УДК 004.94

ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОСИСТЕМАХ С ОТКРЫТЫМ КЛЮЧОМ

***Кондратьев Дмитрий Павлович**, студент 1-го курса*
кафедры «Программное обеспечение информационных систем и технологий»
Белорусский национальный технический университет, г. Минск
(Научный руководитель – Бадак Б.А., заместитель декана ФИТР,
старший преподаватель)

Теория эллиптических кривых является неотъемлемым разделом алгебраической геометрии. Она неразрывно связана с теорией чисел и комплексным математическим анализом. Первооткрывателем свойств эллиптических кривых считается древнегреческий ученый Диофант. Долгое время теория эллиптических кривых не имела приложений, но в 80-х годах прошлого века независимо друг от друга ученые Нил Коблиц и Виктор Миллер предложили использовать в криптографии алгебраические свойства эллиптических кривых. Это направление получило название эллиптическая криптография (англ. Elliptic Curve Cryptography - ECC). На сегодняшний день эллиптические кривые используются для нахождения факториалов чисел, для поиска и проверки чисел на простоту, в криптосистемах, в протоколах распределения ключей, в протоколах цифровой подписи и т.д.

Главное преимущество криптосистем, основанных на эллиптических кривых в сравнении с другими – аналогичный уровень безопасности при более коротких ключах, однако их существенным недостатком является высокая сложность вычислений, именно поэтому исследования в этой сфере не прекращаются и довольно часто появляются новые алгоритмы шифрования.

Криптография существует уже более двух тысяч лет, однако свою популярность эта наука получила только в середине 1970-х годов, когда были созданы первые алгоритмы криптографии с открытым ключом: DH (Diffie-Hellman) и RSA (Rivest, Shamir, Adleman). Сейчас рассмотрим конкретные приложения эллиптических кривых в криптографии, а именно ECSDA- и ECMQV- алгоритмы, находящие применение в защите электронной информации.

ECDSA (Elliptic Curve Digital Signature Algorithm) – криптографический алгоритм для создания электронной цифровой подписи (ЭЦП).

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, который позволяет подтвердить авторство электронного документа и его целостность [1].

Как пример, здесь можно вспомнить создание биткоина Сатоши Накамото.

Идея Накамото состояла в том, чтобы обеспечить приватный обмен открытыми ключами с низкими вычислительными затратами и простотой в использовании. Эти задачи стали возможными в реализации благодаря применению криптографии на основе эллиптических кривых. Помимо этого, данный алгоритм отличается высоким уровнем безопасности и быстрой верификацией, что объясняет его широчайшее применение в области шифрования электронной информации.

Также стоит упомянуть про алгоритм ECPVS (Elliptic Curve Pintsov Vanstone Signature). Он уникален тем, что поддерживает восстановление лишь части сообщения из подписи. Алгоритм входит в многочисленные стандарты электронной безопасности, такие как I EEE P1363a, ANSI X9.92 и ISO 9796-3. Применяется в почтовых сервисах, для верификации чеков и подписи сообщений, занимающих 1 байт (к примеру, сообщений с ответом “да” или “нет” и др.).

Далее приведено краткое описание работы ECDSA-алгоритма.

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) – открытый ключ.

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 число k.
4) Вычисление $s = k^{-1}(H(m) + x * r) \ mod \ q$.
5) Если $s = 0$, то выбирается другое число 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 $v = r$, то подпись верна.

ECDSA-стандарт является безопасным для работы систем цифровой подписи (DSA). Их применение на сегодняшний день настолько разнообразно, что они используются во всех компьютерных областях, в том числе и в криптовалюте блокчейна.

ECMQV (Elliptic Curve Menzes-Qu-Vanstone) – алгоритм авторизации для проверки подлинности пользователей при согласовании. Он базируется на основе алгоритма Диффи-Хеллмана (Diffie-Hellman) и предоставляет защиту против активных атак путем сочетания статического и временного ключей. Его смысл заключается в том, что два пользователя A и B могут получить общий секретный ключ для использования его в дальнейшем в симметричной криптосистеме, что находит применение в разных областях шифрования и дешифрования сообщений.

Далее приведено краткое описание работы ECMQV-алгоритма.

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) B генерирует пару (Y, y), где y – случайное число; $Y = yP$.

3) A вычисляет $S_a = x + \bar{X} a\ mod\ n$ и отправляет точку X пользователю B.

4) 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 основывается на свойствах и прикладном применении эллиптических кривых в криптографии, кроме того, данная тема оставляет обширные возможности для дальнейших исследований и поиска более совершенных алгоритмов шифрования и защиты данных в связи с постоянным ростом вычислительных мощностей компьютерных средств, что является их очевидным плюсом по сравнению с другими методами и подходами к решению задач подобного рода.

Литература:

1. Жданов О.Н., Чалкин В.А. Эллиптические кривые: Основы теории и криптографические приложения. – М. : Книжный дом ЛИБРИКОМ, 2013. – 200 с.