преобразования, содержит результаты расчетов, в которых применяются дискретные вейвлеты. Это предпочтение связано с тем, что используемые базисы на основе непрерывных вейвлетов не всегда являются ортонормированными. С дискретными вейвлетами этих проблем не возникает. Поэтому они приводят обычно к более точному преобразованию и представлению сигнала и к его обратному восстановлению после процедуры сжатия.

Так как вейвлет-преобразования хорошо приспособлены для быстрого численного алгоритма, использующего процедуру БПФ, то большой интерес представляет применимость вейвлет-преобразований (особенно, дискретных) к построению эффективных алгоритмов.

В разделе обсуждается подход использования пирамидального алгоритма дискретного вейвлет-преобразования с ортогональным базисом для быстрого умножения многоразрядных чисел. Вейвлет-преобразования обеспечивают быстрые пирамидальные алгоритмы вычисления вейвлет-коэффициентов, требующихся для завершения только $O(N)$ операций.

При этом для вычисления коэффициентов $\mathrm{C_{jk}}$ разложения функции из пространства $L_2(R)$ в равномерно сходящийся ряд $f(t) = \sum_{j,k=-\infty}^{\infty} C_{jk}\varphi_{jk}(t)$ по ортонормированному базису $\varphi_{\mathrm{jk}} = 2^{\frac{j}{2}}\varphi(2^j t - k),\ j,k \in Z$, с базисным вейвлетом $\varphi(t)$, локализованной функцией из $L_2(R)$ с носителем [a, b], определяются с помощью вейвлет-преобразования как скалярное произведение:

$$\mathrm{C_{jk}} = \int_{-\infty}^{\infty} f(t)\varphi_{jk}(t)dt,\ \ j,k \in Z\ .$$

Кроме того, в разделе сделан сравнительный анализ вычислительной сложности алгоритмов умножения многоразрядных чисел на основе априорных оценок количества вычислительных затрат для их реализаций.

В этом разделе рассмотрен и вопрос об оптимизации эффективных алгоритмов выполнения базисной операции модулярной арифметики – вычисления остатка от деления одного целого числа на другое. Среди них особое внимание уделено методу Монтгомери, более удобному и быстрому при выполнении быстрых арифметических действий по модулю степени двойки и заменяющему деление на n делением на степень двойки, которая легко выполняется на компьютере, благодаря двоичному представлению.

При этом в этом алгоритме рассматривается более быстрая процедура умножения при вычислении n-вычета произведения двух целых чисел, у

которых даны их n-вычеты, а произведение Монтгомери по данным n-вычетам чисел $\bar{a}$ и $\bar{b}$ определяется как n-вычет:

$$\bar{R} = \bar{a} \cdot \bar{b} \cdot r^{-1} \bmod n,$$

где r^{-1} – инверсия числа r по модулю n, и является n-вычетом произведения

$$R = a \cdot b \bmod n.$$

Описание рассмотренного алгоритма вычисления остатка осуществлено посредством введения величины n', являющейся целым числом, удовлетворяющим условию: $r \cdot r^{-1} - n \cdot n' = 1$.

Для ускорения вычисления n' рассмотрена упрощенная программа $Mon\,\mathrm{Pro}$, использующая умножение с одинарной точностью при перемножении t и n', где $t = \bar{a} \cdot \bar{b}$, и специализированный алгоритм Евклида вместо общего расширенного алгоритма Евклида.

Результаты сравнения сложности некоторых алгоритмов вычисления остатка и некоторых известных программ приведены в нижеследующих таблицах 1-2, где в обозначении K(A,B) коэффициенты ускорения: A – алгоритм вычисления остатка, B – алгоритм умножения.

Таблица 1 – Сложность алгоритмов нахождения остатка

Операция	***Стандартный***	***Монтгомери***
Умножение	$n(n+2.5)$	$n(n+1)$
Деление	n	0

Таблица 2 – Сравнение программ для вычисления остатка

n	***K(VI,IIIa)***	***K(DIL,MD)***	***K(MOD, MD)***	***K(K,Б)***	***K(B,Б)***	***K(M,Б)***
1	2	3	4	5	6	7
8	1.71	1.85	1.63	1.43	1.61	1.110
32	1.68	1.28	1.23	1.21	1.11	1.019
64	1.61	1.19	1.16	1.15	1.02	1.013

Из этих результатов следует, что без учета предварительных и дополнительных вычислений, наиболее быстрым является алгоритм Монтгомери, который дает лучшие временные показатели и при применении для вычисления экспоненциальной модулярной функции.

В третьем разделе рассмотрены некоторые модификации эффективных алгоритмов решения задач защиты информации и электронной цифровой подписи.

Известно, что в современных условиях взаимного недоверия субъектов информационных систем защита информации обеспечивается на основе криптографических методов с открытым ключом с широкими функциональными возможностями, которые получают все большее применение в системах передачи и обработки информации и

рассматриваются как перспективное направление аутентификации и шифрования данных.

Обобщенная модель асимметричной криптосистемы с открытым ключом выглядит следующим образом:

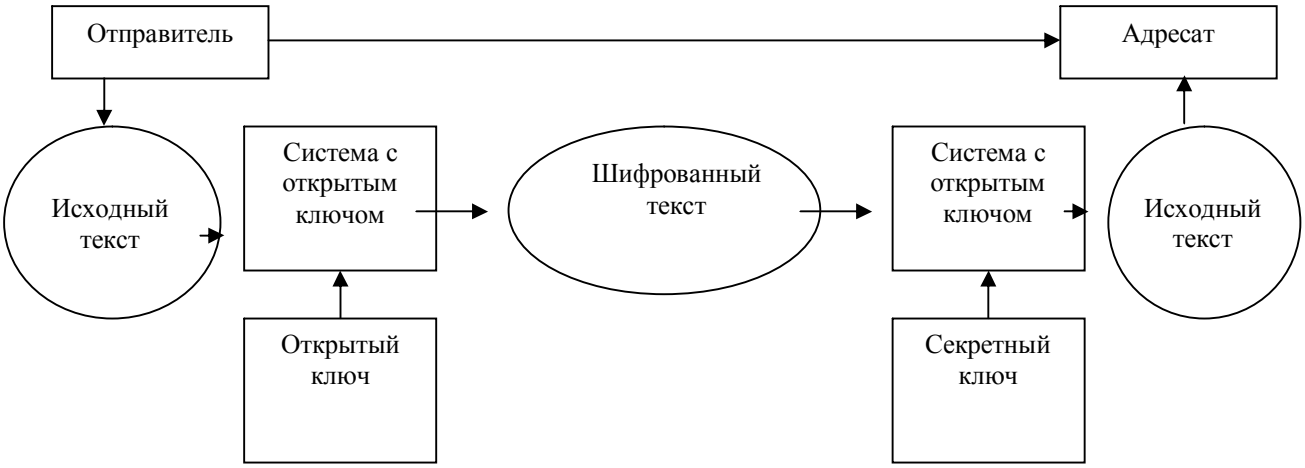

Рисунок 1 - Обобщенная модель асимметричной криптосистемы с открытым ключом

Исходный текст шифруется открытым ключом адресата и передается ему. Дешифрование этого текста возможно с использованием секретного ключа, известного только адресату.

Разнообразие асимметричных систем порождается множеством классов, так называемых односторонних (или однонаправленных, или необратимых) функций $f(x)$, обладающих следующим свойством:

по заданному x значение $f(x)$ вычисляется просто, а вычисление значения x из заданного равенства $f(x) = y$ – непросто.

Основными требованиями к системам с открытым ключом для надежной защиты информации являются:

а) необратимость преобразования исходного текста и невозможность восстановления текста с помощью открытого ключа;

б) невозможность на современном технологическом уровне определения секретного ключа на основе открытого ключа.

Современная асимметричная криптосистема опирается на один из следующих односторонних преобразований:

– разложение больших чисел на простые множители;

– вычисление логарифма на конечном поле;

– нахождение корней алгебраических уравнений,

и может быть использована как самостоятельное средство защиты данных, как средство распределения ключей и как средство аутентификации пользователей.

Среди теоретических и практических проблем, связанных с наиболее распространенными алгоритмами асимметричной криптографии, больше внимания обращают на себя вопросы применения схемы открытого шифрования RSA и построенные на ее основе схемы подписи и аутентификации, схем подписи типа Эль-Гамаля и некоторых других схем.

Сначала рассмотрена одна модификационная версия алгоритма RSA-MOD-1 с соответствующей компьютерной технологией, отличающаяся от известного алгоритма тем, что для более быстрого выполнения модульного возведения в степень, необходимого при зашифровании и расшифровании, предлагается использование алгоритма Монтгомери, бинарного метода и Китайской теоремы об остатках.

Далее, рассмотрена схема реализации многопользовательского варианта RSA-защиты, предназначенная для обмена информацией между несколькими пользователями. А именно, в случае, когда модуль N равен произведению трех простых чисел, т.е.

$$\mathrm{N} = \mathrm{P}_1 \cdot \mathrm{P}_2 \cdot \mathrm{P}_3,\ m = \varphi(\mathrm{N}) = (\mathrm{P}_1 - 1)(\mathrm{P}_2 - 1)(\mathrm{P}_3 - 1),$$

выбирается один открытый ключ $K_e = \{L, \mathrm{N}\}$, два секретных ключа $K_{d_1} = \{S_1, \mathrm{N}\}$ и $K_{d_2} = \{S_2, \mathrm{N}\}$, исходя из условия: $L \cdot S_1 \cdot S_2 = 1 (\mathrm{mod}\, \mathrm{N})$, тем самым, общий секретный ключ S разделяется на две части S_1 и S_2, что имеет существенное значение в тех случаях, когда пользователи не доверяют друг другу.

Тогда после шифрования исходного текста с помощью открытого ключа посредством функции шифрования вида

$$\mathrm{X(t)} = \mathrm{t}^{\mathrm{L}} (\mathrm{mod}\, \mathrm{N})$$

криптограмма E_1, полученная от первого пользователя в виде последовательности чисел, преобразуется вторым пользователем с помощью ключа K_{d_1} в криптограмму E_2, которую третий пользователь преобразует ключом K_{d_2} и получает исходный открытый текст.

В разделе уделено внимание и к вопросу оптимизации алгоритма схемы Эль-Гамаля, используемой как для шифрования, так и для цифровых подписей. Дано поэтапное описание соответствующего алгоритма и его компьютерная технология с учетом оптимизации. При этом удается избежать слабости алгоритма цифровой подписи RSA, связанной с возможностью подделки цифровой подписи под некоторым сообщением без определения секретного ключа. Рассмотрен пример, подтверждающий тот факт, что схема Эль-Гамаля допускает пересылку сообщения в открытой форме с присоединенным аутентификатором и при заданном уровне стойкости алгоритма целые числа, участвующие в вычислениях, имеют записи на четверть короче, что уменьшает сложность вычислений почти вдвое, сократив тем самым объем используемой памяти компьютера.

Особое место в разделе занимает вопрос об использовании подхода на основе эллиптических кривых для оптимизации шифрования с открытым ключом и создания подписей “вслепую”. Данный подход является наиболее перспективным среди криптографических систем с открытым ключом, что

связано с тем, что использование эллиптических кривых обеспечивает эквивалентную защиту при очень небольшом числе разрядов и уменьшает загрузку процессора.

Исходя из протоколов Диффи-Хеллмана и Эль-Гамаля рассмотрен метод шифрования с использованием эллиптических кривых и дано пошаговое описание соответствующего алгоритма. При этом для зашифрования сообщения $\mathrm{M}, 0 \le \mathrm{M} \le \mathrm{r}\text{-}1$, $\mathrm{r}-$ простой порядок группы с образующей Q из совокупности $\{Q, P\}$, являющейся открытым ключом зашифрования, где $P-$ точка из этой группы, отправитель генерирует случайное число – показатель $k, 0 \le k \le r-1$, вычисляет точку $R = kQ$ и криптотекст $C = \mathrm{M} + \mathrm{c} (\mathrm{mod r})$. Здесь: $c = h(kP), h-$ некоторая хэш-функция от координат точки kP.

Для расшифрования криптотекста $\{R, C\}$ получатель умножает точку R на число l, являющееся секретным ключом, т.е. получает $lR - klQ = kP$, вычисляет $c = h(lR)$, и находит исходный текст: $\mathrm{M} = C - c (\mathrm{mod}\, r)$.

Известно, что протокол Эль-Гамаля для обычной подписи на эллиптической кривой, заключающийся в вырабатывании подписывающей стороной случайного показателя k, вычислении точки $R = kQ$ и решении относительно S сравнения по модулю порядка группы $m = lh(R) + kS$, поддается эффективному изменению для обеспечения возможности подписи “вслепую”. Протокол подписи “вслепую” должен обеспечивать возможность подписи сообщения, текст которого не известен подписывающему. При этом в основе безопасности протоколов лежит задача логарифмирования в группе точек кривой.

В разделе дано описание протокола подписи “вслепую” на эллиптической кривой над конечным полем, основанного на протоколе Эль-Гамаля, который опирается на существование категорного морфизма.

Так как подпись “вслепую” используется, в основном, в протоколах электронных платежей, основанных на использовании электронной “монеты” – информации, не имеющей трудно подделываемого воплощения в отличие от обычных денег, то с помощью данного протокола подпись “вслепую” выполняется банком для уникального номера монеты, известного только ее владельцу.

Далее рассмотрен алгоритм, позволяющий передавать сообщение по открытому каналу связи без предварительной передачи какой бы то ни было ключевой информации, и являющийся аналогом ящика, запираемого на один или два замка.

В качестве замков участники A и B используют ключи (d_A, e_A), (d_B, e_B), для организации которых используется большое простое число p – открытый параметр.

При этом алгоритм генерации ключей схематично выглядит так:

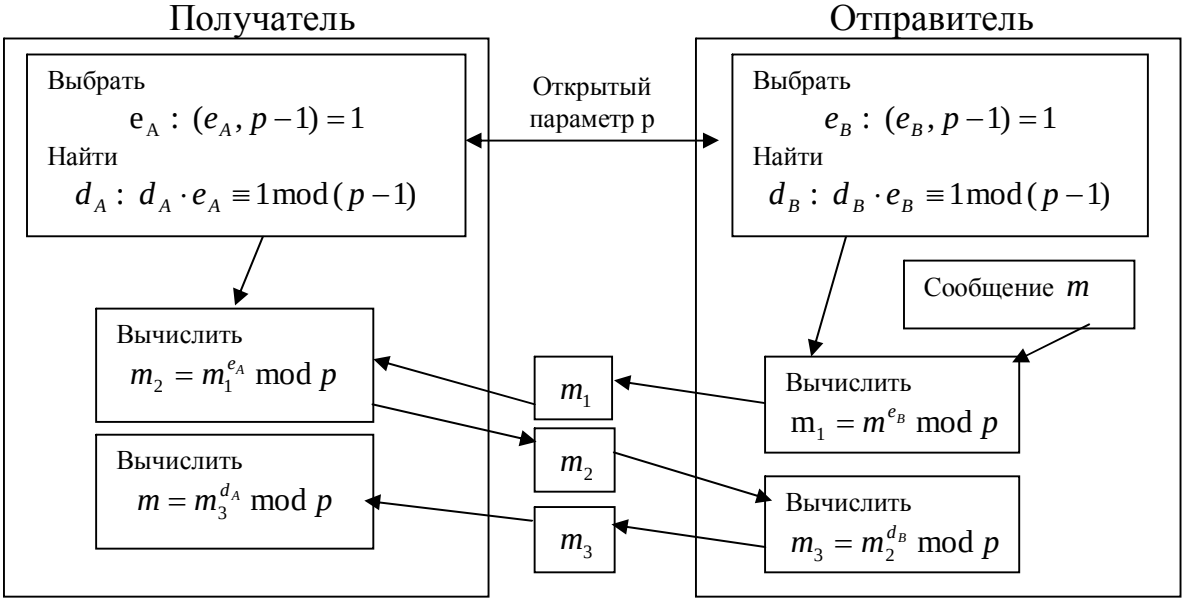

Рисунок 2 - Алгоритм генерации ключей

Таким образом, в алгоритме процедура шифрования представляет собой процесс последовательного “навешивания замков” на открытый текст отправителем и получателем, путем шифрования по схеме $m_i = m_{i-1} \bmod p$. При этом, благодаря свойству пары ключей-замков (d_A, e_A): $m^{e_A d_A} = m$, $0 < m < p$ имеет место: $m_3 = m$. Поэтому криптоаналитик не сможет вскрыть открытый текст m по известным ему значениям m_1, m_2 и m_3 из-за трудоемкости решения задачи вычисления дискретного логарифма.

В связи с тем, что на практике нередко для получения быстрого шифрования в сочетании с удобным распределением ключей асимметричные криптосистемы применяются в комбинировании с симметричными, рассмотрена реализация комбинирования алгоритма DES-3 тройного шифрования с тремя ключами и модифицированного алгоритма RSA-MOD-1, являющегося более эффективным по быстродействию.

В разделе также рассмотрен вопрос повышения эффективности алгоритмов электронной цифровой подписи, являющейся неотъемлемой частью применения криптографии с открытым ключом. Предложена схема, согласно которой зашифрование окончательного результата обработки электронного документа хэш-функцией осуществляется при помощи асимметричного алгоритма. Обсуждены возможности применения основных алгоритмов слепой подписи, цель которой состоит в препятствовании подписывающей стороне ознакомиться с сообщением, которое она подписывает, и с соответствующей подписью под этим сообщением.

В разделе рассмотрены практические аспекты обеспечения конфиденциальной информации, которым должно быть обращено внимание заинтересованных специалистов, с позиции системного подхода к защите информации, и даны рекомендации по реализации соответствующей функциональной структуры.

ЗАКЛЮЧЕНИЕ

По итогам исследований диссертационной работы получены следующие основные результаты:

– разработаны модификации алгоритмов быстрого умножения многоразрядных чисел на основе использования быстрых преобразований Фурье и на основе быстрых вейвлет-преобразований с указанием оценок их основных характеристик и с обоснованием их оптимальности по порядку по быстродействию;

– предложены способы оптимизации ряда известных быстрых алгоритмов вычисления остатка (деления с восстановлением, деления без восстановления, Blakey, Монтгомери), отличающихся друг от друга своими предвычислениями, поствычислениями и временными показателями по реализации;

– разработаны некоторые модификации известных алгоритмов асимметричных криптосистем RSA и Эль-Гамаля, а именно, модификация алгоритма RSA-MOD-1 с подробным описанием технологической схемы реализации, многопользовательский вариант системы защиты алгоритма RSA в случае, когда модуль равен произведению трех простых чисел и модифицированный вариант алгоритма цифровой подписи Эль-Гамаля, допускающий пересылку сообщения в открытой форме вместе с присоединенным аутентификатором;

– рассмотрены возможности использования подхода на основе эллиптических кривых для оптимизации шифрования с открытым ключом и подписи “вслепую”, обеспечивающей возможность подписи сообщения, текст которого не известен подписывающему;

– приведен сравнительный анализ вычислительной сложности рассмотренных алгоритмов асимметричных криптосистем с указанием недостатков и преимуществ последовательности действий сторон, обменивающихся информациями, при использовании того или иного способа обмена;

– разработана схема для повышения эффективности алгоритма электронной цифровой подписи, которая осуществляет зашифрование окончательного результата обработки электронного документа хэш-функцией при помощи асимметричного алгоритма;

– предложена эффективная система защиты информации для достижения целенаправленного предотвращения потенциального ущерба интересам той или иной акционерной или коммерческой организации, основанная на системном подходе к защите конфиденциальной информации, и даны рекомендации по реализации технологии обеспечения защиты информации;

– на основе предложенных алгоритмов разработано программное обеспечение для решения задач обработки информации и информационной безопасности, осуществлено его внедрение в ряде организаций. Имеются акты о внедрении результатов исследований.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Абдикаликов К.А., Абдикаликова Н.И., Отар Е.Х. Смарткарты и персональные компьютеры – технологии будущего // IV Междунар. науч. конф. «Проблемы дифференциальных уравнений, анализа и алгебры». (Актобе, 18-21 октября 2006г.). Тез. докл. – Актобе, 2006 – С. 122-123;
2. Абдикаликов К.А., Отар Е.Х. Об особенностях применения схем подписи «вслепую» // Матер. IV Междунар. науч. конф. «Проблемы дифференциальных уравнений, анализа и алгебры». – Актобе. 2006. – С. 3-6;
3. Абдикаликов К.А., Абдикаликова Н.И., Отар Е.Х. Построение систем защиты информации на базе асимметричных алгоритмов // Матер. Междунар. науч.-техн. конф. «II Ержановские чтения». – Актобе, 2007. – С. 332-335;
4. Абдикаликов К.А., Отар Е.Х. О вейвлет-преобразованиях и их применениях // Матер. Междунар. науч. конф. «Современные проблемы математики, информатики и управления», посвящ. 60-летию д.ф.-м.н., проф., акад. Междунар. академии информатизации М.Б.Айдарханова. – Алматы, Институт проблем информатики и управления, 2008. – С. 237-239;
5. Абдикаликов К.А., Абдикаликова Н.И., Отар Е.Х. Информационная безопасность электронных банковских систем // Вестник Каз. нац. ун-та им. Аль-Фараби. Сер. мат., мех., информат. – Алматы, 2008.– № 4 (59). – С. 121-124;
6. Абдикаликов К.А., Отар Е.Х. К вопросам применения схем электронной подписи // Междунар. науч. альманах. – Галле-Москва-Минск-Бишкек-Актобе, 2009. – № 4. – С. 250-252;
7. Отар Е.Х. О способах применения блочных шифров к решению задач аутентификации данных // Междунар. науч. альманах. – Таганрог-Актюбинск, 2009. – № 6. – С. 259-261;
8. Абдикаликов К.А., Отар Е.Х. Многопользовательский вариант системы защиты алгоритма RSA // Матер. V Междунар. конф. – Актобе, 2009. – С. 354-356;
9. Отар Е.Х. Об алгоритмической реализации схемы слепой подписи на основе асимметричной криптографии // Матер. Междунар. конф. «Актуальные проблемы математики, информатики, механики и теории управления». – Алматы, 2009. – С. 306-308;
10. Отар Е.Х. Об алгоритмической реализации схемы слепой подписи на основе системы RSA-M // Вестник Актюб. гос. ун-та им. К.Жубанова. – Актобе, 2009. – № 3 (40). – С. 47-50;
11. Отар Е.Х. Об использовании эллиптических кривых для построения метода шифрования с открытым ключом // Вестник науки Костан. соц.-техн. ун-та им. акад. Зулхарнай Алдамжар. Сер. естест.-техн. наук. – Костанай, 2009. – № 4. – С. 232-236;

12. Отар Е.Х. Об одной функциональной структуре технологии обеспечения безопасности информации // Вестник науки Костан. соц.-техн. ун-та им. акад. Зулхарнай Алдамжар. Сер. естест.-техн. наук. – Костанай, 2009. – № 4. – С. 159-162;
13. Отар Е.Х. Схема слепой подписи на основе асимметричных криптосистем // Вестник Каз. нац. ун-та им. Аль-Фараби. Сер. мат., мех., информат. – Алматы, 2009. – № 5 (64). – С. 164-166;
14. Отар Е.Х. О применении эллиптических кривых в алгоритмах слепой подписи // Науч. журнал «Ізденіс-Поиск». Сер. естест. и техн. наук. – Алматы, 2010. – № 1. – С. 182-185;
15. Отар Е.Х. Модифицированная криптографическая система Месси-Омуры // Матер. Междунар. науч.-техн. конф., посвящ. 20-летию Нац. инженер. академии РК. Ч. 2. – Актобе, 2010. – С. 243-246;
16. Абдикаликов К.А., Задирака В.К., Отар Е.Х. Технологическая схема решения задач с заданными характеристиками качества // Матер. Междунар. науч.-техн. конф., посвящ. 20-летию Нац. инженер. академии РК. Ч. 2. – Актобе, 2010. – С. 14-16;
17. Абдикаликов К.А., Айтчанов Б.Х., Отар Е.Х. Проблемы защиты информации в компьютерных системах // Вестник Актюб. гос. ун-та им. К.Жубанова. – Актобе, 2010. – № 3 (44). – С. 64-71.

ТҮЙІН
Отар Ерлан Хасенұлы

АСИММЕТРИЯЛЫҚ КРИПТОЖҮЙЕЛЕРДЕ ЭФФЕКТИВТІ АЛГОРИТМДЕРДІ ҚҰРУ

05.13.01 – Жүйелі талдау, басқару және ақпаратты өңдеу
"Техника ғылымдарының кандидаты" ғылыми дәрежесін алу үшін дайындалған диссертация

Зерттеу барысында төмендегідей нәтижелер алынды:

- Фурьенің жылдам түрлендірулері және жылдам вейвлет-түрлендірулер негізінде көпразрядты сандарды жылдам көбейту алгоритмдерінің жекелеген өзгертулері құрылды, олардың негізгі сипаттамалары берілді;
- асимметриялық RSA және Эль-Гамаль жүйелерінің белгілі алгоритмдерінің кейбір модифкациялары, мысалы, RSA қорғаныс жүйесінің тұтынушылар саны үшеу болған жағдайдағы нұсқасы, цифрлік қолтаңбаның Эль-Гамаль алгоритмінің хабарламаны ашық түрде аутентификатормен бірге жіберуге мүмкіндік беретін бір нұсқасы құрылды;
- ашық кілтпен шифрлау және мәтіні қол қоюшыға белгісіз хабарлама үшін "соқыр" қолтаңба алу процедураларын эллиптикалық қисықтарды қолдану негізінде жетілдіру мүмкіндіктері қарастырылып, тиімді тәсілдері көрсетілді;
- қарастырылған алгоритмдердің есептеу қиындықтарына салыстырмалы талдаулар жасалды, ақпарат алмасушы жақтардың іс-әрекеттері реттерінің артықшылықтары мен кемшіліктері көрсетілді;
- электрондық құжатты өңдеудің түпкі нәтижесін хэш-функция арқылы шифрлауды асимметриялық алгоритм арқылы жүзеге асыратын электрондық цифрлік қолтаңба алгоритмін жетілдіру схемасы құрылды;
- құпия ақпаратты қорғауға жүйелік тұрғыдан көзқарас негізінде коммерциялық немесе қаржылық мекеме мүддесіне нұқсан келтірілуінің алдын-алу смақсатында қолданыла алатын ақпараттық қорғау жүйесі ұсынылды;
- ақпараттық қорғаудың және электрондық цифрлік қолтаңбаның қарастырылған алгоритмдерінің және оларға сәйкес компьютерлік технологиялардың тиімділіктерін негіздейтін бағдарламалық кітапхана құрылды;
- ұсынылған алгоритмдер негізінде ақпаратты өңдеу мен ақпараттық қауіпсіздік мәселелерін шешуге арналған бағдарламалық қамтамасыздандыру құрылып, оны бірқатар мекемелерге ендіру жұмысы іске асты. Зерттеу нәтижелерін ендіру актілері алынды.

SUMMARY
Otar Erlan Khassenuly

WORKING OUT OF EFFECTIVE ALGORITHMS IN ASYMMETRIC CRYPTOSYSTEMS

05.13.01 – System analysis, control and information processing
Dissertation is presented for the degree of candidate of technical sciences

The basic scientific results of dissertational work, practical conclusions and recommendations, received at performance of researches are consist in the following:

– developed modifications of algorithms of fast multiplication of multidigit numbers on the basis of use of fast transformations of Fure and on the basis of fast weivlet-transformations with instructions of estimations of their basic characteristics and with a substantiation of their optimality one after another on speed;

– specified ways of optimization of some known fast algorithms of calculation of the rest (division with restoration, divisions without restoration, Blakey, Montgomery), different from each other the recalculations, a post calculations and time indicators on realization;

– developed some updating of known algorithms of RSA and El-Gamal asymmetric cryptosystems, namely, updating of algorithm RSA-MOD-1 with the detailed description of the technological scheme of realization, the multi-user variant of system of protection of algorithm RSA in a case when module it is equal to product of three simple numbers and the modified variant of algorithm of the digital signature of the El-Gamal, supposing transfer of the message in the open form together with the attached authenticator

– considered possibilities of use of the approach on the basis of elliptic curves for optimization of enciphering with an open key and signatures "blindly", the signature of the message providing possibility, which text is not known to the signing;

– developed the scheme for increase of efficiency of algorithm of the electronic digital signature which carries out enciphering definitive result of processing of the electronic document hesh-function by means of asymmetric algorithm;

– offered the effective system of protection of the information for achievement of purposeful prevention of a potential damage to interests of this or that joint-stock or commercial organization, based on the system approach to protection of the confidential information and made recommendations about realization of technology of maintenance of protection of the information;

– on the basis of the proposed algorithms developed software to solve the problems of information processing and information security, carried out its implementation in a number of organizations. There are acts on the implementation of research results.

Подписано в печать 18.10.2010г.
Формат 60х84/16. Печать KYOCERA
Усл.печ.л.1,3
Тираж 120 экз. Заказ 281

_____

Типография ТОО «Копир&Ка»
050022, г.Алматы, пр-т Абая, 36
т: 2-606-300; 2-606-400