Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Схема цифровой подписи на гиперэллиптических кривых

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы
специальности 090102.65 «Компьютерная безопасность»
факультета компьютерных наук и информационных технологий
Дорофеевой Анастасии Дмитриевны

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

Заведующий кафедрой
профессор, к.ф.-м.н. В.Н. Салий

Саратов 2016

ВВЕДЕНИЕ

Идея о том, что группы, получаемые из гиперэллиптических кривых, подходят для криптосистем, основанных на проблеме дискретного логарифмирования, была впервые выдвинута в 1988 году Нилом Коблицем. Однако долгое время гиперэллиптические кривые не использовались в криптосистемах по причине сложности групповых вычислений, ведущих к худшей производительности по сравнению с другими криптографическими системами. Растущий интерес к подобным системам возник совсем недавно, и за последнее десятилетие было разработано множество криптографических алгоритмов, построенных на гиперэллиптических кривых. Отдельной интересной исследовательской задачей является поиск методов повышения производительности таких криптосистем, и в этом направлении в настоящее время также активно ведется работа. Таким образом, заявленная тема является очень актуальной.

Основной целью данной работы является исследование математического аппарата, позволяющего построить криптосистему на гиперэллиптических кривых. В связи с этим было поставлено несколько задач.

1. Исследование алгоритмов, позволяющих производить операции над элементами группы, образуемой гиперэллиптической кривой, а также их программная реализация; другими словами, написание библиотеки, позволяющей совершать арифметические операции над дивизорами гиперэллиптической кривой;

2. Исследование алгоритмов поиска кривых, подходящих для использования в криптографии;

3. Исследование базового протокола цифровой подписи на гиперэллиптических кривых и последующая программная реализациея этого протокола с помощью результатов, полученных при выполнении двух предыдущих пунктов.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В **главе 1** приводятся основные определения, связанные с гиперэллиптическими кривыми, уравнение гиперэллиптической кривой, ее свойства. Так же, в пункте 2 главы 1, рассмотрен групповой закон для гиперэллиптических кривых, проведено его сравнение с групповым законом на эллиптических кривых, приведено объяснение, почему в качестве элементов группы гиперэллиптической кривой нельзя брать точки и какую роль в этом случае играют дивизоры гиперэллиптической кривой.

Глава 2 посвящена знакомству с дивизорами гиперэллиптической кривой. В пункте 1 приведены определения, связанные с дивизорами, их основные свойства. На базе этого вводится понятие якобиана кривой – он является группой гиперэллиптической кривой. В пункте 2 рассмотрен один из самых распространенных способов представления дивизоров – представление Мамфорда, в виде пары многочленов. Именно в этом виде дивизоры и рассматриваются в последующих главах.

В **главе 3** рассмотрены операции над дивизорами – сложение, удвоение, скалярное произведение. В первом пункте приведены общие алгоритмы – алгоритм Кантора (сложение), лестница Монтгомери (скалярное произведение). Алгоритм скалярного произведения – самый основной, он базируется на операциях сложения и удвоения.

Затем, в пунктах 2 и 3, рассматриваются алгоритмы, рекомендованные к использованию в целях повышения производительности алгоритма скалярного произведения – алгоритмы сложения и удвоения, применимые для кривых определенного рода и обладающие большей скоростью, чем универсальный алгоритм Кантора. При этом для каждого из приведенных алгоритмов проведена оценка его сложности.

Глава 4 посвящена рассмотрению методов подсчета точек якобиана гиперэллиптической кривой над конечным полем. Знать порядок якобиана крайне необходимо для выполнения операций над его элементами, к тому же от количества

элементов якобиана напрямую зависит надежность криптографической системы, построенной на его основе.

В пункте 1 вводится понятие дзета-функции кривой, которая используется далее практически во всех рассмотренных в данной главе алгоритмах. В пункте 2 приведено описание нескольких алгоритмов подсчета точек якобиана, каждый из которых рассчитан на конкретное семейство кривых. Далее, в пункте 3, на основе одного из них – алгоритма Сакая-Сакурая – составлен метод анализа гиперэллиптических кривых и поиска среди них наиболее подходящих для использования в криптографии.

В **главе 5** рассматриваются особенности криптосистем на арифметических (в частности – эллиптических и гиперэллиптических) кривых. Приведено обоснование их криптостойкости.

В пункте 2 приведена достаточно популярная на сегодняшний день схема цифровой подписи на эллиптических кривых (ECDSA), рассматриваются ее основные достоинства и недостатки.

В пункте 3 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. Далее, в пункте 4, рассматривается одна из ее модификаций – коллективная подпись на гиперэллиптических кривых, которая может быть использована для обеспечения юридической силы коллективных электронных документов. В ходе сравнения алгоритмов подписи на эллиптических и гиперэллиптических кривых сделан вывод, о котором в двух словах можно сказать так: преимущество алгоритма на гиперэллиптических кривых в более малой длине ключа и в более высокой надежности, обоснованной более 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.

ЗАКЛЮЧЕНИЕ

На сегодняшний день криптопреобразования на эллиптических кривых вполне удовлетворяют требуемому уровню секретности. Однако увеличение мощностей вычислительной техники и развитие методов криптоанализа в скором будущем может привести к снижению стойкости таких преобразований. Следовательно, актуальными являются задачи исследования стойкости и сложности криптоалгоритмов, лежащих в основе процедур формирования и проверки цифровой подписи, а также поиска новых математических структур, являющихся источником абелевых групп для криптографических приложений и разработка криптографических систем на их основе. В связи с этим достаточно большое внимание в последнее время уделяется исследованиям криптосистем на гиперэллиптических кривых. На основании этого можно сказать, что тема данной работы является очень актуальной.

Практические задачи, сформулированные во вводной части данной работы, можно считать успешно выполненными. В первую очередь, был реализован математический аппарат для выполнения операций над дивизорами гиперэллиптической кривой. Полученная библиотека может быть использована как универсальный инструмент для построения всевозможных криптосистем на ГЭК. В частности, ее работоспособность была продемонстрирована в ходе реализации алгоритмов формирования и проверки ЦП на гиперэллиптических кривых.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Васильев А.В. Высшая алгебра. Конспект лекций. Часть 1 / А.В. Васильев, В.Д. Мазуров [Электронный ресурс] / URL: http://math.nsc.ru/~vasand/algebra_small.pdf (Дата обращения: 2.05.2015)
2. Cohen, H. Handbook of Elliptic and Hyperelliptic Curve Criptography/ H. Cohen, G. Frey – Chapman & Hall/CRC, 2006 – 805 с.: ил. – Библиогр.: с. 737.
3. Хабрахабр [Электронный ресурс] / Эллиптическая криптография: теория / URL: http://habrahabr.ru/post/188958/ (Дата обращения 16.11.2015)
4. Федеральный закон от 10.01.2002 № 1-ФЗ (ред. от 08.11.2007) «Об электронной цифровой подписи» [Электронный ресурс] / КонсультантПлюс / URL:http://www.consultant.ru/document/cons_doc_LAW_34838/7f756f0b351492331efccfd82ac5f928dcf7bbea (Дата обращения 10.11.2015)
5. Menezes A.J. An elementary introduction to hyperelliptic curves / A.J. Menezes, Yi-Hong Wu, Robert J. Zuccherato [Электронный ресурс] / URL: http://www.math.uwaterloo.ca/~ajmeneze/publications/hyperelliptic.pdf (Дата обращения: 20.10.2015)
6. Алешников С.И. Построение системы защита данных на основе гиперэллиптических кривых / С.И. Алешников, А.А. Горбачев [Электронный ресурс] / Pandia.ru : энциклопедия знаний – URL: http://www.pandia.ru/text/78/387/42477.php (Дата обращения: 20.05.2014)
7. Mircea Mustata. Zeta functions in algebraic geometry / Mircea Mustata [Электронный ресурс] / URL: http://www.math.lsa.umich.edu/~mmustata/zeta_book.pdf (Дата обращения: 12.10.2015)
8. Ильяшенко И.Д. Обзор эффективных алгоритмов подсчета числа точек якобиана гиперэллиптической кривой над конечным полем / И.Д. Ильяшенко [Электронный ресурс] / URL: http://journals.kantiana.ru/vestnik/218/610/ (Дата обращения: 12.10.2015)

9. Koblitz, N. Algebraic aspects of cryptography / N. Koblitz [Электронный ресурс] / URL: https://www.emsec.rub.de/media/crypto/attachments/files/2010/04/thesis_andy_rupp.pdf (Дата обращения 12.10.2015)

10. Colm O hEigeartaigh. A Comparison of Point Counting methods for Hyperelliptic Curves over Prime Fields and Fields of Characteristic 2 / Colm O hEigeartaigh [Электронный ресурс] / URL: https://eprint.iacr.org/2004/241.pdf (Дата обращения: 22.10.2015)

11. 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.pdp (Дата обращения: 19.09.2015)

12. Effective generalized equation of secure hyperelliptic curve digital signature algorithms [Электронный ресурс] // The Journal of China Universities of Posts and Telecommunications - April 2010, 17(2): с.100 – 108 [Электронный ресурс] / URL: http://cs.ucsb.edu/~koc/ccs130h/notes/effective-digit-sign-alg.pdf (Дата обращения 13.11.2015)

13. Johnson, D. The Elliptic Curve Digital Signature Algorithm (ECDSA) / D. Johnson, A. Menezes, S. Vanstone [Электронный ресурс] / URL: http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf (Дата обращения 23.11.2015)

14. Неласая А.В. Протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых / А.В. Неласая, Г.Л. Козина, Н.А. Молдовян // Радіоелектроніка. Інформатика. Управління. – 2008. №1(19). С.127-133. [Электронный ресурс] / URL: http://csit.narod.ru/ric/riu_2008_1.pdf (Дата обращения 17.12.2015)

15. Costello, C. Group Law Computations on Jacobians of Hyperelliptic Curves / C. Costello, K. Lauer. [Электронный ресурс] / URL: https://eprint.iacr.org/2011/306.pdf (Дата обращения: 2.05.2014)

16. Scholten, J. An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU Cryptosystem / J. Scholten, F. Vercauteren [Электронный ресурс] / URL: http://www.cse.iitk.ac.in/users/nitin/courses/WS2010-ref4.pdf (Дата обращения: 15.12.2015)

17. Ковтун В. Криптография с открытым ключом / В. Ковтун [Электронный ресурс] / URL: http://www.nrjetix.com/fileadmin/doc/publications/additional_info/public_key_cryptography_-_lecture.pdf (Дата обращения: 20.12.2015)

18. Неласая А.В. Протокол цифровой подписи на гиперэллиптических кривых / А.В. Неласая // Радіоелектроніка. Інформатика. Управління. – 2006. № 1(15). – С. 113-118 [Электронный ресурс] / URL: http://csit.narod.ru/ric/riu_2006_1.pdf (Дата обращения 15.12.2015)

19. Hankerson, D. Guide to Elleptic Curve Cryptography / D. Hankerson, A. Menezes, S. Vanstone [Электронный ресурс] / URL: http://math.boisestate.edu/~liljanab/MATH508/GuideEllipticCurveCryptography.PDF (Дата обращения 10.12.2015)

20. Hankerson, D. Software Implementation of Elliptic Curve Cryptography over Binary Fields / D. Hankerson, J. L. Hernandez, A. Menezes [Электронный ресурс] / URL: http://link.springer.com/chapter/10.1007 (Дата обращения 10.11.2015)

21. Cohen, H. A Course in Computational Algebraic Number Theory / H. Cohen [Электронный ресурс] / URL: http://www.plouffe.fr/simon/math/A%20course%20in%20computational%20algebraic%20number%20theory%20-%20Cohen.pdf (Дата обращения 10.12.2015)

22. Menezes, A.J. Handbook of Applied Cryptography / A. J. Menezes, P. C. Oorschot, S.A. Vanstone [Электронный ресурс] / URL: http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2838&rep=rep1&type=pdf (Дата обращения 10.12.2015)

23. Pelzl, J. Hyperelliptic Cryptosystems on Embedded Microprocessors / J. Pelzl [Электронный ресурс] / URL: http://psquare.de/pelzl/papers/da_pelzl.pdf (Дата обращения: 10.12.2015)

…