ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

Әзірленген топтық қолтаңба хаттамалары кеңейтілген функционалдылыққа және қауіпсіздіктің жоғары деңгейіне ие инновациялық әдістер болып табылады. Оларды практикалық қолдану қаржылық транзакциялар, Құқықтану, мемлекеттік ұйымдар және т.б. сияқты әртүрлі салаларда қауіпсіздікті жақсартуға ықпал етуі мүмкін.

Топтық қолтаңбаларды одан әрі дамыту және зерттеу тиімдірек және сенімді хаттамаларды құруды, сондай-ақ қолданыстағы әдістерді жаңа технологиялық және құқықтық талаптарға бейімдеуді қамтуы мүмкін. Бұл электрондық жүйелердің қауіпсіздігін жақсартуға және олардың заманауи стандарттар мен нормативтерге сәйкестігін қамтамасыз етуге мүмкіндік береді.

Қолданылған әдебиеттер тізімі:

1. Menezes, A. J., Oorschot, P. C. van, & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
2. Коблиц, Н. (1994). A Course in Number Theory and Cryptography. Springer-Verlag.
3. Washington, L. C. (2008). Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC.
4. Stinson, D. R. (2005). Cryptography: Theory and Practice. Chapman and Hall/CRC.
5. Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. Springer.

УДК 004.4

ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Жолдубаева Диана Турлановна
diana-328@mail.ru
Магистрант 2 курса Евразийский национальный
университет имени Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Сулейменов К.М.

Аннотация

Данная статья исследует эффективные методы реализации цифровой подписи на основе эллиптической кривой. Эллиптические кривые представляют собой мощный математический инструмент, используемый в криптографии для обеспечения безопасности передачи данных. В статье рассматриваются основные принципы работы с эллиптическими кривыми в контексте цифровой подписи, а также предлагаются новые методы оптимизации для повышения скорости и безопасности подписи. Результаты исследования могут быть полезны для разработчиков криптографических систем, стремящихся к оптимальной и надежной реализации цифровой подписи на основе эллиптической кривой.

Введение

Цифровая подпись является одним из важнейших инструментов в современной криптографии, обеспечивающим аутентификацию и целостность данных. Одним из наиболее эффективных методов реализации цифровой подписи является использование эллиптических кривых. Эллиптические кривые обладают высоким уровнем безопасности при сравнительно небольшой длине ключа, что делает их привлекательным выбором для многих криптографических протоколов.

Определение эллиптической кривой

Эллиптическая кривая определяется уравнением вида:

$$y^2 = x^3 + ax + b$$

где a и b – коэффициенты кривой. Это уравнение задает набор точек *(x,y),* удовлетворяющих условию. Для выполнения операций над точками на кривой также требуется определить операцию сложения точек.

Операция сложения точек на кривой

Операция сложения точек на эллиптической кривой выполняется с помощью геометрических конструкций, таких как отражение, проведение прямых через две точки и нахождение их пересечения с кривой. Сложение точек на эллиптической кривой обладает особенностью ассоциативности, что позволяет строить алгоритмы умножения точек на кривой.

Параметры эллиптической кривой

Для безопасного применения эллиптических кривых в криптографии важно выбрать подходящие параметры *a, b* и простое число *p,* определяющее поле, над которым определена кривая. Выбор параметров кривой должен учитывать стойкость к различным атакам, включая атаки на основе математических методов и атаки перебором.

Основные принципы работы с эллиптическими кривыми в цифровой подписи

Эллиптические кривые используются в цифровой подписи с использованием алгоритмов, таких как ECDSA (Elliptic Curve Digital Signature Algorithm) или EdDSA (Edwards-curve Digital Signature Algorithm). Основной принцип заключается в использовании математических операций на точках эллиптической кривой для создания и проверки подписи.

Оптимизация процесса подписи

Для повышения эффективности процесса подписи на эллиптической кривой предлагаются различные методы оптимизации. Одним из таких методов является выбор оптимальной параметризации эллиптической кривой, что позволяет сократить количество операций, необходимых для выполнения подписи. Другие методы включают улучшения в алгоритмах скалярного умножения, таких как алгоритмы умножения с применением кратных скользящих окон и методы уменьшения числа операций деления.

Скалярное и мульти скалярное произведение

Общая схема алгоритмов как скалярного умножения (для показателя *k* и точки *P* вычислить *kP*), так и мульти скалярного умножения (для показателей *k1, k2* и точек *P, Q* вычислить *k1P + k2Q*) может быть описана следующим образом:

1. Предварительно вычислите набор точек *iP (iP, jQ или iP + jQ);*
2. Постройте специальное представление показателя степени k (специальное совместное представление пары *(k1, k2));*
3. Установите начальное значение результата равным бесконечной точке, затем “просканируйте” представление экспонент и для каждой цифры добавьте к результату соответствующее кратное соответствующей предварительно вычисленной точке.

Проблема состоит в том, чтобы минимизировать количество сложений, т. е. вес представления, в то время как количество умножений обычно определяется разрядностью экспонент.

Кривые Гесса и Эдвардса

Кривые Гесса и Эдвардса представляют собой особые классы эллиптических кривых, которые имеют свои уникальные математические свойства и применения в криптографии. Рассмотрим каждый из них подробнее:

Кривые Гесса получили свое название в честь математика Огюста Гесса, который впервые изучил эллиптические кривые этого типа. Кривые Гесса определяются уравнением вида:

$$H: Y^2Z = X^3 + aXZ^2 + bZ^3$$

a и b — коэффициенты кривой. Кривые Гесса обладают некоторыми уникальными математическими свойствами, которые могут быть использованы в криптографии для построения алгоритмов шифрования и подписи. Кривые Эдвардса были введены Харольдом Монтгомери Эдвардсом в 2007 году. Они определяются уравнением вида:

$$E: x^2 + y^2 = c^2(1 + dx^2y^2)$$

c и d — параметры кривой. Одно из важных свойств кривых Эдвардса — это их инвариантность относительно операции проективного преобразования, что делает их особенно подходящими для реализации криптографических протоколов.

Кривые Гесса и Эдвардса обладают высокой степенью безопасности и эффективности и широко используются в современной криптографии. Они могут использоваться в качестве основы для алгоритмов цифровой подписи, асимметричного шифрования и других криптографических протоколов. Каждый из этих классов кривых имеет свои особенности, и выбор между ними зависит от конкретных требований и контекста применения.

Список использованных источников

1. D. M. Dygin, S. V. Grebnev, Efficient implementation of the GOST R 34.10 digital signature scheme using modern approaches to elliptic curve scalar multiplication, Mat. Vopr. Kriptogr., 2013, Volume 4, Issue 2, 47–57.
2. Bernstein, D., Birkner, P., Joye, M., Lange, T. and Peters, C. Twisted Edwards curves. — http://eprint.iacr.org/2008/013, 2008.
3. Bernstein, D. and Lange, T. Inverted Edwards coordinates. —http://eprint.iacr.org/2007/410, 2007.
4. Doche, C., Kohel, D. R., Sica, F. Double-base number systems for multi-scalar multiplications // Proc. EUROCRYPT 2009. — Lect. Notes Comput. Sci. — 2009. — V. 5479. — P. 502–519.

УДК 004.85

СТАТИСТИКАДАҒЫ АЛГОРИТМ ҚОЛДАНЫСЫ

Қанат Айнұр
Ainur.kanat.91@mail.ru
Л.Н. Гумилев атындағы Еуразия ұлттық университетінің «Статистика» мамандығының 1-курс студенті
Ғылыми жетекшісі – А.С. Жумаханова, Л.Н. Гумилев атындағы ЕҰУ, «Математикалық және компьютерлік модельдеу» кафедрасының аға оқытушысы

Қазіргі заманда статистика ұғымының маңызы кеңінен артты. Уақыт өте келе, жаңа иновациялар мен техника дамуына байланысты ақпарат саласы эволюцияға ие болды: деректер артқан, бизнес мүмкіндіктері жоғарлуда, дерек дәлділігі жаңа сапаға келді.

Алгоритм - бұл белгілі адамдар тарапынан анықталған амалдарды орындау құрылымы немесе әдістер жиынтығы. Ол өзінде белгілі құрылымдың қалыптасуын немесе белгілі нәтижені құру үшін орындалатын әрекеттер жиынтығы.

Алгоритмді статистикада қолданудың мақсаты – Статистика құрастыруың адам үшін біріншіден оңайлату. Алгоритмдер статистикалық анализді ақпаратты құрастыру, түсіндіру және қаржылау үшін қолданылады. Олар өзіндікті статистикалық өлшемдер мен қаржыландыру мәселелерін шешуге көмектеседі.