Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 003.26

Короткевич
Антон Викентьевич

Методы и средство криптографической передачи информации на базе эллиптических кривых

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик В.Н.
д.т.н., профессор

Минск 2014

ВВЕДЕНИЕ

Проблема безопасного обмена информацией при все большем распространении глобальной сети Интернет и средств мгновенного обмена сообщениями в наше время становится особенно актуальной.

Для обеспечения должного уровня защиты передаваемой информации служат различные криптографические подходы и алгоритмы. Различают симметричные и ассиметричные криптосистемы. В симметричных криптосистемах секретный ключ шифрования совпадает с секретным ключом дешифрования, потому он должен храниться в секрете от посторонних. В ассиметричных криптосистемах открытый ключ шифрования не совпадает с закрытым секретным ключом дешифрования и вычислительно невозможно получить закрытый ключ из открытого. Симметричные криптосистемы выигрывают у ассиметричных в скорости шифрования и дешифрования информации, однако имеют сложности при обмене ключами, т.к. для осуществления данной операции необходим секретный канал для передачи закрытого ключа каждой из сторон. При использовании же ассиметричных криптосистем собеседники могут свободно обмениваться открытыми ключами по незащищенному каналу. С учетом указанных особенностей, использование ассиметричных криптосистем является хорошим решением проблемы защищенности передаваемой между пользователями информации.

В основе любой схемы ассиметричного шифрования лежит определенная трудноразрешимая математическая задача. При этом к данной задаче на самом деле есть способ найти решение, но для этого нужно обладать некоторой дополнительной информаций – в англоязычной литературе ее называют «trapdoor» – потайная дверь. В качестве открытого ключа в ассиметричной криптографии выбирается какое-либо частное уравнение, которое и является трудноразрешимой задачей. Но при составлении этого уравнения оно разрабатывалось так, что лицо, знающее некоторую дополнительную информацию об этом уравнении, может решить его за разумный временной интервал. Эта дополнительная информация и является закрытым ключом. Примерами подобных трудноразрешимых задач являются факторизация чисел большой разрядности и вычисление дискретных логарифмов над такими числами. Наиболее известными ассиметричными криптосистемами являются RSA, схема Эль-Гамаля, эллиптическая криптосистема.

Преимущество подхода на основе эллиптических кривых в сравнении с задачей факторизации числа, используемой в RSA, или задачей целочисленного логарифмирования, применяемой в алгоритме Эль-Гамаля, заключается в том, что в данном случае обеспечивается эквивалентная защита при меньшей длине ключа. К примеру, самые сложные схемы на эллиптических кривых, публично взломанные к настоящему времени, содержали 112-битный ключ для конечного простого поля и 109-битный ключ для конечного поля характеристики 2. В июле 2009 года, кластер из более чем 200 Sony Playstation 3 за 3,5 месяца нашел 109-битный ключ. Ключ над полем характеристики 2 был найден в апреле 2004

года, с использованием 2600 компьютеров, в течение 17 месяцев. В то же время существуют рекомендованные конечные поля с ключом длиной более 500 бит. Потому использование эллиптических кривых может дать прекрасную защиту для передаваемых по сети пользовательских данных.

Таким образом, изучение методов криптографической передачи информации на базе эллиптических кривых и разработка программного средства для безопасной передачи данных по сети Интернет на их основе будет рассмотрена в данной работе.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Областью исследования в данной работе является раздел ассиметричной криптографии, а именно криптография, основанная на свойствах эллиптических кривых.

Целью исследования является изучение методов криптографической передачи информации на базе эллиптических кривых и разработка криптосистемы на их основе. Разработанная криптосистема будет использована при создании приложения для безопасной передачи информации по сети Интернет.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить свойства эллиптических кривых, реализовать базовые операции над точками эллиптических кривых.
2. Разработать метод шифрования последовательности данных на базе эллиптических кривых.
3. Разработать и реализовать необходимые для работы криптосистемы алгоритмы, провести экспериментальный анализ их производительности, отобрать лучшие реализации алгоритмов.
4. Реализовать криптографическую систему с использованием наилучших по производительности алгоритмов, провести экспериментальный анализ производительности криптосистемы в зависимости от размера эллиптической кривой.
5. Разработать архитектуру клиентской и серверной частей программного средства криптографической передачи информации в рамках глобальной сети Интернет с использованием разработанной криптосистемы.
6. Реализовать клиентскую и серверную части программного средства.

Объектом исследования являются методы защиты информации с использованием криптографических алгоритмов.

Предметом исследования являются методы и алгоритмы шифрования данных, основанные на свойствах эллиптических кривых.

Практическая *актуальность* исследования связана с высокой эффективностью и криптостойкостью эллиптических криптосистем, которые позволяют достичь одинакового уровня криптостойкости с использованием меньшего раз-

мера криптографического ключа по сравнению с другими ассиметричными криптосистемами, что позволяет получить преимущество в производительности алгоритмов.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии с научно-техническим заданием и планом работ кафедры «Программное обеспечение информационных технологий» по теме «Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-программных средств систем и сетей сложной конфигурации и внедрить в современные обучающие комплексы» (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР – В. В. Бахтизин).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя В. Н. Ярмолика заключается в формулировке целей и задач исследования.

Апробация и опубликованность результатов диссертации

Результаты исследования были представлены в качестве докладов на 49-й научной конференции аспирантов, магистрантов и студентов (БГУИР, Минск, 6-10 мая 2013 г.) и международной научной конференции «Информационные технологии и системы 2014» (БГУИР, Минск, 29 октября 2014 г.) и опубликованы в соответствующих сборниках [1, 2].

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников и списка публикаций автора. В первой главе представлен аналитический обзор предметной области, анализ существующий видов криптографических систем, постановку задачи и выбор технологий программирования. Вторая глава посвящена анализу математических моделей эллиптических кривых, разработке эллиптической криптосистемы и необходимых для ее работы математических алгоритмов. В третьей главе выполнена реализация разработанной криптосистемы с помощью выбранных средств программирования и практический анализ производительности всей криптосистемы в целом и отдельных алгоритмов в частности. Четвертая глава посвящена разработке программного средства обмена информацией в рамках сети Интернет с использованием полученной эллиптической криптосистемы.

Общий объем работы составляет 77 страниц, из которых основного текста – 57 страниц, 28 рисунков на 13 страницах, 6 таблиц на 2 страницах и список использованных источников из 30 наименований на 2 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** обоснована актуальность диссертационной работы, показана эффективность использования эллиптических кривых для защиты передаваемой информации.

В **первой главе** в разделе 1.1 представлен обзор различных типов эллиптических криптосистем, описаны проблемы современной ассиметричной криптографии, показаны преимущества криптосистем на базе эллиптических кривых.

В разделе 1.2 приведена постановка задача, включающая в себя план исследования, а также общие требования к программного средству. С учетом данных требований в разделе 1.3 произведен анализ технологий программирования и обоснован выбор языка программирования C# и платформы .NET для выполнения поставленной задачи.

Вторая глава содержит математическое описание эллиптических кривых и алгоритмов, необходимых для работы криптографической системы. В разделе 2.1 приводится определение эллиптических кривых и операций сложения точек эллиптической кривой и удвоения точки, а также основных параметров эллиптической группы.

В разделе 2.2 приведены и проанализированы различные алгоритмы по выполнению операции умножения точки эллиптической кривой на число. Рассмотренные алгоритмы:

– умножение точки на число с использованием бинарного представления множителя;

– умножение точки на число с использованием несмежных форм (NAF);

– умножение точки на число с использованием несмежных форм ширины w (NAF_w);

– умножение точки на число с использованием скользящего окна;

– умножение фиксированной точки на число с оконным методом;

– умножение фиксированной точки на число с оконным методом с использованием несмежных форм.

В разделе 2.3 рассматриваются методы нахождения мультипликативной инверсии числа по модулю, которая необходима для выполнения операций сложения точек и удвоения точек эллиптической группы.

Развел 2.4 включает описание и анализ алгоритмов по вычислению результата возведения числа в степень по модулю. Рассмотренные алгоритмы:

– бинарное возведение числа в степень справа налево;

– бинарное возведение числа в степень слева направо;

– возведение числа в степень по модулю с помощью окна ширины w;

– возведение числа в степень по модулю с использованием скользящего

окна.

В разделе 2.5 рассматриваются методы шифрования данных на базе эллиптических кривых. В результате разработана эллиптическая криптосистема, представляющая собой модификацию метода Менезеса-Ванстоуна.

В **третьей главе** выполняется реализация разработанной криптографической системы с помощью выбранных технологий программирования и практический анализ производительности отдельных алгоритмов и всей криптосистемы в целом. Все эксперименты проведены для эллиптических групп различных размеров. В качестве тестовых групп приняты рекомендованных NIST (The National Institute of Standards and Technology – Национальный институт стандартов и технологий США) эллиптические кривые P-192, P-224, P-256, P-384, P-521 (число определяет размер модуля эллиптической группы в битах).

В разделе 3.1 описываются классы модуля операций над точками эллиптической группы и модуля шифрования, которые включают в себя логику криптосистемы, и их методы.

В разделе 3.2 обоснована эффективность разработки через тестирование при реализации криптосистемы, приведен пример модульного теста и перечислены все виды модульных тестов, которые использовались при разработке.

В разделе 3.3 произведен практический анализ производительности рассмотренных в теоретической части алгоритмов по умножению точки эллиптической группы на число. В результате исследования установлено, что лучшим алгоритмом по умножению переменных точек на число является метод на базе несмежных форм ширины 5. Для фиксированных точек наиболее эффективен оконный метод с использованием несмежных форм шириной 4 для кривых P-192, P-224, P-256 и шириной 5 для кривых P-384, P-521. Эти алгоритмы приняты для использования в разрабатываемой криптографической системе.

Раздел 3.4 содержит практический анализ производительности рассмотренных в теоретической части алгоритмов по возведению числа в степень по модулю. По результатам анализа наиболее эффективным оказался алгоритм с использованием скользящего окна ширины 4. Он принят для использования в разрабатываемой криптосистеме.

В разделе 3.5 произведено исследование производительности криптосистемы при различных вариантах разбиения шифруемого набора данных на точки эллиптической группы. В результате установлено, что оптимальной стратегией разбиения набора данных на блоки будет выделение минимального числа точек, координаты которых не выходят за пределы поля эллиптической группы (т.е. меньше модуля данной группы).

После получения финальной реализации криптосистемы, проведен анализ производительности отдельных операций по работе с точками эллиптической группы (сложения точек, удвоения точек, умножения точки на число) и операций кодирования точки эллиптической группы и шифрования текстового сообщения с помощью разработанной криптосистемы в зависимости от размера эллиптической группы. График с результатами исследования приведен на рисунке 1.

Как видно из результатов проведенных исследований, операции сложения точек и удвоения точки растут медленнее всего с увеличением размера поля и увеличиваются для кривой P-521 по сравнению с кривой P-192 приблизительно в 3 раза. Операция умножения точки на число является самой быстрорастущей и именно ее вклад в сложность кодирования точки максимален, что подтверждается схожей формой этих графиков. Сложность умножения точки на число и кодирования точки для кривой P-521 приблизительно в 9 раз выше, чем для кривой P-192.

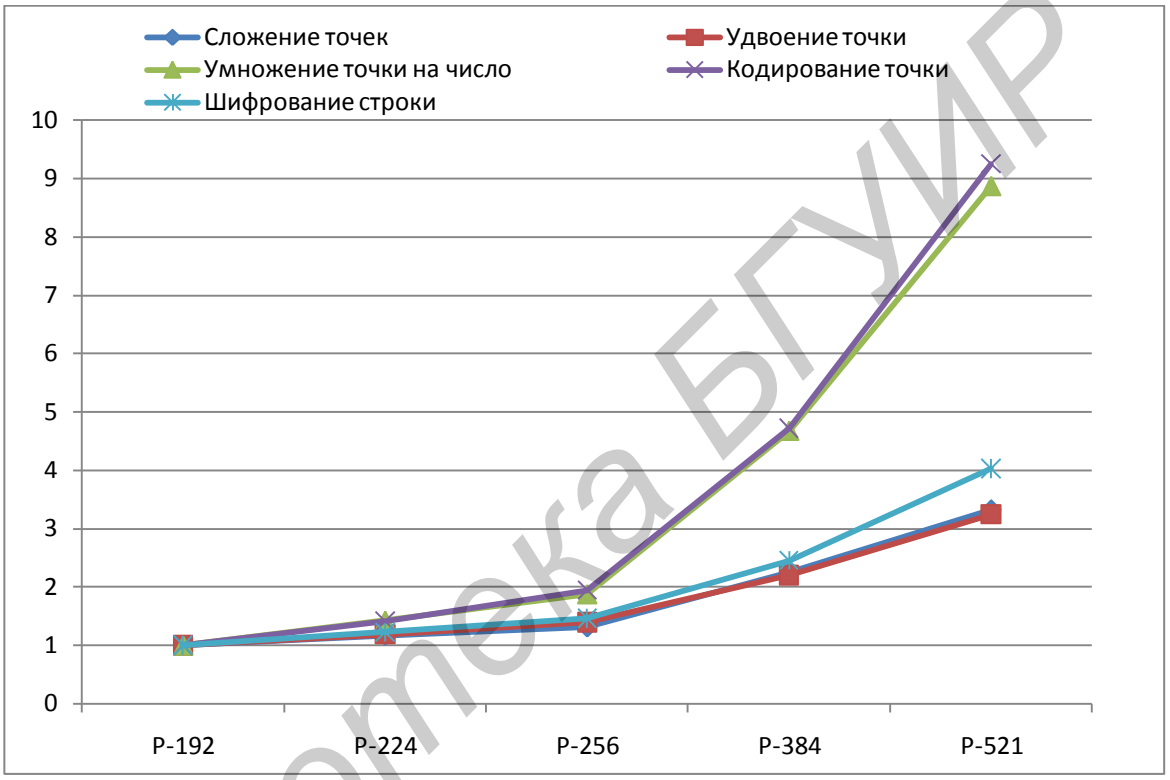

Рисунок 1 – Время выполнения основных криптографических операций

Однако, сложность операции шифрования строки не растет в том же темпе, что и операция кодирование точки, а ее значения для наибольшей и наименьшей по размеру кривых различаются приблизительно в 4 раза. Это объясняется тем, что оптимальной стратегией разбиения шифруемого блока данных на точки является выделение минимального числа точек, размеры которых максимальны и при этом не выходят на пределы эллиптического поля, а это означается, что для большего размера эллиптического поля можно выделить меньшее количество точек, соответственно, для шифрования строки такого же размера понадобится меньшее число операций кодирования точки. Таким образом, для больших блоков данных (битовые размеры которых в несколько раз превышают битовые размеры точек эллиптических групп) рост сложности операции шифрования блока значительно ниже, чем рост сложности операции кодирования одиночной точки.

Но стоит отметить, что и минимальная из используемых для исследова-

ний кривая P-192 обеспечивает высокий уровень безопасности данных, потому может быть хорошим выбором для эллиптической криптосистемы, при этом обеспечивая более высокую скорость шифрования и дешифрования данных по сравнению с другими кривыми.

В **четвертой главе** выполнена разработка программного средства передачи криптографической информации с использованием разработанной криптосистемы на базе эллиптических кривых. Спецификация требований к этому программному средству представлена в разделе 4.1.

В разделе 4.2 описывается общая структура программного средства. Приведены диаграмма сценариев использования и диаграмма компонентов программного средства, структура базы данных сервера авторизации, схема общего алгоритма работы клиентского приложения, схемы алгоритмов шифрования и дешифрования данных. Также описаны некоторые особенности реализации программного средства.

Раздел 4.3 содержит описание основных классов и методов программного средства.

В разделе 4.4 перечислены модульные и функциональные тесты, которые успешно прошло программное средство после его разработки.

Раздел 4.5 представляет собой руководство по использованию программного средства и включает в себя поясняющие рисунки с изображением основных окон приложения.

ЗАКЛЮЧЕНИЕ

В результате работы над магистерской диссертацией разработана криптографическая система, базирующаяся на свойствах эллиптических кривых, и проведен анализ ее производительности в зависимости от размера эллиптической группы. Для демонстрации работы и использования этой криптосистемы было создано программное средство передачи криптографической информации, которое позволяет пользователям безопасно обмениваться данными в рамках глобальной сети Интернет.

Основные результаты проделанной работы:

– проведен анализ типов современных криптографических систем и обоснован выбор эллиптических кривых в качестве основы для разрабатываемой криптосистемы;

– изучены основные принципы и свойства эллиптических кривых, включая операции сложения точек эллиптической кривой и удвоения точки;

– исследованы и разработаны алгоритмы для выполнения операций умножения точки эллиптической кривой на число, мультипликативной инверсии числа по модулю, возведения числа в степень по модулю, которые необходимы для работы эллиптической криптосистемы;

– изучены различные методы шифрования данных с использованием криптосистем на базе эллиптических кривых;

– на основе метода Менезеса-Ванстоуна по шифрованию данных с помощью эллиптических кривых предложен модифицированный метод, позволяющий

шифровать данные произвольного размера;

– выполнен практический анализ разработанных алгоритмов по умножению точки эллиптической группы на число, по результатам которого выбраны лучшие по производительности алгоритмы для умножению произвольных и фиксированных точек;

– выполнен практический анализ разработанных алгоритмов по возведению числа в степень по модулю, по результатам которого выбран лучший по производительности алгоритм;

– выполнен практический анализ производительности различных вариантов разбиения исходной последовательности байт на точки в эллиптической группы, по результатам исследования разработан алгоритм оптимального выделения точек из шифруемого набора данных;

– используя оптимизированные алгоритмы, реализована криптографическая система на базе эллиптических кривых;

– выполнен практический анализ производительности разработанной криптографической системы в зависимости от размера эллиптической группы в ее основе, выработаны рекомендации по выбору размера эллиптической группы;

– разработана спецификация требования к программного средству передачи криптографической информации на базе эллиптических кривых;

– спроектирована и разработана серверная часть программного средства, соответствующая функциональным требованиям;

– спроектирована и разработана клиентская часть программного средства, соответствующая функциональным требованиям;

– разработанное клиентское приложение имеет интуитивно-понятный графический пользовательский интерфейс, благодаря чему для работы с ним не требуется специальной квалификации.

Практическое использование разработанной криптосистемы является актуальным, поскольку эллиптические кривые являются современной и надежной основой для криптосистем и позволяют достичь аналогичного уровня безопасности, используя ключи меньшего размера по сравнению с другими типами ассиметричных криптографических систем. Особое внимание при работе с эллиптическими кривыми следует обратить оптимизации скорости выполнения используемых алгоритмов, что и было сделано в данной магистерской работе.

Рекомендации по практическому использованию результатов:

1. Полученные результаты формируют теоретическую и практическую базу для разработки программного обеспечения для решения задач защиты информации с помощью шифрования на базе эллиптических кривых.

2. Результаты разработки и экспериментального анализа алгоритмов, приведенные в главе 3, могут применяться в программном обеспечении различного рода, особенно если скорость выполнения алгоритмов имеет важное значение.

3. Разработанное программное средство может использоваться для обмена мгновенными сообщениями между пользователями в рамках глобальной се-

ти Интернет с обеспечением высокого уровня безопасности передаваемой информации.

По результатам работы были представлены доклады на 49-й научной конференции аспирантов, магистрантов и студентов БГУИР и международной научной конференции «Информационные технологии и системы 2014», материалы которых опубликованы в соответствующих сборниках [1, 2].

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Короткевич, А.В. Криптографическая передача информации на базе эллиптических кривых / А.В. Короткевич // Компьютерные системы и сети: материалы 49-й научной конференции аспирантов, магистрантов и студентов (Минск, 6–10 мая 2013 г.). – Минск: БГУИР, 2013. – С. 51.

2. Короткевич, А.В. Криптографическая защита информации на базе эллиптических кривых / А.В. Короткевич // Информационные технологии и системы 2014 (ИТС 2014): материалы международной научной конференции (БГУИР, Минск, Беларусь, 29 октября 2014). – Минск: БГУИР, 2014. – С. 264-265.