Литература

1. Yumeng YanResearch on the A Star Algorithm for Finding Shortest PathURL:https://www.researchgate.net/publication/370573811_Research_on_the_A_Star_Algorithm_for_Finding_Shortest_Path

2. Шагабазян. Д.В. Алгоритмы сортировки. Анализ, реализация, применение / Шагабазян. Д.В. , Штанюк А.А., Малкина Е.В. – Нижний Новгород: Нижегородский госуниверситет, 2019. – 42с.

УДК 681.3.06:519.248.681

ECDSA- И MQV-АЛГОРИТМЫ: ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

Кондратьев Д.П.
Научный руководитель – Бадак Б.А., старший преподаватель кафедры «Высшая математика»

Теория эллиптических кривых является неотъемлемым разделом алгебраической геометрии. Более того, она неразрывно связана с теорией чисел и комплексным анализом. Первооткрывателем свойств таких кривых считается древнегреческий ученый Диофант. Структуру группы на эллиптических кривых впервые ввёл французский математик Анри Пуанкаре. На протяжении долгого времени теория эллиптических кривых не имела применения, но в конце прошлого века она получила приложения в области построения алгоритмов факторизации больших чисел, а позднее и в криптографии. В 1985 году независимо друг от друга Нил Коблиц и Виктор Миллерпредложили использовать в криптографии алгебраические свойства эллиптических кривых. Это направление получило название **криптография на эллиптических кривых**(англ. EllipticCurveCryptography - ECC), или же эллиптическая криптография[1]. На сегодняшний день эллиптические кривые используются для нахождения факториалов чисел, для поиска и проверки простых чисел, в криптосистемах, в протоколах распределения ключей, в протоколах цифровой подписи и т.д.

Главное преимущество криптосистем, основанных на эллиптических кривых в сравнении с другими заключается в том, что сохраняется аналогичный уровень безопасности при более коротких ключах, однако существенным недостатком является высокая сложность вычислений, именно поэтомуисследования в этой сфере не прекращаются и довольно часто появляются новые алгоритмы.

Криптография существует уже более двух тысяч лет, однако свою популярность эта наука получила только в середине семидесятых годов

прошлого века, когда были созданы первые алгоритмы публичной криптографии (криптографии с открытым ключом) DH(Diffie-Hellman) и RSA (Rivest, Shamir, Adleman). Сейчас хотелось бы рассмотреть прикладное применение эллиптических кривых в криптографии, а именно **ECSDA- и MQV- алгоритмы**, находящие применение в защите электронной информации.

Электронная цифровая подпись (ЭЦП*)* – это реквизит электронного документа, который позволяет подтвердить авторство электронного документа и его целостность.

ECDSA(EllipticCurveDigitalSignatureAlgorithm) – криптографический алгоритм для создания электронной цифровой подписи.

Как пример, здесь можно вспомнить создание биткоина Сатоши Накамото.

Видение Накамото состояло в том, чтобы организоватьприватный обмен открытыми ключами с низкими вычислительными затратами и простотойв использовании. Эти задачи были бы возможными благодаря применению криптографии на основе эллиптических кривых. Именно поэтому Накамото решил использовать ECDSA– алгоритм для своей системы блокчейна.

Помимо этого, данный алгоритм отличается высоким уровнем безопасности и быстрой верификацией, что объясняет его широчайшее применение в области шифрования информации.

Также стоит упомянуть и про альтернативный алгоритм**ECPVS (Elliptic Curve Pintsov Vanstone Signature**). Этот алгоритм уникален тем, что он поддерживает восстановление лишь части сообщения из подписи. Алгоритм входит в многочисленные стандарты, такие как I EEE P1363a, ANSI X9.92 и ISO 9796-3. Применяется в почтовых сервисах, а также для верификации чеков и подписи коротких сообщений, занимающих 1 байт (к примеру, сообщение с ответом да/нет и т.д.).

Далее приведено краткое описание работы алгоритмаECDSA.

Необходимые рабочие параметры:

1) Хеш-функция H(x);
2) q(простое число) – порядок одной из циклических подгрупп группы точек эллиптической кривой;
3) P–характеристика поля;

Генерация ключей:

1) E – эллиптическая кривая над полем F_p, $P \in E(F_p)$ – точка порядка q;
2) Выбирается случайное число $x \in (0, q)$;
3) Вычисляется $Q = xP$.

x – закрытый ключ, Q – открытый ключ при фиксированных E и P. Если E и P генерируются для каждого пользователя, то тройка (E, P, Q) является открытым ключом.

Алгоритм подписи:

1) Выбор случайного числа $k \in (0, q)$.
2) Вычисление $kP = (x_1, y_1); r = x_1 \ mod \ q$.
3) Если $r = 0$, то выбирается другое k.
4) Вычисление $s = k^{-1}(H(m) + x * r) \ mod \ q$.
5) Если $s = 0$ то выбирается другое k.
6) Подписью является пара (r, s) длинной 2N.

Алгоритм проверки:

1) Вычисление $u_1 = H(m) * s^{-1} \ mod \ q$.
2) Вычисление $u_2 = r * s^{-1} \ mod \ q$.
3) Вычисление $(x_1, y_1) = u_1 P + u_2 Q; r = x_1 \ mod \ q$.
4) Если выполнено равенство $v = r$, то подпись верна.

ECDSA-стандарт считается безопасным для функционирования систем цифровой подписи (DSA). Их примененииена сегодняшний день настолько разнообразно, что они используются почти во всех компьютерных областях, в том числе и в криптовалюте блокчейна.

MQV (Menzes-Qu-Vanstone) – алгоритм аутентификации для согласования ключей, т.е. проверки подлинности пользователей при согласовании. Базируется на основе **алгоритма Диффи-Хеллмана** и предоставляет защиту против активных атак путем сочетания статического и временного ключей. В нашем случае, этот алгоритм используется в группах эллиптических кривых, где известен как **ECMQV (EllipticCurveMenzes-Qu-Vanstone)**–алгоритм. Его смысл состоит в том, что два пользователя Аи Вмогут получить общий секретный ключ для использования его в дальнейшем в симметричной криптографической системе, что находит применение в различных областях шифрования и дешифрования сообщений, передаче этих сообщений (как раз-таки при помощи ECDSA- алгоритма) и др.

Необходимые рабочие параметры:

1) Пара ключей (A, a) и (B, b) пользователей *A* и *B*соответственно. A, B-открытые ключи; a, b – закрытие ключи.
2) Пусть $R = (x, y)$– точка на эллиптической кривой, тогда $\bar{R} = (x \ mod \ 2^L) + 2^L; L = \left\lceil \frac{\lfloor \log_2 n \rfloor + 1}{2} \right\rceil; n$ –порядок группы.
3) h – кофактор группы, $h = \frac{|G|}{n}$.

Алгоритм:

1) *A* генерирует пару (X, x) где x – случайное число; $X = xP$.
2) Аналогично *B* генерирует пару (Y, y).
3) *A* вычисляет $S_a = x + \bar{X} a \ mod \ n$ и отправляет точку *X* пользователю ***B*.**
4) Аналогично *B*вычисляет $S_b = y + \bar{Y} b \ mod \ n$ и отправляет точку *Y* пользователю ***A*.**
5) *A* вычисляет $K = h * S_a(Y + \bar{Y} B)$ и *B* вычисляет $K = h * S_b(X + \bar{X} A)$.

6) K – общий секретный ключ.

Таким образом, работа ECDSA- и MQV- алгоритмов основана на свойствах и прикладном применении эллиптических кривых в криптографии, помимо этого, эта тема оставляет обширные возможности для дальнейших исследований и поиска более совершенных алгоритмов шифрования и защиты данных, что является их неоспоримым плюсом в сравнении с иными методами и подходами к задачам подобного рода.

Литература

1. Элементарное введение в эллиптическую криптографию, Алгебраические и алгоритмические основы, Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А., 2006.

УДК 004.89

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЭНЕРГЕТИКЕ И МАТЕМАТИКЕ

Куцепалова Д. А, Адаменко А. О.
Научный руководитель – Бань Л.В., старший преподаватель

Искусственный интеллект (ИИ) представляет собой систему, которая позволяет пользователю через формулирование целей получать нужные результаты, а также помогает оптимизировать процесс работы, анализ данных, улучшает качество решений. При этом человек не разрабатывает отдельные алгоритмы - система должна сама уметь обнаруживать решения в установленных пределах под определённую цель. Его применение в энергетике и математике открывает новые способности для развития этих областей, предлагая решения для сложных задач, повышение эффективности процессов.

В наше время энергетика сталкивается с рядом проблем, таких как: выбросы углекислого газа, повышение эффективности производства, а также обеспечение надежности и безопасности энергосистем. ИИ предлагает решение для этих проблем:

1) Использование алгоритмов машинного обучения - позволяет точно прогнозировать спрос и предложение энергии, что важно для оптимизации работы энергосистем.

2) Управление распределением энергии - ИИ способствует созданию более гибких и эффективных систем распределения энергии, включая умные сети. Smart grids (умные сети) – это сочетание обеспечения электроэнергией с информационными технологиями. Их функции: отслеживать изменения в сети, а также облегчить управление системой. Это