МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Сравнительный анализ криптосистем вероятностного шифрования и шифрования на эллиптических кривых

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Минуситова Амиля Куанышкалиевича

Научный руководитель
д. ф.-м. н., профессор _____ В. А. Молчанов
22.01.2024 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2024 г.

Саратов 2024

ВВЕДЕНИЕ

Асимметричная криптография, и в частности, криптосистема RSA, решает проблему распределения ключей, позволяя свободно публиковать открытый ключ. Однако этот факт дает противнику возможность выяснить значение шифротекста методом подбора. Обладая открытым ключом получателя и имея в своем распоряжении перехваченный шифротекст, противник может генерировать различные открытые тексты, зашифровывать их и затем сравнивать со значением шифротекста. Даже учитывая трудоемкость такого подбора, приходится признать, что возможна некоторая частичная утечка информации. Кроме того, два одинаковых сообщения, отправленные одному получателю, будут зашифрованы одинаково.

Таким образом, криптосистема RSA не позволяет скрыть некоторую априорную информацию о шифруемых сообщениях. Поэтому если содержание сообщений ограничивается всего несколькими вариантами (простые инструкции из конечного набора, ответы «да»/«нет», имя из списка), шифрование RSA не сможет обеспечить его достаточно надежное скрытие.

Одним из способов повышения криптографической стойкости шифров является создание неопределенности хода шифрования информации. Данная идея может быть реализована путем введения в преобразуемое сообщение случайных данных. Введение элементов случайности в процесс шифрования преследует цель затруднить использование методов криптоанализа, таких как методы выявления статистических закономерностей в алгоритмах шифрования путем подбора открытых или шифрованных сообщений. Иной способ повышения криптографической стойкости шифров основывается на использовании разнообразных алгебраических структур.

В данной работе рассмотрим 2 подхода к решению проблемы повышения криптографической стойкости шифров:

1) применение криптографических алгоритмов вероятностного шифрования;

2) применение криптографических алгоритмов шифрования на основе эллиптических кривых.

Целью данной работы является рассмотрение существующих схем и алгоритмов вероятностного шифрования и шифрования на основе эллиптических кривых, реализация криптосистемы вероятностного шифрования и шифрования на основе эллиптических кривых, а также проведение сравнительного анализа реализованных криптосистем.

Для достижения поставленной цели были сформулированы следующие задачи:

1) изучить существующие системы, схемы и алгоритмы вероятностного шифрования;

2) рассмотреть принципы работы систем вероятностного шифрования;

3) изучить алгебраические свойства эллиптических кривых;

4) программно реализовать криптосистему Гольдвассера–Микали, модернизировать её с целью повышения криптостойкости;

5) программно реализовать криптосистему на основе эллиптических кривых;

6) разработать программный комплекс с пользовательским интерфейсом, упрощающим работу с этими программами;

7) провести сравнительный анализ реализованных криптосистем.

Данная работа частично представлена на XX Белорусско-российской научно-технической конференции «Технические средства защиты информации».

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 66 страниц, из них 53 страницы – основное содержание, включая 35 рисунков и 7 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В 1 разделе работы описываются появление систем вероятностного шифрования, их основные принципы функционирования и отличия от систем с открытым ключом.

Подраздел 1.1 содержит общее описание схем вероятностного шифрования. Вероятностное шифрование для одного открытого текста может давать большое количество различных шифротекстов, в отличие от систем с открытым ключом. Вероятностная система шифрования состоит из ключевого пространства K, пространства открытых текстов M, пространства шифротекстов C, пространства случайных значений R и функций:

$$E = f_{pkg}: M \times R \to C \text{ и } D = f_{skg}^{-1}: C \times R \to M,$$

для которых верно: $D(E(m,r)) = m$ для каждого сообщения $m \in M$ открытого текста M и источника случайности $r \in R$.

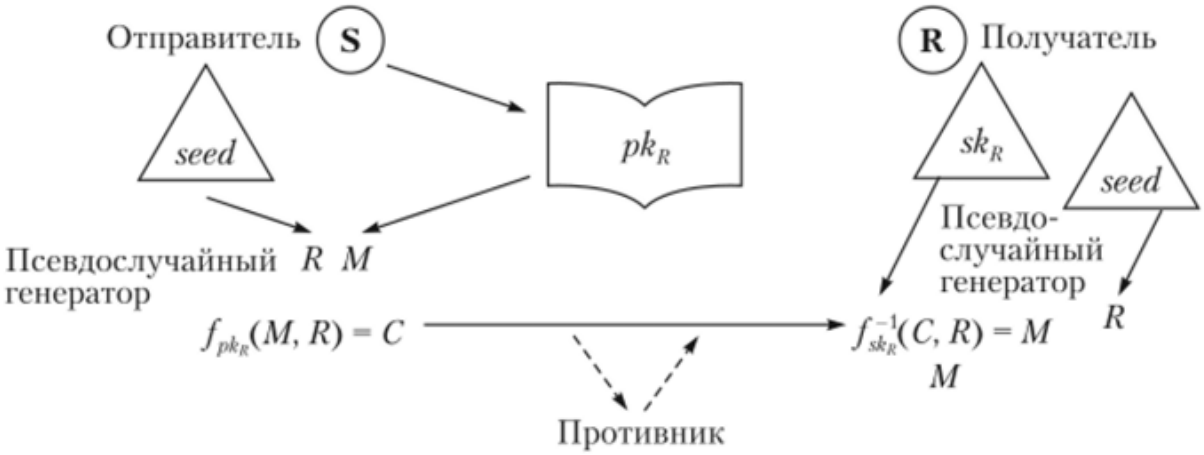

Рисунок 1 – Принцип функционирования схем вероятностного шифрования

Для любого ключа $k \in K$ должна легко обеспечиваться эффективная генерация алгоритмов E_k и D_k, но в то же время получение любого эффективного алгоритма для вычисления D_k только по данному алгоритму E_k должно быть вычислительно невозможно.

В подразделе 1.2 рассказывается про систему Гольдвассера–Микали. Изобретённая ими схема предполагает шифрование сообщения побитно,

причем вся сложность, связанная с поиском отдельного зашифрованного бита в тексте c, заключается в проверке, принадлежит ли число c множеству квадратичных вычетов или невычетов. Подраздел 1.3 содержит информацию о модернизации системы Гольдвассера–Микали, а именно использование числа блюма в качестве N и внедрение в криптограмму случайных данных с помощью BBS-генератора.

В подразделе 1.4 рассказывается о более эффективной системе Блюма–Гольдвассера. Стойкость криптосистемы базируется на непредсказуемости влево BBS генератора, определяемой однонаправленностью функции $f(x) = x^2 \, mod \, N$, N – число Блюма, и трудности факторизации числа N. Вероятностное шифрование Гольдвассера и Микали является не эффективным и устаревшим способом, однако именно благодаря им вероятностное шифрование получило имя и начало свое развитие, что привело к появлению системы Блюма–Гольдвассера, которая является более надежным и лучшим вариантом.

В разделе 2 рассказывается о появление эллиптической криптографии. Предложение об использование алгебраических свойств эллиптических кривых, послужило толчком к появлению нового направления в области шифрования. Криптография с использованием эллиптических кривых особенно привлекательна благодаря своим преимуществам, таким как высокое быстродействие и короткий ключ.

В подразделе 2.1 приводятся понятия алгебраической и эллиптической кривых, сложения, удвоения и скалярного умножения точек. Описываются свойства кривых, и то какие из них представляют интерес в криптографии. Рассмотрен алгоритм поиска точек эллиптической кривой, а также теорема Хассе, определяющая нижнюю и верхнюю границы количества точек N эллиптической кривой E над полем F_q (q – простое число элементов поля):

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

Подраздел 2.2 содержит информацию о том, что стойкость шифров на эллиптических кривых определяется сложностью решения задачи дискретного логарифмирования в группе точек кривой, т.е. сложностью решения уравнения $sP = Q$ относительно s, где точки P и Q принадлежат одной циклической подгруппе. Считается, что задача дискретного логарифмирования на эллиптической кривой даже более сложная, чем эта же задача в конечных полях и для её решения существуют только экспоненциальные алгоритмы. Также приведено сравнение криптосистем над простым конечным полем и криптосистем на эллиптической кривой над конечным полем. Суть перехода к эллиптическим кривым заключается в замене относительно медленной операции возведения в степень по большому модулю в алгоритме RSA на более быструю операцию умножение на скаляр на эллиптической кривой, при этом сохраняются операции над целыми числами по небольшому модулю.

В подразделе 2.3 описывается система шифрования с открытым ключом на эллиптических кривых, основанная на протоколах Эль–Гамаля и Диффи–Хеллмана.

В 3 разделе дипломной работы рассматривается программная реализация модернизированной криптосистемы Гольдвассера–Микали и криптосистемы шифрования на эллиптических кривых. Программный комплекс разработанный на языке программирования Python, позволяет генерировать эллиптическую кривую, пары закрытого и открытого ключей, выполнять шифрование данных, считанных из файла формата .txt, а также расшифрование полученной криптограммы. Программа имеет пользовательский интерфейс, написанный с помощью библиотеки PySimpleGUI.

Подраздел 3.1 содержит пример использования криптосистемы Гольдвассера–Микали. В подразделе 3.2 приводится алгоритм генерации эллиптической кривой и пример использования криптосистемы на основе эллиптических кривых.

В подразделе 3.3 проведено сравнение рассмотренных криптосистем. Входными данными являются 6 файлов размерами: 1 Кбайт, 8 Кбайт, 61 Кбайт,

136 Кбайт, 561 Кбайт и 1114 Кбайт. Приводятся результаты исследований: время генерации параметров, шифрования и дешифрования файлов, а также размеры исходных и зашифрованных файлов, для реализованных криптосистем, объясняется разница в результатах.

Таблица 1 – Время генерации параметров (размер 32 бит)

Время	Эллиптическая кривая (с)	Ключи ECC (с)	Ключи GM (с)
Среднее	29,9879	7,6602	0,01001
Минимальное	4,057	3,4699	0,0039
Максимальное	94,8932	10,8368	0,0408

Условий, накладываемых на параметры для эллиптической кривой, намного больше и поэтому время их генерации значительно выше, чем для ключей системы Гольдвассера–Микали. Так как время генерации параметров не детерминировано, в таблице 1 представлено среднее, минимальное и максимальное время.

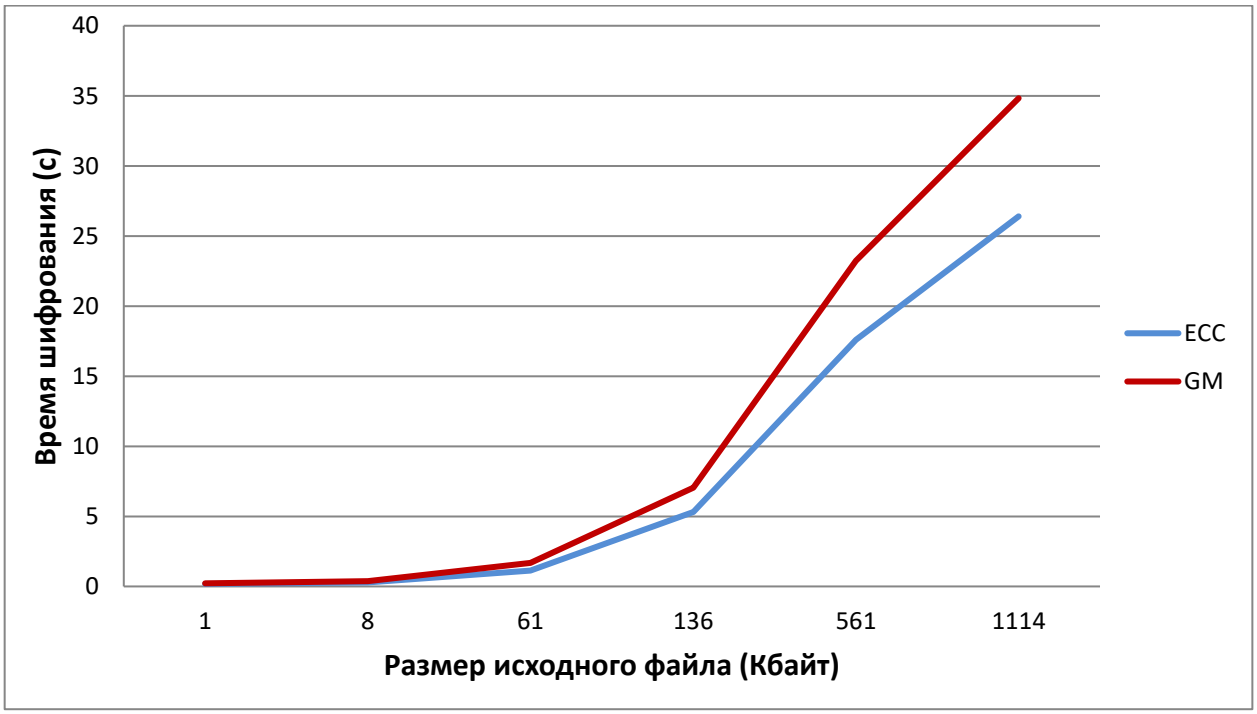

Рисунок 32 – График зависимости времени шифрования (в с) от размера исходного файла (в Кбайт) криптосистем ECC и GM (ключ 32 бит)

Таблица 2 – Сравнение размеров исходного файла и полученной шифрограммы на ключе 32 бита

Размер исходного файла	Размер шифрограммы ECC	Размер шифрограммы GM
1 Кбайт	5	80
8 Кбайт	26	764
61 Кбайт	144	5123
136 Кбайт	486	11289
561 Кбайт	1322	47213
1114 Кбайт	2622	93774

Можем заметить сильное увеличение размера шифрограммы в криптосистеме GM, это происходит по причине того, что одному биту исходного текста соответствует $log_2 N$ бит зашифрованного текста, где N – часть открытого ключа.

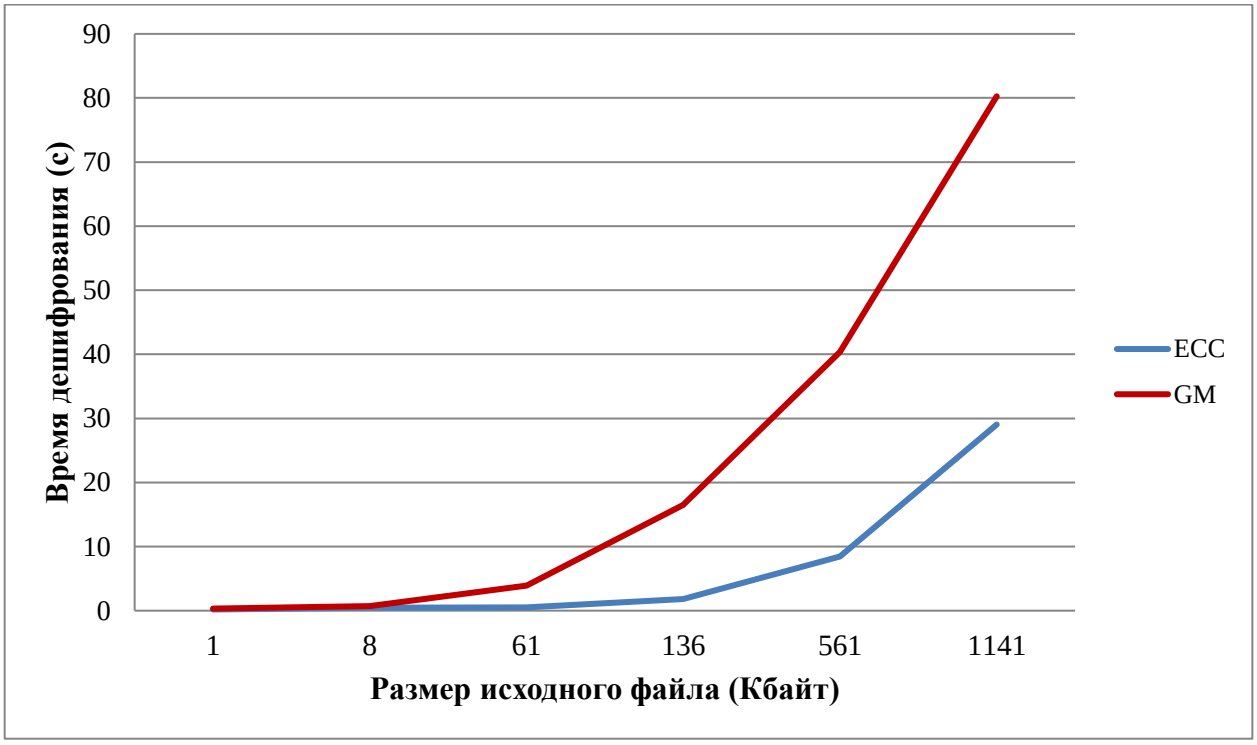

Рисунок 33 – График зависимости времени дешифрования (в с) от размера исходного файла (в Кбайт) криптосистем ECC и GM (ключ 32 бит)

Из полученных результатов эксперимента можно сделать следующие выводы:

1) производительность GM выше, чем у ECC по показателю времени генерации ключей;

2) производительность ECC выше, чем у GM по показателям времени шифрования и дешифрования;

3) степень расширения размера криптограммы по сравнению с исходным файлом ECC ниже, чем у GM.

ЗАКЛЮЧЕНИЕ

Вероятностное шифрование представляет собой метод защиты информации, основанный на использовании случайных величин и непредсказуемости хода шифрования. Шифрование на эллиптических кривых основано на решении задачи дискретного логарифмирования и является одним из наиболее перспективных методов криптографии, так как оно обеспечивает высокий уровень безопасности данных при относительно низких затратах на вычисление и хранение.

В ходе написания данной работы изучены схема и алгоритмы вероятностного шифрования, алгебраические свойства эллиптических кривых, рассмотрены системы Гольдвассера–Микали, Блюма–Гольдвассера, а также система шифрования на эллиптических кривых, основанная на протоколах Эль–Гамаля и Диффи–Хеллмана.

В практической части работы разработан программный комплекс на языке Python для реализации модернизированной криптосистемы Гольдвассера–Микали и криптосистемы шифрования на эллиптических кривых. Так же произведён сравнительный анализ разработанных криптосистем, оценивающий время генерации параметров, шифрования и дешифрования и размеры исходных файлов и шифрограмм.

Таким образом, все поставленные задачи решены, цель работы достигнута.