МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

Группа точек гладкой кривой проективного пространства и ее приложения в криптографических протоколах

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Бирюкова Валерия Евгеньевича

Научный руководитель
доцент, к. ф.-м. н. _____ В.Е. Новиков
18.01.2019 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
18.01.2019 г.

Саратов 2019

ВВЕДЕНИЕ

Эллиптические кривые и их свойства изучались как чисто математическое понятие долгое время со второго или третьего веко нашей эры, но их использование в криптографии началось совсем недавно. Само имя «эллиптический» было дано в XIX веке, которое нашло широкое распространение среди математиков. Использование эллиптических кривых в криптографии не было известно до 1984 года. Первым применением кривых в криптографии было их использование в факторизации целых чисел алгоритмом Ленстры, у которого было несколько преимуществ над существовавшими тогда алгоритмами факторизации. Это в свою очередь привело в движение процесс поиска других криптографических применений для многих «чистых» математических дисциплин, особенно алгебраической геометрии, которые никогда до этого не рассматривались для этих целей.

В 1985, Виктор Миллер и Нил Коблиц независимо друг от друга предложили совершенно другой подход к кривым в криптографии: сконструировали протокол аналогичный протоколу Диффи-Хеллмана с использованием точек эллиптической кривой, определенной над конечным полем, а не мультипликативной группы конечного поля. Данный факт способствовал увеличению интереса к группам точек эллиптической кривой, так как они предоставляли большую безопасность, вместе с меньшой длинной ключа.

На ранних стадиях развития эллиптической криптографии популярным выбором кривой для демонстрационных целей, служили так называемые суперсингулярные кривые. Это обосновывалось быстротой операций над ними. Но в 1991 годы был найден алгоритм решения задачи дискретного логарифмирования на суперсингулярной кривой, который работает быстрее, чем на большинстве кривых.

В конце 2013 года группа американских ученых проанализировала четыре популярных протокола, использующих эллиптическую криптографию: Bitcoin,

SSH, TLS и Austrian e-ID. Эксперты подсчитали, что из 12 млн хостов, поддерживающих SSH в 10,3% реализован ECDSA (алгоритм цифровой подписи, основанный на эллиптических кривых) для аутентификации и в 13,8% – ECDH (аналог протокола Диффи-Хеллмана с использованием эллиптической криптографии) для обмена ключами. Авторы также исследовали 30,2 млн TLS-серверов, обнаружив, что 7,2% из них поддерживают ECDH. Из 829 тысяч Austrian Citizen Card в 58% используется ECDSA. Также отмечается, что вся асимметричная криптография, на которой построена защита системы Bitcoin, основана на математическом аппарате эллиптических кривых. Но эллиптическая криптография не избавляет от таких уязвимостей, как низкая энтропия и ошибки программной реализации.

В следствии быстрого развития технологий и мощности вычислительных компьютерных систем, а также, методов и средств криптоанализа, возникает необходимость увеличивать размеры общесистемных параметров протокола, вследствие чего увеличивается ресурсоемкость и сложность выполнения базовых операций в полях. Для увеличения криптографической стойкости и уменьшения размера параметров протокола целесообразно использовать эллиптические кривые. К примеру, ключ длиной 4096 бит для RSA предоставляет тот же уровень безопасности, что и ключ длины 313 бит в криптосистеме, основанной на эллиптической кривой.

Кроме этого эллиптические кривые над конечными полями предоставляют неисчерпаемый источник конечных абелевых групп, которые удобны для вычисления и обладают богатой структурой. Во многих отношениях эллиптические кривые – естественный аналог этих групп, но более удобный, так как существует большая свобода в выборе эллиптической кривой, чем в выборе конечного поля.

Целью данной работы является рассмотрение преимуществ эллиптических криптографии, а также разработка и реализация аналогов протоколов аутентификации на эллиптической кривой.

Работа состоит из введения, девяти глав, двух приложений и заключения.

В первой главе описываются основные теоретические сведенья о конечных полях и группах, которые необходимы для изложения материала об эллиптических кривых.

В следующей главы вводятся понятие эллиптической кривой различной характеристики, а также рассматриваются операции над точками этой кривой в поле вещественных чисел.

В третьей главе описываются закономерность, которые обосновывают возможность построения криптосистем с использованием эллиптических кривых, аналогичных системам над конечными полями.

Четвертая глава посвящена аутентификации, ее видам, факторам, по которым она осуществляется. Это необходимо, так как далее следует описание криптосистем с открытым ключом и примеры протоколов аутентификации, использующие доказательство с нулевым разглашением, сначала над конечными полями, а после над эллиптическими кривыми. В главах шесть, семь и восемь рассмотрено 3 протокола аутентификации: протокол Шнорра, Окамото и протокол основанный на криптосистеме Диффи-Хеллмана.

КРАТКОЕ СОДЕРЖАНИЕ

В первой главе рассматриваются основные определения и другие теоретические знания необходимые для дальнейшего изложения теории эллиптических кривых. Основными здесь являются определения поля и характеристики поля, т.к. эти сведенья используются в определение эллиптических кривых.

Полем называется кольцо F с единицей, множество ненулевых элементов которого с операцией умножения является абелевой группой. Эта группа называется мультипликативной группой поля.

Конечные поля называются *полями Галуа*. *Порядком поля* называется число его элементов. Конечное поле порядка q обозначается $GF(q)$ или F_q.

Характеристикой поля называется наименьшее натуральное число m такое, что $m \times 1 = 0$, или число 0, если такого числа m не существует. Иными словами, характеристика поля определяется как аддитивный порядок мультипликативной единицы поля.

Во второй главе вводится понятие эллиптической кривой, а также рассматривается частный случай, кривой над полем вещественных чисел, для того чтобы продемонстрировать как осуществляется сложение в группе точек такой кривой.

Пусть K – поле характеристики, отличной от 2, 3, и $x^3 + ax + b$ (где $a, b \in K$) – кубический многочлен без кратных корней. *Эллиптическая кривая над* K – это множество точек (x, y), $x, y \in K$, удовлетворяющих уравнению

$$y^2 = x^3 + ax + b, \qquad (1)$$

вместе с единственным элементом, обозначаемым O и называемым «точка в бесконечности».

Если K – поле характеристики 2, то *эллиптическая кривая над* K – это множество точек, удовлетворяющих уравнению либо типа

$$y^2 + cy = x^3 + ax + b, \qquad (2)$$

либо типа

$$y^2 + xy = x^3 + ax^2 + b, \quad (3)$$

(здесь кубические многочлены в правых частях могут иметь кратные корни), вместе с «точкой в бесконечности» O.

Если K – поле характеристики 3, то *эллиптическая кривая над* K – это множество точек, удовлетворяющих уравнению

$$y^2 = x^3 + ax^2 + bx + c, \quad (4)$$

(где кубический многочлен справа не имеет кратных корней), вместе с «точкой в бесконечности» O.

Пусть E – эллиптическая кривая над вещественными числами, и пусть P и Q – две точки на E. Определим точки $-P$ и $P + Q$ по следующим правилам.

1. Если P – точка в бесконечности O, то $-P = O$ и $P + Q = Q$, т.е. O является тождественным элементом по сложению группы точек. В следующих пунктах предполагается, что ни P, ни Q не являются точками в бесконечности.

2. Точки $P = (x, y)$ и $-P$ имеют одинаковые x-координаты, а их y-координаами различаются только знаком, т.е. $-(x, y) = (x, -y)$. Из (1) следует, что $(x, -y)$ – также точка на E.

3. Если P и Q имеют различные x-координаты, то прямая $l = \overline{PQ}$ имеет с E еще в точности одну точку пересечения R (за исключением двух случаев: когда она оказывается касательной в P и мы тогда полагаем $R = P$, или касательной в Q, и мы тогда полагаем $R = Q$). Определяем теперь $P + Q$ как точку $-R$, т.е. как отражение от оси x третьей точки пересечения.

4. Если $Q = -P$ (т.е. x-координата Q та же, что и у P, а y-координата отличается лишь знаком), то полагаем $P + Q = O$ в следствии правила 1.

5. Остается возможность $P = Q$. Тогда считаем, что l – это касательная к кривой в точке P. Пусть R – единственная другая точка пересечения l с E. Полагаем $P + Q = -R$ (в качестве R берем P, если касательная прямая в P имеет двойное касание, т.е. если P есть точка перегиба кривой).

Кроме этого в подпункте 2 рассматривается теорема Хассе о числе точек на эллиптической кривой, определенной над конечным полем.

Теорема 3 (Хассе). Пусть N – число F_q-точек на эллиптической кривой определенной над F_q. Тогда

$$|N - (q + 1)| \leq 2\sqrt{q}. \quad (5)$$

В следующей главе проводится аналогия между группой точек эллиптической кривой, определенной над конечным полем, и мультипликативной группой конечного простого поля. Их схожесть позволяет нам воспроизвести алгоритмы, которые работают с применением операций в мультипликативной группе, с использование эллиптических кривых, а именно с использованием операций над точками этих кривых.

В четвертой главе и её подпунктах вводится основные теоретические сведенья о аутентификации, её факторах и задачах.

Аутентификация – это процедура, позволяющая одной сущности проверить объявленные свойства другой.

Фактор аутентификации – определенный вид информации, предоставляемый субъектом системе при его аутентификации.

Выделяют три фактора аутентификации, используемые в различных комбинациях:

1) На основе знания чего-либо,
2) На основе обладания чем-либо,
3) На основе биометрических характеристик.

В аутентификации можно выделить следующие три задачи: аутентификация источника данных (data-origin authentication), аутентификация сущности (entity authentication) и генерация аутентифицированных ключей (authenticated key establishment).

В пятой главе рассматривается криптография с открытым ключом и задачи, решающиеся с её помощью.

В криптографии с открытым ключом (асимметричная криптография) алгоритмы используют связанные между собой пары ключей, состоящие из

открытого и закрытого ключа. Для каждого человека или объекта генерируется ключевая пара:

1) открытый ключ, доступный для всех;

2) закрытый ключ, известный только человеку, которому он выдан, и никому другому не раскрывается и никуда не передается.

Информация, зашифрованная с помощью одного ключа из ключевой пары, может быть расшифрована только с помощью другого ключа их этой же пары. Ключи математически связаны между собой так, что, зная открытый ключ, практически невозможно вычислить закрытый. Пользователь может повсеместно распространять свой открытый ключ, но он должен обязательно защищать свой закрытый ключ.

Криптографию с открытым ключом можно использовать для:

1) предотвращения возможности несанкционированного ознакомления с информацией при её хранении в компьютере или на отчуждаемых носителях, а также при передаче по каналам связи;

2) подтверждения подлинности электронного документа, доказательства авторства документа и факта его получения от соответствующего источника информации;

3) обеспечения гарантий целостности – исключение возможности необнаружения несанкционированного изменения информации;

4) аутентификации пользователей системы – владельцев секретных ключей.

В главах шесть, семь и восемь вводятся схемы аутентификации Шнорра, Окамото и Диффи-Хеллмана, а также их аналоги с использованием эллиптической криптографии.

Протокол Шнорра. Прежде исполнения этого протокола сторона A выбирает случайное число x из $\{1, \dots, q-1\}$ в качестве своего секретного ключа и держит его в секрете. Далее A вычисляет $y = g^{-x} \bmod p$. Значение y объявляется открытым ключом стороны A, выкладывается в открытый доступ и для всех сторонних пользователей ассоциируется с личностью A.

Шаг 1. A выбирает случайное число k из множества $\{1, \dots, q-1\}$, вычисляет $r = g^k \bmod p$ и посылает r стороне B.

Шаг 2. Абонент B выбирает случайный запрос e из множества $\{0, \dots, 2^t - 1\}$, где t –параметр надежности от обмана стороны A, и посылает e абоненту A.

Шаг 3. A вычисляет $s = k + xe \bmod q$ и посылает s абоненту B.

Шаг 4. Абонент B проверяет соотношение $r = g^s y^e \bmod p$ и, если оно выполняется, то сторона B убеждается в том, что стороне A известно значение x, которое не известно никому, что подтверждает личность A.

Протокол Окамото. Перед исполнением этого протокола сторона A, доказывающая сторона, выбирает два случайных числа a_1, a_2 из $\{1, \dots, q-1\}$ в качестве своего секретного ключа. Далее A вычисляет $Y = g_1^{a_1} g_2^{a_2} (\bmod p)$, которое объявляется открытым ключом стороны A и выкладывается в открытый доступ.

Шаг 1. Сторона A выбивает случайным образом величины x_1, x_2 из $\{1, \dots, q-1\}$, вычисляет значение $X = g_1^{x_1} g_2^{x_2} \ (\bmod p)$ отсылает стороне B.

Шаг 2. Сторона B выбирает случайное значение c из $\{1, \dots, q-1\}$ и отправляет c стороне A.

Шаг 3. A считает значения $s_1 = x_1 + a_1 c \ (\bmod q)$, $s_2 = x_2 + a_2 c \ (\bmod q)$ и отправляет их B.

Шаг 4. Стороной B осуществляется проверка $g_1^{s_1} g_2^{s_2} = X Y^c$. Если равенство выполняется, то подлинность стороны A подтверждена.

В последней главе приводятся примеры аутентификации, с помощью написанной программы, по описанным протоколам Шнорра и Окамото. В программной реализации протоколов в качестве параметров кривой берутся числа, рекомендованные NIST (National Institute of Standards and Technology). Алгоритмы аутентификации Шнорра и Окамото на основе доказательства с нулевым разглашением были реализованы на языке программирования Java в качестве двух программ (двух сторон, участвующих в протоколе), которые общаются между собой при помощи запросов HTTP протокола.

ЗАКЛЮЧЕНИЕ

Криптографические протоколы, основанные на доказательстве с нулевым разглашением, позволяют произвести процедуры идентификации, обмена ключами и другие криптографические операции без утечки секретной информации в течение информационного обмена. Их применение в криптографии позволяет уменьшить общих параметров протоков и вместе с тем увеличить их производительность.

Кроме того, протоколы на эллиптических кривых обеспечиваю увеличенную стойкость, так как не известны субэкспоненциальные алгоритмы вскрытия таких систем.

В ходе работы были изучены эллиптические кривые и их применение в криптографии. Также были разработаны программы, которые реализовывают протоколы аутентификации Шнорра и Окамото на эллиптической кривой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. М.: Научное изд-во ТВП, 2001. 254 с.

2 Болотов, А. А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А. А. Болотов, С. Б Гашков, А. Б. Фролов, А. А. Часовских. М.:КомКинга, 2006. 328 с.

3 Мао, Венбо. Современная криптография: теория и практика / Венбо Мао. М.: Издательский дом «Вильямс», 2005. 768 с.

4 Смит, Ричард, Э. Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. М. : Издательский дом «Вильямс», 2002. 432 с.

5 Афанаьев А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов. Изд-во «Горячая линия – Телеком», 2009. 552 с.

6 Zviran, M. Identification and Authentication: Technology and Implementation Issues / M. Zviran, Z. Erlich // Communications of Association for Information Systems. 2006. Vol. 17. C. 90-105.

7 Menezes, Alfred J. Handbook of Applied Cryptography / Alfred J. Menezes, Jonathan Katz, Paul C. van Oorschot, Scott A. Vanstone. CRC Press, 1996. 810 с.

8 Онацкий, А.В. Криптографические протоколы доказательства с нулевым разглашением на эллиптических кривых / А.В. Онацкий, О.В. Жарова // Цифровые технологии. №18, 2015. С. 153-164

9 Ященко, В. В. Введение в криптографию / В. В. Ященко. М.: Изд-во МЦНМО, 2012. 348 с.

10 Efficient identification and signatures [Электронный ресурс]. URL: https://pdfs.semanticscholar.org/8d69/c06d48b618a090dd19185aea7a13def894a5.pdf (дата обращения 13.01.2019). Загл. с экрана. Яз. англ.

11 Advanced Cryptography [Электронный ресурс]. URL: https://cs.nyu.edu/courses/spring07/G22.3220-001/lec2.pdf (дата обращения 13.01.2019). Загл. с экрана. Яз. англ.

12 Stinson, R. Douglas, Cryptography: Theory and Practice, Third Edition / Douglas R. Stinson. CRC Press, 2005. 616 с.

13 О применении эллиптических кривых в некоторых протоколах аутентификации и распределения ключей [Электронный ресурс]. URL: http://apu.npomars.com/images/pdf/48_5.pdf (дата обращения 13.01.2019). Загл. с экрана. Яз. англ.

14 U.S. Department of Commerce/National Institute of Standards and Technology. [Электронный ресурс]. URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (дата обращения 13.01.2019). Загл. с экрана. Яз. англ.

15 Elliptic Curve Cryptography in Practice [Электронный ресурс] // Cryptology ePrint Archive: Report 2013/734 [Электронный ресурс]. URL: https://eprint.iacr.org/2013/734.pdf (дата обращения 13.01.2019). Загл. с экрана. Яз. англ.