Современные инновации, системы и технологии // Modern Innovations, Systems and Technologies

2023; 3(2)
eISSN: 2782-2818
https://www.oajmist.com

УДК: 004.428.4
DOI: https://doi.org/10.47813/2782-2818-2023-3-2-0225-0233

EDN: LNFAHM

Java библиотека для работы с эллиптическими кривыми

В. Д. Хазиева

Казанский (Приволжский) федеральный университет, Казань, Россия

Аннотация. В настоящее время эллиптическая криптография активно используются в протоколах SSH, в криптовалютах, в протоколах электронного голосования и во многих других сферах. В подобных информационных системах ставится упор на высокий уровень безопасности и повышенную производительность используемых криптографических примитивов, что обуславливает актуальность проведения анализа и реализации различных методов эллиптической криптографии. В данной статье дается описание разработанной под язык Java криптографической библиотеки для работы с эллиптическими кривыми. Библиотека содержит реализацию основных операций для таких форм кривых как: каноническая кривая Вейерштрасса, кривая Эдвардса, квартика Якоби. Были реализован функционал для различных координатных представлений точек, а также реализованы алгоритмы скалярного умножения такие как: NAF, mbNAF и их “оконные” варианты, лестница Монтгомери. Приводится сравнение быстродействия реализации стандарта электронной цифровой подписи ECDSA с существующим решением из пакета java.security.

Ключевые слова: криптография, эллиптические кривые, операции с точками на эллиптических кривых, стандарты электронной цифровой подписи, разработка библиотеки на языке Java.

Для цитирования: Хазиева, В. Д. (2023). Java библиотека для работы с эллиптическими кривыми. Современные инновации, системы и технологии - Modern Innovations, Systems and Technologies, 3(2), 0225–0233. https://doi.org/10.47813/2782-2818-2023-3-2-0225-0233

Java library designed to work with elliptic curves

Vera Khazieva

Kazan (Volga Region) Federal University, Kazan, Russia

Abstract. Currently, elliptical cryptography is actively used in SSH protocols, in cryptocurrencies, in electronic voting protocols and in many other areas. In such information systems, emphasis is placed on a high level of security and increased performance of the cryptographic primitives used, which determines the relevance of the analysis and implementation of various methods of elliptic cryptography. This article describes a cryptographic library developed for the Java language for working with elliptic curves. The library contains the implementation of basic operations for such forms of curves

as: canonical Weierstrass curve, Edwards curve, Jacobi quartic. Functionality was implemented for various coordinate representations of points, as well as scalar multiplication algorithms such as: NAF, mbNAF and their “window” variants, the Montgomery ladder. A comparison of the performance of the implementation of the ECDSA electronic digital signature standard with the existing solution from the java.security package is given.

Keywords: cryptography, elliptic curves, operations with points on elliptic curves, electronic digital signature standards, Java library development.

For citation: Khazieva, V. D. (2023). Java library designed to work with elliptic curves. Modern Innovations, Systems and Technologies, 3(2), 0225–0233. https://doi.org/10.47813/2782-2818-2023-3-2-0225-0233

ВВЕДЕНИЕ

В настоящее время эллиптические кривые (далее – ЭК) широко используются в криптографии: существует алгоритм Ленстры для факторизации, а также алгоритм проверки числа на простоту на основе ЭК; были разработаны стандарты электронной цифровой подписи (далее – ЭЦП) и шифрования, протокол Диффи-Хеллмана. Данная область криптографии активно развивается и является перспективной [1-4], поэтому для проведения исследований и для разработки новых продуктов и алгоритмов в этой сфере очень удобным становится использование библиотеки, которая бы содержала базовые арифметические операции с точками на эллиптических кривых. Обзор существующих криптографических пакетов для различных языков программирования показал, что зачастую в них отсутствует возможность использования базовых функций (например сложение, скалярное умножение точек и др.), а также поддерживается ограниченное число определенных кривых. Для языка Java существует библиотека ECCelerate, однако в ней нет возможности выбора определенного алгоритма скалярного умножения и выбора, в каких координатах будут представлены точки кривой, нет операции утроения точки и операции пятикратного увеличения по упрощенным формулам, а также нет возможности добавления данного пакета к проекту через фреймворк Apache Maven. Исходя из вышеперечисленных факторов была реализована новая криптографическая Java библиотека для работы с эллиптическими кривыми.

МАТЕРИАЛЫ И МЕТОДЫ

Из общего уравнения Вейерштрасса (1) выводятся уравнения для форм кривых, каждая из которых обладает специфическим набором свойств и формулами для основных операций.

$$y^2 + ay + b = x^3 + cx^2 + dx + e \quad (1)$$

В данной библиотеке были реализованы: каноническая кривая Вейерштрасса, кривая Эдвардса (а также ее скрученный вариант) [5], квартика Якоби [6]. Две последние кривые вызывают большой интерес, поскольку нахождение суммы двух точек, а также удвоение точки на них можно реализовать с меньшими затратами по времени по сравнению с другими формами кривых.

Основными операциями считаются: сложение/вычитание двух различных точек, удвоение и утроение точки (в некоторых случаях можно вывести формулы для пятикратного увеличения), а также скалярное умножение точки, которое реализуется через описанные выше операции. Существует база данных для ЭК [7], созданная математиками Д. Бернштейном и Т. Ланге, которая содержит выведенные формулы для вычисления операций над точками для разных форм кривых. Данная база активно использовалась при реализации данной библиотеки.

Для применения ЭК в криптографии необходимо брать кривые над некоторыми конечными полями. Соответственно приходится иметь дело с модулярной арифметикой и большими числами. В Java есть дополнительный тип данных – BigInteger, разработанный специально для таких вычислений. Многие модулярные функции с этим типом данных имеют оптимизации.

Помимо базовых операций в данной библиотеке были реализованы стандарты ЭЦП: ECDSA [8] и ГОСТ 34.10-2018. Для их создания были использованы криптографические примитивы такие как: символ Лежандра, вероятностный тест простоты Миллера-Рабина, а также алгоритм Тонелли-Шенкса.

Для проведения тестирования использовался фреймворк JUnit. Сборка и развертывание проводилось при помощи фреймворка Apache Maven.

РЕЗУЛЬТАТЫ

Было выделено два абстрактных класса: Elliptic_curve (ЭК) и Signature (ЭЦП). Каждый абстрактный класс имеет классы, которые его реализуют: для ЭК это определенные формы кривых, а для ЭЦП это классы стандартов ECDSA и ГОСТ 34.10-2018. На рисунке 1 представлена UML-диаграмма классов проекта.

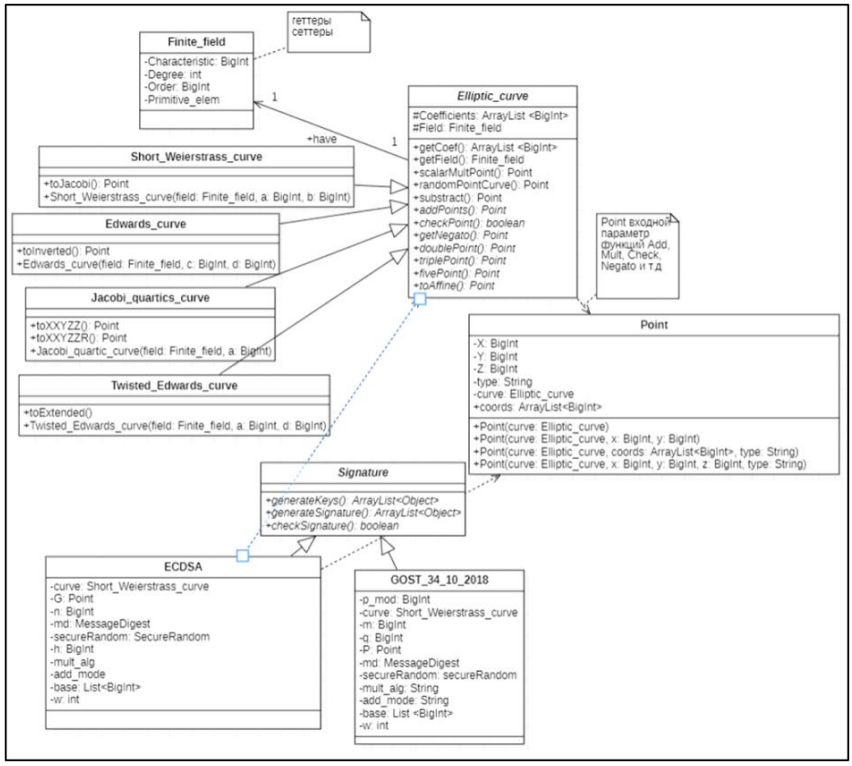

Рисунок 1. UML-диаграмма классов проекта.

Figure 1. UML class diagram of the project.

Функция скалярного умножения - scalarMultPoint() представлена в двух формах. Первая реализует метод умножения mbNAF [9], а вторая методы: удвоения-сложения (double-and-add), NAF метод (binary_NAF), NAF метод с некоторым окном предвычислений (NAF_w), а также метод лестницы Монтгомери (montgomery_ladder). Обе реализации принимают на вход параметр add_mode, который устанавливает в каком координатном представлении будет происходить умножение. Перевод в аффинные координаты в конце не производится – это действие остается на усмотрении пользователя. Вторая реализация принимает на вход параметр alg_name, указывающий алгоритм скалярного умножения.

В классах ECDSA и GOST_34_10_2018 при формировании основных параметров было необходимо находить произвольную точку на кривой. Специально для этого была написана функция randomPointCurve(), реализация которой использовала алгоритм Тонелли-Шенкса. Также были добавлены конструкторы, в которых параметр curve (эллиптическая кривая) может быть выбран из списка рекомендованных кривых, включая рекомендации NIST [10] и рекомендации Росстандарта [11].

В ходе работы было проведено сравнение методов ECDSA для создания электронной подписи, реализованных в данном проекте, с существующими решениями

в этой области, включая класс Signature из пакета java.security. Были рассмотрены кривые P-256, P-384 и P-512. На рисунке 2 представлен график, полученный в результате проведенного исследования.

Рисунок 2. Сравнение быстродействия реализаций ECDSA.

Figure 2. Performance comparison of ECDSA implementations.

С целью обеспечения доступности данной библиотеки для любого Java-разработчика, было принято решение опубликовать артефакт в центральном репозитории Maven Central. На рисунке 3 представлена информация о проекте, доступная на сайте MVN Repository после его размещения.

Рисунок 3. Информация об опубликованном артифакте.

Figure 3. Information about the published artifact.

ОБСУЖДЕНИЕ

Посмотрим на результаты исследования, касающиеся производительности ECDSA (см. рисунок 2). На кривых P-256 и P-384 оба подхода демонстрируют примерно одинаковую производительность (с разницей, которая достигает до 3 миллисекунд), однако на кривой P-512 мы наблюдаем явное преимущество использования java.security, с выигрышем до 15 миллисекунд. Можно предположить, что это связано с применением особенностей обобщенных чисел Мерсенна [12], которые позволяют эффективно выполнять модулярные операции. Этот факт дает мотивацию к дальнейшим доработкам библиотеки.

В пакете java.security имеется класс Signature, предназначенный для работы с электронной цифровой подписью. Для использования ECDSA возможно задать алгоритм через параметр algorithm (например, SHA256withECDSA). Кривая может быть выбрана с помощью класса ECGenParameterSpec, где параметры кривых определены в соответствующей документации. Это означает, что определение собственных параметров для кривой может представлять проблему. С одной стороны, это обеспечивает защиту пользователя, не обладающего достаточными знаниями в криптографии, от выбора небезопасной кривой. Однако, с другой стороны, это ограничивает гибкость в выборе кривой. В данной библиотеке есть возможность использования кривых с пользовательскими параметрами, однако они сначала должны пройти валидацию (может произойти вызов исключения).

ЗАКЛЮЧЕНИЕ

Разработанная криптографическая библиотека для работы с эллиптическими кривыми может быть использована в качестве средства для изучения свойств различных эллиптических кривых, а также в качестве средства обеспечения информационной безопасности. В дальнейшем в библиотеку возможно добавление алгоритма EdDSA (ЭЦП на основе кривых Эдвардса), а также методов генерации параметров случайных кривых: например, при помощи алгоритма Шуфа или метода комплексного умножения. Стоит отметить, что созданный продукт удобен в плане подключения его к другим проектам (подключение зависимости при помощи Apache Maven), а также предоставляет пользователям возможность выбора различных алгоритмов скалярного умножения,

координатного представления точки, а также пользовательской кривой в алгоритмах электронной цифровой подписи.

СПИСОК ЛИТЕРАТУРЫ

[1] Mahto D., Khan D., Yadav D. Security analysis of elliptic curve cryptography and RSA: Proceedings of the World Congress on Engineering. 2016, June 29 - July 1; London, U.K.

[2] Gövem B., Järvinen K., Aerts K., Verbauwhede I., Mentens N. A fast and compact FPGA implementation of Elliptic Curve Cryptography using lambda coordinates: Proceedings of the 8-th International Conference on Cryptology in Africa - AFRICACRYPT 2016. 2016, April 13-15; Fes, Morocco. Cham: Springer; 2016: 63-83.

[3] Durairaj M., Muthuramalingam K. A new authentication scheme with Elliptical Curve Cryptography for internet of things (IoT) environments. Int. J. Engineering and Technology. 2018; 7 (2.26): 119-124.

[4] Luma A., Selimi B., Ameti L. Audio message transmitter secured through Elliptical Curve Cryptosystem. Int. J. Applied Mathematics, Electronics and Computers. 2014; 2(4): 54-58.

[5] Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография: монография. Киев: Політехника; 2017. 272.

[6] Василенко О.Н. О вычислении кратных точек на эллиптических кривых над конечными полями с использованием нескольких оснований систем счисления и новых видов координат. Математические вопросы криптографии. 2011. 2 (1): 5-28.

[7] Bernstein D., Lange T. Explicit-Formulas Database. URL: https://hyperelliptic.org/EFD/ (дата обращения: 01.05.2023).

[8] Hankerson D., Vanstone S., Menezes A. Guide to Elliptic Curve Cryptography. New York : Springer; 2004. 312.

[9] Miri A., Longa P. New Multibase Non-Adjacent Form Scalar Multiplication and its Application to Elliptic Curve Cryptosystems. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2008/052.pdf (дата обращения: 09.06.2023)

[10] FIPS PUB 186-4 Digital Signature Standard. Gaithersburg : Information Technology Laboratory National Institute of Standards and Technology; 2013. 77.

[11] Р 50.1.114-2016 – Параметры эллиптических кривых для криптографических алгоритмов и протоколов: дата введения 2016-11-28. М.: Стандартинформ; 2016. 15.

[12] Соколов А.А. Формирование цифровой подписи на основе эллиптических кривых.

Вестник магистратуры. 2015; 6 (45): 25-30.

REFERENCES

[1] Mahto D., Khan D., Yadav D. Security analysis of elliptic curve cryptography and RSA: Proceedings of the World Congress on Engineering. 2016, June 29 - July 1; London, U.K.

[2] Gövem B., Järvinen K., Aerts K., Verbauwhede I., Mentens N. A fast and compact FPGA implementation of Elliptic Curve Cryptography using lambda coordinates: Proceedings of the ъ8-th International Conference on Cryptology in Africa - AFRICACRYPT 2016. 2016, April 13-15; Fes, Morocco. Cham: Springer; 2016: 63-83.

[3] Durairaj M., Muthuramalingam K. A new authentication scheme with Elliptical Curve Cryptography for internet of things (IoT) environments. Int. J. Engineering and Technology. 2018; 7 (2.26): 119-124.

[4] Luma A., Selimi B., Ameti L. Audio message transmitter secured through Elliptical Curve Cryptosystem. Int. J. Applied Mathematics, Electronics and Computers. 2014; 2(4): 54-58.

[5] Bessalov A.V. Ellipticheskie krivye v forme Edvardsa i kriptografiya: monografiya [Elliptic curves in the Edwards form and cryptography: monograph]. Kyiv: Politekhnika; 2017. 272 (in Russian).

[6] Vasilenko O.N. O vychislenii kratnykh tochek na ellipticheskikh krivykh nad konechnymi polyami s ispol'zovaniem neskol'kikh osnovanii sistem schisleniya i novykh vidov koordinat [On the calculation of multiple points on elliptic curves over finite fields using several bases of number systems and new types of coordinates]. Matematicheskie voprosy kriptografii. 2011. 2 (1): 5-28 (in Russian).

[7] Bernstein D., Lange T. Explicit-Formulas Database. Available at: https://hyperelliptic.org/EFD/ (accessed: 01.05.2023).

[8] Hankerson D., Vanstone S., Menezes A. Guide to Elliptic Curve Cryptography. New York : Springer; 2004. 312.

[9] Miri A., Longa P. New Multibase Non-Adjacent Form Scalar Multiplication and its Application to Elliptic Curve Cryptosystems. Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2008/052.pdf (accessed: 09.06.2023).

[10] FIPS PUB 186-4 Digital Signature Standard. Gaithersburg : Information Technology Laboratory National Institute of Standards and Technology; 2013. 77.

[11] R 50.1.114-2016 – Parametry ellipticheskikh krivykh dlya kriptograficheskikh

algoritmov i protokolov: data vvedeniya 2016-11-28 [Elliptic Curve Parameters for Cryptographic Algorithms and Protocols: date of introduction 2016-11-28]. Moscow: Standartinform; 2016. 15 (in Russian).

[12] Sokolov A.A. Formirovanie tsifrovoi podpisi na osnove ellipticheskikh krivykh [Formation of a digital signature based on elliptic curves]. Vestnik magistratury. 2015; 6 (45): 25-30 (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Хазиева Вера Денисовна, факультет «Фундаментальная информатика и информационные технологии», ФГАОУ ВО «Казанский (Приволжский) федеральный университет», Казань, Россия
e-mail: vkhazieva@inbox.ru
ORCID: 0009-0003-6297-6041

Vera Khazieva, Faculty of Fundamental Informatics and Information Technologies, Kazan (Volga Region) Federal University, Kazan, Russia

Статья поступила в редакцию 02.06.2023; одобрена после рецензирования 15.06.2023; принята к публикации 16.06.2023.

The article was submitted 02.06.2023; approved after reviewing 15.06.2023; accepted for publication 16.06.2023.