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

Арифметические операции на гиперэллиптических кривых

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Белышевой Оксаны Александровны

Научный руководитель
доцент, к.ф.-м.н. _____ А. Н. Гамова
18.01.2019 г.

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

Саратов 2019

ВВЕДЕНИЕ

В 1989 году Коблиц предложил использовать в криптографии гиперэллиптические кривые как альтернативу эллиптическим кривым. В отличие от эллиптических кривых, точки гиперэллиптической кривой не образуют группы. Однако аддитивную абелеву группу можно построить с использованием дивизоров. Порядок такой группы значительно превышает количество точек кривой, что позволяет достигать приемлемой стойкости при меньшем размере основного поля. Прямые и обратные криптографические преобразования в этом случае являются более сложными. До недавнего времени исследовательское сообщество считало, что криптографические преобразования на гиперэллиптических кривых выходят за рамки практического применения. Однако, последние улучшения в алгоритмах для вычисления группового закона имеют тенденцию доказывать, что криптосистемы, основанные на гиперэллиптических кривых, могут быть конкурентоспособными. Кроме того, при обеспечении примерно одинаковой степени защиты данных в системах на гиперэллиптических кривых требуется на порядок меньшая длина ключа, чем по сравнению, например, с широко распространенной системой RSA или эллиптическими кривыми. Это свойство востребовано в связи с потребностью в быстрых асимметричных алгоритмах, для небольших устройств. Также до настоящего времени не разработаны эффективные алгоритмы взлома таких систем.

Сегодня в мире ведутся интенсивные работы по изучению стойкости преобразований гиперэллиптических кривых. Возможно, этот математический аппарат будет использован в новых стандартах цифровой подписи и направленного шифрования. В настоящее время принят ряд стандартов цифровой подписи, основанных на эллиптических кривых, которые вполне удовлетворяют требуемому уровню секретности. Однако увеличение мощности вычислительной техники и развитие методов

криптоанализа в скором будущем может привести к снижению стойкости таких преобразований. Таким образом актуальность проблемы обусловлена, прежде всего, постоянно возрастающими вычислительными мощностями, посредством которых используемые в современных криптосистемах алгоритмы могут быть взломаны.

Дипломная работа посвящена разработке программной реализации алгоритмов арифметических операций на гиперэллиптических кривых и демонстрации работы протокола цифровой подписи. Для достижения этой цели было поставлено несколько задач.

1. Рассмотрение алгоритмов, позволяющих производить операции над элементами группы, образуемой гиперэллиптической кривой, а также их программная реализация;
2. Исследование алгоритмов поиска кривых, подходящих для использования в криптографии;
3. Программная реализация алгоритма верификации и создания цифровой подписи на гиперэллиптических кривых.

Дипломная работа состоит из введения, 10 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 105 страниц, из них 55 страниц – основное содержание, включая 17 рисунков и 6 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В главе 1 вводятся основные определения, связанные с гиперэллиптическими кривыми, уравнение гиперэллиптической кривой и ее свойства. Также приведено объяснение, почему в качестве элементов группы гиперэллиптической кривой нельзя брать точки. В этой главе рассматриваются функции на кривой и вводятся понятия нуля и поля, которые в главе 2 будут использоваться для введения дивизоров.

Глава 2 посвящена знакомству с дивизорами гиперэллиптической кривой. Приведены определения, связанные с дивизорами, их виды. На базе этого вводится понятие якобиана кривой – он является группой гиперэллиптической кривой. Далее рассмотрен один из самых эффективных способов представления дивизоров – представление Мамфорда, в виде пары многочленов. В дальнейшем это представление используется в последующих главах и в практической реализации.

В главе 3 рассмотрены арифметические операции над дивизорами. В этой главе также продемонстрировано сложение дивизоров с геометрической точки зрения. Для выполнения операции сложения в общем случае рассмотрен алгоритм Кантора и приведена его модификация в случае удвоения дивизора. В качестве алгоритм скалярного произведения приведен бинарный метод, который базируется на операциях сложения и удвоения. Сделаны выводы, о том, что для создания криптосистем являются пригодными кривые только 2 и 3 рода. Затем представлена таблица сравнения для алгоритма Кантора и точной формулы, в которой можно увидеть порядок эффективности применения точной формулы для сложения дивизоров.

В главе 4 приведена схема цифровой подписи на гиперэллиптических кривых (HECDSA). В основе алгоритмов ее формирования и проверки лежит операция скалярного произведения над дивизорами, рассмотренная ранее в главе 3. Преимущества алгоритма цифровой подписи на гиперэллиптических кривых в более малой длине ключа и в более высокой надежности,

обоснованной сложным математическим аппаратом; однако у его сложности есть и другая сторона – она является причиной более низкой производительности алгоритма. Однако в области повышения скорости выполнения операций над дивизорами в настоящее время ведется активная работа.

Глава 5 посвящена рассмотрению метода поиска наиболее подходящих с точки зрения криптографии гиперэллиптических кривых. В данном алгоритме рассчитывается порядок якобиана, который крайне необходим для выполнения операций над его элементами, к тому же от количества элементов якобиана напрямую зависит надежность криптографической системы, построенной на его основе.

В главе 6 приведен алгоритм генерации случайного дивизора на гиперэллиптической кривой. На основании глав 5 и 6 создаются общие параметры, которые используются в программной реализации HECDSA.

В главах 7 и 8 рассматриваются алгоритмы для арифметических операции для элементов бинарного и конечного поля простой характеристики, соответственно. Операции над элементами поля являются основополагающими для программной реализации.

В главе 9 приведены алгоритмы для умножения и деления элементов кольца многочленов. Данные алгоритмы также являются основополагающими для программной реализации арифметических операций над гиперэллиптическими кривыми.

В главе 10 описывается программная реализации всех описанных выше алгоритмов и даны инструкции по использованию данного программного обеспечения.

ЗАКЛЮЧЕНИЕ

В результате выполнения работы были обнаружены следующие достоинства и недостатки криптосистем на гиперэллиптических кривых.

Одним из главных достоинств этих систем является более высокая криптостойкость, при меньшей длине ключа, что позволит использовать алгоритмы на гиперэллиптических кривых на устройствах с ограниченной памятью.

К недостаткам же гиперэллиптической криптографии, относится высокая сложность применяемых в ней алгоритмов и множество тонкостей, которые необходимо учитывать при построении криптосистемы. При массовом переходе это может послужить причиной большого количества уязвимостей, которые уже были отработаны для более привычных, традиционных методов.

Еще одним недостатком данных криптосистем является более низкая производительность по сравнению с системами на эллиптических кривых. Однако, в настоящее время в мире ведутся интенсивные работы по изучению алгоритмов, которые могут существенно повысить скорость работы систем на гиперэллиптических кривых. И вполне возможно, что уже скоро этот математический аппарат будет использоваться в новых международных стандартах цифровой подписи и направленного шифрования.

Согласно цели работы были рассмотрены теоретические аспекты базисных арифметических операций на гиперэллиптических кривых. Для программной реализации в качестве языка программирования было решено выбрать Java, который является объектно-ориентированным и предоставляет множество полезных при решении поставленной задачи возможностей. В результате была получена библиотека с арифметическими операциями над дивизорами гиперэллиптической кривой. Эта библиотека может быть использована как универсальный инструмент для построения всевозможных криптосистем на гиперэллиптических кривых. Для демонстрации

корректности работы арифметических операций над дивизорами представлена цифровая подпись на гиперэллиптических кривых. Таким образом, практические задачи сформулированные в вводной части данной работы можно считать успешно выполненными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Scheidler, R. An Introduction to Hyperelliptic Curve Arithmetic [Электронный ресурс] URL: people.ucalgary.ca/~rscheidl/Papers/IntroHCA.pdf (дата обращения: 6.11.2018) Загл. с экрана. Яз. англ.

2 Ростовцев, А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. Санкт-Петербург: НПО «Профессионал», 2004. 486с.

3 Washington, L. C. Elliptic curves: number theory and cryptography / L. C. Washington. Maryland, U.S.A: University of Maryland College Park, 2008. 524с.

4 Blake, I. F. Advances in Elliptic Curve Cryptography / I. F. Blake, G. Seroussi, N. P. Smart. Cambridge University Press, 2005. 299с.

5 Бессалов, А.В. Представление элементов якобиана гиперэллиптической кривой рода 2 / А.В. Бессалов, Д.Б. Третьяков [Электронный ресурс] URL: http://elibrary.kubg.edu.ua/1494/1/A_Bessalov_D_Tretjakov_SZI_4_2010_IS_IM.p dp (Дата обращения: 05.12.2018) Загл. с экрана.

6 Sadanandan, S. ADDITION IN JACOBIAN OF HYPERELLIPTIC CURVES / S. Sadanandan. Indian Institute of Technology Madras Germany India, 2004. [Электронный ресурс] URL: http://wwwmayr.informatik.tu-muenchen.de/personen/sadanand/local_files/MTechThesis.pdf (Дата обращения: 07.12.2018).

7 Неласая, А.В. Протокол цифровой подписи на гиперэллиптических кривых / А.В. Неласая // Радіоелектроніка. Інформатика. Управління, 2006. С.113-117. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/protokol-tsifrovoy-podpisi-na-giperellipticheskih-krivyh (Дата обращения 07.12.2018).

8 Cohen, H. Handbook of Elliptic and Hyperelliptic Curve Criptography/ H. Cohen, G. Frey. Chapman & Hall/CRC, 2006. 805 с.

9 Неласая, А.В. Программная реализация криптографических операций на гиперэллиптических кривых / Долгов В. И., Неласая А. В. //Системи обробки інформації, 2010. №. 3. С. 17-19.

10 Katagi, M. Novel efficient implementations of hyperelliptic curve cryptosystems using degenerate divisors / M. Katagi, I. Kitamura, T. Takagi, T. Akishita. WISA LNCS 2004, № 3325, С. 345 – 359.

11 Неласая, А.В. Теоретическая и экспериментальная оценка сложности криптографических преобразований на эллиптических и гиперэллиптических кривых/ Неласая А. В., Долгов В. И. Системи обробки інформації, 2010. №. 7. С. 82-86.

12 Болтнев, Ю.Ф. Реализация алгоритма поиска гиперэллиптических кривых, подходящих для криптографии/ Ю.Ф. Болтнев // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2006 № 10 С.101-105. [Электронный ресурс] URL: cyberleninka.ru/article/n/realizatsiya-algoritma-poiska-giperellipticheskih-krivyh-podhodyaschih-dlya-kriptografii (Дата обращения 07.12.2018).

13 Соловьев, Ю.П. Эллиптические кривые и современные алгоритмы теории чисел/ Ю.П. Соловьев, В.А. Садовничий, Е.Т. Шавгулидзе, В.В. Белокуровю. Москва-Ижевск: Институт компьютерных исследований, 2003. 192 стр.

14 Perlzl, J. Hyperelliptic Cryptosystems on Embedded Microprocessors / J. Pelzl [Электронный ресурс] URL: emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2010/04/da_pelzl.pdf (Дата обращения: 10.12.2018).

15 Самсонов, Б. Б. Теоретическая криптография / Б. Б. Самсонов, Е. М. Плохов, А. И. Филоненков. Ростов-на-Дону: Феникс, 2002. 512с.

16 Поштаренко, В. М. РАЗРАБОТКА КЛАССА ДЛЯ РАБОТЫ С ЭЛЕМЕНТАМИ ПОЛЕЙ GF(2^m)/ В. М. Поштаренко, А. Ю. Варлыгина // Вестник Национального технического университета Харьковский политехнический институт. Серия: Информатика и моделирование, 2006. С.118-124.

17 Hankerson, D. Guide to Elleptic Curve Cryptography / D. Hankerson, A. Menezes, S. Vanstone. Springer-Verlag New York, 2004. 311с.

18 Thamer, F.A.A. Finite Field Arithmetic (Galois field) [Электронный ресурс] / Thamer F.A.A. // Information Theory 4th Class in Communication URL: uotechnology.edu.iq/depeee/lectures/4th/Communication/Information%20theory/8.pdf (дата обращения 30.11.2018) Загл. с экрана. Яз. англ.
19 Cohen, H. A. Course in Computational Algebraic Number Theory / H. Cohen. New York: Springer, 1996/ 563 с.
20 Герберт, Ш. Java 8. Руководство для начинающих / Ш. Герберт.; Пер. с англ. А. Г. Гузикевич - М.: Диалектика, Вильямс, 2015. - 899 с.