ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

“Алгебраическая геометрия и ее применение в криптографии”

Мометова Даната Фарруховна, BMA 76 R

Содержание:

Введение.

Криптография - это наука о том, как защищать информацию, чтобы только те, кому она предназначена, могли ее прочитать. Она использует различные методы, такие как шифрование, чтобы сделать данные непонятными для посторонних. Ее изучают, чтобы обеспечить конфиденциальность, целостность и аутентификацию данных, например, в сфере банковского дела, интернет-безопасности, коммуникаций и т. д. Мне нравится данная наука и мне бы хотелось рассказать о ней в данной научной статье.

Криптография включает различные аспекты информационной безопасности, такие как :

- конфиденциальность данных – невозможность прочтения информации посторонним;
- целостность данных – невозможность незаметного изменения информации;
- аутентификация – проверка подлинности авторства или иных свойств объекта;
- шифрование – кодировка данных.

Алгебраическая геометрия - это раздел математики, который изучает геометрические объекты, такие как кривые и поверхности, используя алгебраические методы. Она исследует свойства этих объектов, связанные с их уравнениями и взаимосвязями между ними. Также, она имеет дело с кривыми или поверхностями, которые можно рассматривать и как геометрические объекты, и как решения алгебраических уравнений, объединяя, таким образом, алгебру и геометрию.

Рассмотрим два вышеперечисленных научных термина вкратце. В данной статье, я раскрою вам основные понятия данной темы.

В 1670-х годах Исаак Ньютон, используя приёмы аналитической геометрии, делает попытку классифицировать кубические кривые. В ходе исследований Ньютон заметил, что решение Диофанта состоит, по существу, в пересечении кривой, заданной уравнением $y(6 - y) = x\ 3 - x$, с касательной $x = 3y - 1$. Открытие Ньютона в конечном итоге привело к формулам сложения точек на эллиптической кривой. В XIX веке эллиптические кривые находят применение в теории эллиптических функций, которые, в свою очередь, тесно связаны с эллиптическими интегралами. Таким образом, исторически термин «эллиптическая кривая» происходит от термина «эллиптический интеграл».

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

Криптографическая система с открытым ключом – это система шифрования или электронной подписи, при которой открытый ключ передаётся по открытому (то есть незащищённому) каналу и используется для проверки подписи и для шифрования сообщения. Для генерации электронной подписи и для расшифровки сообщения используется закрытый ключ. Эллиптическая криптография (elliptic curve cryptography, ECC) – это раздел криптографии с открытым ключом, подходы которого основаны на алгебраической структуре эллиптических кривых над конечными полями. Эллиптическая криптография позволяет использовать ключи меньшего размера по сравнению с криптографией, использующей простые поля Галуа для обеспечения эквивалентной безопасности.

Концепцию криптографии на основе эллиптических кривых независимо друг от друга предложили математики Нил Коблиц и Виктор С. Миллер в 1985 году. Хотя их модель стала прорывом в криптографии, эллиптическая криптография стала широко использоваться только с 2000-го года, когда ее внедрили интернет-провайдер.

В этой научной статье мы рассмотрим несколько направлений и тем по данной теме с примерами и подробным описанием.

Эллиптические кривые в криптографии.

Алгоритмы эллиптических кривых будут работать в циклической подгруппе эллиптической кривой над конечным полем. Поэтому алгоритмам потребуются следующие параметры:

1. простое p, задающее размер конечного поля,
2. коэффициенты a и b уравнения эллиптической кривой,
3. базовая точка G, генерирующая подгруппу,
4. порядок n подгруппы,
5. кофактор h подгруппы.

В результате параметрами области определения для алгоритмов является шестёрка (p, a, b, G, n, h).

Терминология в ECC совершенно стандартная:

- Закрытый ключ – это случайное целое d, выбранное из $\{1, \ldots, n-1\}$ (где n – порядок подгруппы).
- Открытый ключ – это точка $H = dG$ (где G – базовая точка подгруппы).

Если мы знаем d и G (вместе с другими параметрами области определения), то найти H «просто». Но если мы знаем H и G, то поиск закрытого ключа d является «сложной» задачей, потому что требует решения задачи дискретного логарифмирования.

Теперь я опишу два основанных на этом принципе алгоритма с открытым ключом: ECDH (Elliptic curve Diffie Hellman, протокол Диффи-Хеллмана на эллиптических кривых), используемый для шифрования, и ECDSA (Elliptic Curve Digital Signature Algorithm), используемый для цифровых подписей.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

Шифрование с помощью ECDH.

В качестве условных обозначений взаимодействующих агентов или архетипичных символов в таких областях, как криптография, обычно используются имена Алиса и Боб. Используются для удобства объяснения работы сетевых протоколов: фраза «Алиса посылает Бобу сообщение, зашифрованное его открытым ключом» гораздо легче воспринимается, чем «сторона А посылает стороне Б сообщение, зашифрованное открытым ключом стороны Б». Со временем сформировались традиции, какими именами обозначать каких участников процесса.

Мне кажется, что «Алиса», «Боб» и т. п. обозначают не обязательно людей, а вообще агентов, независимо от их реализации: это могут быть, например, компьютерные программы, действующие от имени людей. С помощью этого примера, как мне кажется, легче всего понять суть темы.

Протокол Диффи-Хеллмана на эллиптических кривых – это криптографический протокол, позволяющий двум сторонам, имеющим пары открытый/закрытый ключ на эллиптических кривых, получить общий секретный ключ, используя незащищённый от прослушивания канал связи. Этот секретный ключ может быть использован как для шифрования дальнейшего обмена, так и для формирования нового ключа, который затем может использоваться для последующего обмена информацией с помощью алгоритмов симметричного шифрования.

Это вариация протокола Диффи-Хеллмана с использованием эллиптической криптографии. Протокол Диффи Хеллмана состоит в том, что Алиса и Боб могут «просто» вычислить общий секретный ключ, посреднику же придётся решать «сложную» задачу. На самом деле это скорее протокол согласования ключей, а не алгоритм шифрования. В сущности, это означает, что ECDH задаёт (в определённой степени) порядок генерирования ключей и обмена ими. Способ шифрования данных с помощью таких ключей мы можем выбирать сами.

Протокол решает следующую проблему: две стороны (обычно обозначаемые как «Алиса» и «Боб») хотят безопасно обмениваться информацией, чтобы третья сторона (посредник, Man In the Middle) мог перехватывать её, но не мог расшифровать. Например, это один из принципов протокола защиты транспортного уровня TLS (англ. Transport layer security), обеспечивающего защищённую передачу данных между узлами в сети Интернет.

Сначала Алиса и Боб генерируют собственные закрытые и открытые ключи. У Алисы есть закрытый ключ dA и открытый ключ $HA = dAG$, у Боба есть ключи dB и $HB = dBG$. И Алиса, и Боб используют одинаковые параметры области определения: одну базовую точку G на одной эллиптической кривой в одинаковом конечном поле. Алиса и Боб обмениваются открытыми ключами HA и HB по незащищённому каналу.

Посредник (Man In the Middle) перехватывает HA и HB, но не может определить ни dA, ни dB, не решив задачу дискретного логарифмирования. Алиса вычисляет $S = dAHB$ (с помощью собственного закрытого ключа и открытого ключа Боба), а Боб вычисляет $S = dBHA$ (с помощью собственного закрытого ключа и открытого ключа Алисы). Секретный ключ S одинаков и для Алисы, и для Боба:

$S = dAHB = dA(dBG) = dB(dAG) = dBHA.$

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

Однако посреднику известны только HA и HB (вместе с другими параметрами области определения), и он не сможет найти общий секретный ключ S. Эта ситуация известна как задача Диффи-Хеллмана, которую можно сформулировать следующим образом: Каким будет результат abP для трёх точек P, aP и bP?

Или, в аналогичной формулировке:

Каким будет результат $k\,xy$ для трёх целых k, $k\,x$ и ky (данная формулировка используется в исходном алгоритме Диффи-Хеллмана, основанном на модулярной арифметике)?

Получив общий секретный ключ, Алиса и Боб могут обмениваться данными с симметричным шифрованием.

Например, они могут использовать координату x ключа S как ключ для шифрования сообщений такими безопасными шифрами, как AES или 3DES. Примерно это и делает протокол TLS, разница в том, что TLS соединяет координату x с другими числами, относящимися к подключению, а затем вычисляет хэш получившейся строки байтов.

Задача Диффи-Хеллмана для эллиптических кривых считается «сложной». Считается, что она так же «сложна», как задача дискретного логарифмирования, но математических доказательств этому нет. Мы можем только с уверенностью сказать, что она не может быть «сложнее», потому что решение задачи логарифмирования – это способ решения задачи Диффи-Хеллмана.

Примеры с ECDH.

В отличие от показанных ранее примеров, в этом скрипте используется стандартизированная кривая, а не простая кривая на небольшом поле. Была выбрана кривая secp256k1 группы SECG («Standards for Efficient Cryptography Group», основанной Certicom). Та же самая кривая используется в Bitcoin для цифровых подписей. Вот параметры области определения (эти числа взяты из исходного кода OpenSSL):

p = 0xffffffff ffffffff ffffffff ffffffff ffffffff ffffffff fffffffe fffffc2f
a = 0
b = 7
x_G = 0x79be667e f9dcbbac 55a06295 ce870b07 029bfcdb 2dce28d9 59f2815b 16f81798
y_G = 0x483ada77 26a3c465 5da4fbfc 0e1108a8 fd17b448 a6855419 9c47d08f fb10d4b8
n = 0xffffffff ffffffff ffffffff fffffffe baaedce6 af48a03b bfd25e8c d0364141
h = 1

Возможно изменить скрипт и использовать другие кривые и параметры области определения, при условии использования простых полей и обычной формулировки Вейерштрасса, иначе скрипт не будет работать.

Скрипт очень прост и содержит некоторые из описанных выше алгоритмов: сложение точек, удвоение-сложение, ECDH. Рекомендуется изучить и запустить его. Он создаёт примерно такие выходные данные:

Curve: secp256k1
Alice's private key:
0xe32868331fa8ef0138de0de85478346aec5e3912b6029ae71691c384237a3eeb
Alice's public key:

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

(0x86b1aa5120f079594348c67647679e7ac4c365b2c01330db782b0ba611c1d677,
0x5f4376a23eed633657a90f385ba21068ed7e29859a7fab09e953cc5b3e89beba)
Bob's private key:
0xcef147652aa90162e1fff9cf07f2605ea05529ca215a04350a98ecc24aa34342
Bob's public key:
(0x4034127647bb7fdab7f1526c7d10be8b28174e2bba35b06ffd8a26fc2c20134a,
0x9e773199edc1ea792b150270ea3317689286c9fe239dd5b9c5cfd9e81b4b632)
Shablack secret:
(0x3e2ffbc3aa8a2836c1689e55cd169ba638b58a3a18803fcf7de153525b28c3cd,
0x43ca148c92af58ebdb525542488a4fe6397809200fe8c61b41a105449507083)

Шифрование с помощью ECDSA.

Алиса подписывает хэш z с помощью закрытого ключа dA и случайного k. Боб проверяет правильность подписи сообщения с помощью открытого ключа Алисы HA. Проще говоря, этот алгоритм сначала генерирует секретный ключ k. Благодаря умножению точек (которое, как мы знаем, является «простым» в одну сторону и «сложным» в обратную) секретный ключ прячется в r. Затем r привязывается к хэшу сообщения уравнением $s = k −1 (z + rdA) \bmod n$.

Нужно учесть, что для вычисления s мы вычислили обратную величину k по модулю n. Как было сказано в предыдущей части, это гарантировано сработает только если n – простое число. Если подгруппа имеет порядок непростого числа, ECDSA использовать не удастся. Неслучайно все стандартизированные кривые имеют простой порядок, а имеющие непростой порядок неприменимы для ECDSA.

Примеры с ECDSA.

Andrea Corbellini написал скрипт на Python для генерирования и проверки подписей. Код копирует некоторые части из скрипта ECDH, в частности, параметры области определения и алгоритм генерирования пары закрытого и открытого ключей. Этим скриптом создаются нижеследующие выходные данные:

Curve: secp256k1
Private key:
0x9f4c9eb899bd86e0e83ecca659602a15b2edb648e2ae4ee4a256b17bb29a1a1e
Public key:
(0xabd9791437093d377ca25ea974ddc099eafa3d97c7250d2ea32af6a1556f92a,
0x3fe60f6150b6d87ae8d64b78199b13f26977407c801f233288c97ddc4acca326)
Message: b'Hello!'
Signature:
(0xddcb8b5abfe46902f2ac54ab9cd5cf205e359c03fdf66ead1130826f79d45478,
0x551a5b2cd8465db43254df998ba577cb28e1ee73c5530430395e4fba96610151)
Verification: signature matches
Message: b'Hi there!'

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

Verification: invalid signature Message: b'Hello!'
Public key:
(0xc40572bb38dec72b82b3efb1efc8552588b8774149a32e546fb703021cf3b78a,
0x8c6e5c5a9c1ea4cad778072fe955ed1c6a2a92f516f02cab57e0ba7d0765f8bb)
Verification: invalid signature

Алгебраические и секретные коды.

Алгебраические коды представляют собой математическую конструкцию, используемую в теории кодирования для обеспечения коррекции ошибок в передаче данных. Основными принципами алгебраических кодов являются использование алгебраических структур, таких как группы и поля, для создания кодовых слов, которые могут быть декодированы с минимальными ошибками.

Пример:

Я рассмотрела **код Хэмминга (7, 4)**.

- возьмем 4 бита данных: 1101.
- код Хэмминга добавляет 3 контрольных бита, дополняя данные: 1101 000.
- контрольные биты вычисляются так, чтобы обеспечить четное количество единиц в каждой "позиции" (бит с номерами 1, 2, 4): 1 110 100.
- теперь мы имеем кодовое слово 1110100.

Обнаружение ошибок:

- если при передаче данных произошла ошибка (например, 1010100), контрольные биты помогут обнаружить ошибку.
- путем анализа контрольных битов мы можем определить позицию ошибки и даже исправить ее.

Применение:

- такие коды применяются в беспроводных связях, где помехи могут исказить передаваемую информацию.

Секретные коды - это методы шифрования, направленные на сокрытие информации от несанкционированного доступа. Они используют алгоритмы шифрования и ключи для преобразования понятного текста в зашифрованный вид.

Тут я рассмотрела пример с AES (Advanced Encryption Standard):

- пусть у нас есть текстовое сообщение: "HELLO".
- мы выбираем ключ (например, KEY123).
- алгоритм AES использует ключ для преобразования сообщения в непонятный вид (шифр), например, 1a3b5f8c....

Дешифрование:

- тот же ключ используется для дешифрования, возвращая исходное сообщение.

Применение:

- секретные коды применяются в онлайн-банкинге, защите конфиденциальных данных на серверах, в военных коммуникациях и многих других областях.

Общий наглядный пример:

Предположим, у нас есть беспроводная система передачи данных, например, медицинская информация от датчиков до сервера.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

Использование алгебраических кодов:

- для обеспечения целостности данных мы применяем код Хэмминга, чтобы обнаруживать и исправлять ошибки, возможные из-за помех в беспроводной передаче.

Использование секретных кодов:

- чтобы обеспечить конфиденциальность медицинских данных, мы шифруем их с использованием AES и передаем по защищенному каналу.

Взаимодействие:

- обе технологии работают вместе, гарантируя, что данные будут переданы целостными и конфиденциальными.

Таким образом, в данном примере алгебраические коды и секретные коды взаимодействуют для обеспечения надежности, целостности и конфиденциальности передаваемых данных.

Гиперэллиптические кривые и их криптографические применения.

Гиперэллиптические кривые - это обобщение эллиптических кривых, используемых в математике и криптографии Форма гиперэллиптической кривой в проективных координатах: y^2=x^2g+1+ax^g+1+b, где g - параметр.

Криптографические характеристики гиперэллиптических кривых:

- криптографические свойства: гиперэллиптические кривые используются в криптографии из-за их сложности и математических свойств, сопоставимых с эллиптическими кривыми.
- криптографические параметры: Выбор параметров, таких как степень g и коэффициенты a и b, критически влияет на безопасность системы.

Криптографические применения гиперэллиптических кривых:

- гиперэллиптические кривые в криптографии с открытым ключом:

Пример - Электронная подпись:

Подпись сообщения m создается путем вычисления S=kP, где k - закрытый ключ, P - базовая точка кривой.

Проверка подписи включает в себя использование открытого ключа для проверки, что S соответствует открытому тексту m.

- гиперэллиптические кривые в протоколах ключевого обмена: Пример - Протокол Диффи-Хеллмана на гиперэллиптических кривых:

Алиса и Боб выбирают случайные числа и генерируют соответствующие точки на кривой.

Они обмениваются открытыми ключами, а затем используют их для генерации общего секретного ключа.

Защита от криптоанализа:

Дискретный логарифм на гиперэллиптических кривых: Атака, направленная на вычисление закрытого ключа по известным открытым ключам, труднее в сравнении с классическими методами.

Преимущества и ограничения:

- преимущества:

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

гиперэллиптические кривые предлагают аналогичный уровень безопасности с меньшей длиной ключа по сравнению с эллиптическими кривыми. Они поддерживают эффективные алгоритмы для криптографии.

- ограничения:

использование гиперэллиптических кривых требует дополнительных вычислительных ресурсов по сравнению с более распространенными эллиптическими кривыми.

Примеры стандартов:

Supersingular Isogeny Key Exchange (SIKE): Пример стандарта, использующего изогении на гиперэллиптических кривых для квантовоустойчивого ключевого обмена.

Заключение:

Гиперэллиптические кривые представляют собой интересный математический инструмент, который успешно применяется в сфере криптографии. Их применение охватывает широкий спектр криптографических протоколов, предоставляя безопасные и эффективные средства для обеспечения конфиденциальности и целостности данных.

Решетки и Коды на Решетках в Криптографии.

Решетка - это абстрактная математическая структура, представляющая собой совокупность векторов с целыми координатами, образующих сетку в n-мерном пространстве. Решетки в криптографии используются для создания криптографически стойких схем, таких как схемы обмена ключами и шифрование.

Шифрование на основе решеток:

Пример - Габора система шифрования на решетках:

Используется решетка для создания открытого ключа, а шифрование осуществляется с использованием этого ключа.

Решетчатые коды в современной криптографии:

Пример - Криптография на решетчатых кодах:

Решетчатые коды могут использоваться для построения криптосистем, устойчивых к атакам с использованием квантовых компьютеров.

Сложность решеточных проблем:

- Решеточные проблемы, такие как SIS (Small Integer Solution) или LWE (Learning With Errors), являются основой для криптографических схем на решетках.

Преимущества и Ограничения:

Преимущества:

- решеточные криптосистемы считаются квантовоустойчивыми, так как решеточные проблемы сложны для решения с использованием квантовых компьютеров.
- использование решеток в криптографии может обеспечить дополнительные слои безопасности.

Ограничения:

- вычислительные требования могут быть высокими, особенно при работе с большими размерностями решеток.
- существует риск появления новых алгоритмов, способных решать решеточные проблемы, что может угрожать криптостойкости.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

Заключение:

Исследуя данное направление моей основной темы научной статьи, я думаю, что решетки и коды на решетках представляют собой важные математические инструменты в современной криптографии. Их применение охватывает широкий спектр задач, включая защиту от квантовых атак, построение схем обмена ключами и шифрования, а также создание криптографически стойких кодов с исправлением ошибок.

Интерактивные доказательства и алгебраическая геометрия.

Интерактивные доказательства представляют собой форму доказательств, в которых доказывающая сторона взаимодействует с проверяющей стороной, обеспечивая ей информацию, которая позволяет убедиться в верности утверждения. Это взаимодействие может включать запросы и ответы, а результатом является убеждение проверяющей стороны в корректности утверждения, несмотря на то, что она не имеет полного доступа ко всей информации. Исследуя данный термин в криптографии, я могу утверждать, что интерактивные доказательства в криптографии используются для доказательства знаний, алгебраическая геометрия - для построения криптосистем, например, с использованием эллиптических кривых. Снизу я привела пример.

Пример:

Рассмотрим ситуацию, где Алиса хочет убедить Боба, что у нее есть определенная информация, но она не хочет раскрывать эту информацию напрямую. Алиса может предоставить доказательство, на которое Боб может задавать вопросы, и Алиса предоставляет ответы. В конечном итоге, Боб должен быть убежден в том, что Алиса обладает необходимой информацией.

Алгебраическая геометрия - это раздел математики, который изучает геометрические объекты, определенные алгебраическими уравнениями и их свойства. Обычно, это включает в себя изучение алгебраических множеств, которые являются множествами решений полиномиальных уравнений с коэффициентами из некоторого алгебраического поля. Снизу я привела примеы.

Примеры:

Эллиптические кривые: Одним из ключевых объектов в алгебраической геометрии являются эллиптические кривые, определенные уравнением вида y2=x3+ax+b, где a и b - коэффициенты. Эллиптические кривые имеют много приложений в криптографии, особенно в схемах эллиптической криптографии (ЭЦП).

Проективные пространства: Алгебраическая геометрия включает в себя рассмотрение проективных пространств, которые обобщают аффинные пространства, добавляя бесконечно удаленные точки. Это имеет приложения в построении криптографических протоколов, таких как схемы обмена ключами на решетках.

Решетки и Алгебраическая Геометрия: В криптографии на решетках используются методы алгебраической геометрии для построения сложных криптосистем, которые устойчивы к атакам, таким как атаки с использованием квантовых компьютеров.

Значение в криптографии:

Алгебраическая геометрия играет важную роль в разработке криптографических протоколов, так как многие из ее концепций, таких как группы точек на кривых, могут быть

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

использованы для построения безопасных криптосистем. Также, алгебраическая геометрия может быть привлечена для решения математических проблем, связанных с криптографией.

Преимущества и Ограничения:

Преимущества:

- Интерактивные доказательства предоставляют эффективный способ доказательства без раскрытия полной информации.
- Алгебраическая геометрия предоставляет математический фреймворк для построения безопасных криптографических схем.

Ограничения:

- Некоторые интерактивные доказательства могут быть ресурсоемкими.
- Необходимость работы с высокоуровневыми математическими задачами.

Теория игр и криптография.

Теория игр - это область математики, которая изучает взаимодействие между различными участниками, называемыми игроками, в условиях конфликта или сотрудничества. Она исследует стратегии, которые могут принимать игроки, и как они влияют на итоговый результат или выигрыш.

Структура игры:

Теория игр обычно определяет игру через следующие элементы:

Игроки: Люди, организации или агенты, принимающие решения.

Стратегии: Возможные действия, доступные игрокам.

Выигрыши и убытки: Оценки, которые игроки получают в зависимости от выбранных стратегий других участников.

Информация: Уровень знаний, который игроки имеют о других участниках.

Пример:

Представьте двух игроков, Алису и Боба, играющих в шахматы. Они принимают решения (ходы) в зависимости от хода друг друга, стремясь выиграть партию. Теория игр помогает предсказать их решения и стратегии.

Криптография - это наука об обеспечении конфиденциальности, целостности и подлинности информации при передаче или хранении. Она включает в себя разработку методов шифрования (защиты информации от несанкционированного доступа) и создание средств для аутентификации (подтверждения подлинности данных).

Элементы криптографии:

Шифрование: Преобразование данных таким образом, чтобы они стали непонятными для тех, кто не имеет ключа для расшифровки.

Хэширование: Преобразование данных в фиксированный размер для обеспечения целостности и проверки подлинности.

Электронные подписи: Методы аутентификации и проверки авторства данных.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-4, ISSUE-7

Протоколы безопасности: Специальные правила и процедуры для обеспечения безопасного обмена информацией.

Пример:

Если Алиса хочет отправить конфиденциальное сообщение Бобу через открытую сеть, она может использовать криптографию. Она зашифровывает сообщение ключом, который знает только Боб, и только он сможет его расшифровать.

Взаимосвязь:

Теория игр может быть использована для моделирования ситуаций конфликта в области криптографии. Например, когда злоумышленник (игрок) пытается взломать систему, а разработчик криптографии создает методы (стратегии), чтобы предотвратить его атаки.

Пример:

Рассмотрим сценарий, где злоумышленник пытается подобрать пароль для взлома учетной записи. Здесь теория игр может помочь разработать стратегии для защиты, например, блокировку учетной записи после нескольких неудачных попыток.

Заключение:

Теория игр и криптография, хотя и принадлежат разным областям математики, могут взаимодействовать для создания более надежных и безопасных систем. Изучение стратегий и ситуаций конфликта помогает разрабатывать эффективные методы защиты в информационной безопасности.

Вывод:

В заключение своей научной статьи об алгебраической геометрии в криптографии, хочу подчеркнуть значимость этого пересечения математики и информационной безопасности. Алгебраическая геометрия предоставляет мощный математический инструментарий для решения сложных криптографических задач, открывая новые перспективы в области разработки безопасных протоколов и систем шифрования.

В этой работе я рассмотрела несколько ключевых концепций алгебраической геометрии и их применение в сфере криптографии. Эллиптические кривые, алгебраические и секретные коды и гиперэллиптические кривые представляют собой лишь часть богатого арсенала методов, которые можно использовать для обеспечения безопасности информации.

Применение алгебраической геометрии в криптографии не только улучшает стойкость шифров и схем обмена ключами, но и позволяет эффективно справляться с вызовами, стоящими перед современной криптографией, такими как квантовые атаки.

Эксплорация решечетых кодов и гиперэллиптических кривых в контексте криптографии после квантового компьютера открывает двери для новых методов обеспечения безопасности, устойчивых к атакам, которые ранее казались труднопреодолимыми.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889,
2024-6.875 ResearchBib IF: 8.848 / 2024

Однако, несмотря на значительные достижения в данной области, следует отметить, что вычислительные трудности и поиск более эффективных методов остаются актуальными направлениями исследований. Большое внимание должно быть уделено как теоретическим аспектам, так и реализации этих методов с целью обеспечения их практической применимости.

В заключении хочу выразить уверенность в том, что дальнейшие исследования в области алгебраической геометрии в криптографии приведут к созданию еще более надежных и устойчивых криптографических схем, открывая новые возможности для защиты информации в эру быстрого развития цифровых технологий.

Список источников информации:

https://www.researchgate.net/publication/369032712_Metody_algebraiceskoj_geometrii_v_kriptografii_ucebnoe_posobie
- учебное пособие МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

- учебное пособие национального исследовательского университета «Высшая школа экономики»
- сайт Википедия