Эссе по курсу "Защита информации"
физтех-школа радиотехники и компьютерных технологий
Моковский физико-технический институт (национальный исследовательский университет)
по теме

«Эллиптическая криптография»

студента группы Б01-814
Горбачева Никиты Сергеевича
17 декабря, 2021

1 Предисловие

В данной статье будет рассмотрена тема эллиптической криптографии. Сначала будет разобрана база для описания существующих алгоритмов. После этого будут описаны существующие алгоритмы, базирующиеся на математике эллиптических кривых. Так же в рамках статьи будут подниматься темы преимуществ, недостатков и тонкостей при использовании эллиптической криптографии.

Статья является обзорной, так что некоторые факты будут оставлены без строгого математического доказательства, а некоторые технологии будут упомянуты без конкретной реализации с упоминанием названия для дальнейшего изучения при необходимости.

2 Эллиптические кривые

2.1 Вид кривой

Под эллиптической кривой над полем K в общем случае понимается гладкая проективная кубическая кривая, задаваемая уравнением 3 степени с «точкой на бесконечности» O вида:

$$y^2 + a_1xy + a_3y = x^3 + a_2x + a_4x + a_6.$$

В зависимости от значения коэффициентов и самого поля K кривая может принадлежать к различным классам. В данном обзоре будет рассматриваться кривая в форме Вейерштрассе над полем вещественных чисел, а затем и над полем целых чисел по модулю p.

Эллиптическая кривая E над полем вещественных чисел - это плоская кривая, определяемая уравнением Вейерштрассе, на которой так же определена точка O:

$$y^2 = x^3 + Ax + B, \text{ где A и B - вещественные числа.}$$

Корнями такого уравнения являются числа x_1, x_2, x_3. Дискриминант $D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = -16(4A^3 + 27B^2)$. Если дискриминант равен нулю, то кривая называется сингулярной. Иначе кривая называется гладкой. Гладкая имеет две связные компоненты, при условии что дискриминант положителен, и одну, если отрицателен. Подразумевается, что кривая находится в проективной плоскости, причем точка O является единственной точкой на бесконечности.

2.2 Групповой закон для эллиптических кривых

На эллиптической кривой можно алгебраически определить групповой закон, по отношению к которому она является абелевой группой. В этом случае элементы группы - это элементы эллиптической кривой. O является нейтральным элементом.

Обратной величиной точки P будет являться точка, симметричная ей относительно оси x. Сложение определено правилом, что сумма трех ненулевых точек P, Q, R', лежащих на одной прямой, будет равна O. Такой оператор обладает свойствами ассоциативности и коммутативности. Тогда суммой точек P и Q на эллиптической кривой является такая точка $R = P + Q$, симметричная точке R' относительно горизонтальной оси координат.

2.3 Алгебраическое представление сложения

Пусть точка P имеет координаты (x_P, y_P), а точка Q соответственно (x_Q, y_Q). Тогда координаты (x_R, y_R) точки $R = P + Q (P \neq Q)$ можно вычислить следующим способом:

$$\begin{gathered} S = \tfrac{y_Q - y_P}{x_Q - x_P}. \\ x_R = S^2 - x_P - x_Q. \\ y_R = -y_P + S(x_P - x_R). \end{gathered}$$

В случае же $P = Q$, то есть при удвоении значения x_R и y_R находятся по тем же формулам, а значение S:

$$S = \tfrac{3x_P^2 + A}{2y_P}.$$

2.4 Скалярное умножение

Так же помимо сложения, на эллиптических кривых определена операция скалярного умножения на натуральное число

$$L = mP = \underbrace{P + P + ... + P}_{m}.$$

Для вычисления mP по определению требуется m сложений. То есть сложность вычисления $O(m)$. И если m в двоичном виде представимо в виде числа с k знаками, то сложность вычисления составит $O(2^k)$. Сложность можно уменьшить, например воспользовавшись алгоритмом удвоения-сложения (англ. double-and-add). Разберем его на примере $m = 33 = 100001_2$. Тогда выполняется равенство:

$$L = 33P = 2^5P + P.$$

То есть, нам потребуется 5 операций удвоения и одно сложение вместо 32 сложений. Сложность данного алгоритма $O(k)$ или $O(log\ m)$.

3 Эллиптические кривые над полем целых чисел по модулю p

Если ограничить эллиптические кривые полем F_p, то непрерывная кривая станет множеством точек на плоскости xy. Причем кривая, определенная над конечным полем, имеет конечное число точек. При этом эллиптические кривые над F_p по-прежнему образуют абелеву группу. Единственное, что теперь все раннее упомянутые операции будет необходимо совершать по $mod\ p$.

Для введения еще нескольких понятий заметим, что при сложении двух точек, кратных некоторой точке G, мы получаем точку, так же кратную G:

$$aG + bG = (a + b)G$$

Тогда точки, кратные G, замкнуты относительно операции сложения. Из этого следует, что множество кратных G точек является циклической подгруппой группы, образованной эллиптической кривой. Точка G называется генератором эллиптической кривой.

Порядок подгруппы, порожденной генератором G – это такое минимальное положительное n, что выполняется $nG = 0$. Причем по теореме Лагранжа порядок n данной подгруппы является делителем порядка N группы точек, образованной эллиптической кривой $hn = N$, где целое число h называется кофактором подгруппы.

Из этого следует, что для любой точки кривой P выполняется $NP = 0$. Тогда выполняется и соотношение $NP = (hn)P = n(hP) = 0$, а значит для простого n точка $G = hP$ является генератором подгруппы порядка n, за исключением случая, когда $G = 0$, когда порядок равен 1.

Задача же нахождения значения m по заданным P и L в случае $L = mP$ называется задачей дискретного логарифмирования для эллиптических кривых (англ. Elliptic Curve Discrete Logarithm Problem, ECDLP). Пока не был найден алгоритм ее решения в общем виде за полиномиальное время, но и математического доказательства его не существования тоже нет. Причем на текущий момент решение данной задачи для определенных классов эллиптических кривых вычисляется гораздо труднее, чем решение задачи обращения g^x в некоторой конечной мультипликлативной группе, применяемом во многих криптографических системах с открытым ключом.

Таким образом, для эллиптической кривой мы можем определить следующие необходимые нам в дальнейшем параметры:

a, b – коэффициенты, задающие эллиптическую кривую.
p – простое число, определяющие размер конечного поля.
G – точку кривой, являющуюся генератором подгруппы.
n – порядок подгруппы.
h – кофактор подгруппы.

4 Эллиптическая криптография(Elliptic-curve cryptography, ECC)

4.1 Общее описание

Эллиптическая криптография - это система шифрования с открытым ключом, основанная на теории эллиптических кривых. Чтобы зашифровать какое-либо сообщение, помимо раннее упомянутых параметров, нам потребуются еще 2:
1) Закрытый ключ d со случайным значением не менее 1 и не более $n - 1$.
2) Открытый ключ $Q = dG$.

Тогда можно заметить, что зная d и G достаточно просто найти значение Q. Но нахождение же закрытого ключа d по Q и G будет гораздо сложнее из-за решения задачи дискретного логарифмирования.

Далее я бы хотел рассмотреть алгоритмы, основанные на эллиптических кривых.

4.2 ECDH

Протокол Диффи-Хеллмана на эллиптических кривых (англ. Elliptic curve Diffie–Hellman, ECDH) — это криптографический протокол, позволяющий двум сторонам, у каждой из которых имеется пара открытый/закрытый ключ на эллиптических кривых, получить секретный ключ при помощи общего незащищенного канала связи. Этот алгоритм по своей сути похож на классический алгоритм Диффи-Хеллмана, за исключением использования умножения точек вместо подсчета экспоненты. Помимо этого при 528-битном ключе протокол ECDH более стойкий, чем классический протокол DH с 2048-битным ключом.

ECDH основан на том, что:

$$da * (d_b * G) = d_b * (d_a * G)$$

Пусть нашими закрытыми ключами являются числа d_a и d_b, а G – генератор подгруппы. Тогда назовем открытыми ключами точки $Q_b = (d_b * G)$ и $Q_a = (d_a * G)$. Тогда общий секрет можно вычислить как:

$$S = d_b * Q_a = d_a * Q_b.$$

Сам алгоритм имеет вид:
1) Алиса генерирует случайную пару ключей da и $Q_a = d_a * G$.
2) Боб генерирует случайную пару ключей db и $Q_b = d_b * G$.
3) Алиса и Боб обмениваются своими открытыми ключами через незащищенный канал связи.
4) Алиса вычисляет общий ключ $= d_a * Q_b$.
5) Боб вычисляет общий ключ $= d_b * Q_a$.
6) Алиса и Боб имеют один и тот же общий ключ, например координату x полученной точки.

Протокол уязвим против атаки посредника (англ. man in the middle, MITM) в случае, если посредник перехватит сообщения с открытыми ключами и вместо них отправит участникам свои сгенерированные ключи. Для предотвращения этой уязвимости необходима доверенная третья сторона, которая подпишет оба ключа. Помимо этого у протокола существуют вариация ECMQV против активных атак путем сочетания статического и временного ключей.

4.3 ECDSA

Алгоритм цифровой подписи на эллиптических кривых (англ. (Elliptic Curve Digital Signature Algorithm, ECDSA) – алгоритм с открытым ключом для создания цифровой подписи, определенный в группе точек эллиптической кривой. Похож по своей сути на алгоритм RSA, но при этом 256-битная подпись имеет такой же уровень безопасности, что и 3072-битный ключ в алгоритме RSA. Пара ключей состоит и закрытого ключа d и открытого ключа $Q = d * G$, являющегося точкой на эллиптической кривой. Так же необходимо заметить, что в алгоритме будет присутствовать вычисление обратного элемента по модулю n. Это накладывает ограничение на данный параметр: n должно быть простым, иначе может оказаться, что обратного элемента не существует.

Для подписи алгоритм ECDSA берет закрытый ключ и сообщение msg и выдает на выходе подпись в виде пары чисел r, s:
1) Вычисляется хеш h от сообщения: $h = hash(msg)$.
2) Генерируется некоторый случайный параметр k.
3) На его основе вычисляется точка $R = k * G$, тогда r является ее x-координатой.
4) Вычисляем $s = k^{-1}(h + rd)(mod\ n)$.
5) Возвращаем подпись r, s.

Для проверки подлинности необходимо:
1) Вычисляется хеш h от сообщения: h = hash(msg).
2) Вычислить обратный элемент $s_1 = s^{-1}(mod\ n)$.
3) Восстановить случайную точку $R' = (hs_1) * G + (rs_1) * Q$.
4) Взять x-координату точки R'.
5) Сравнить x и x'.

С математической точки зрения проверка на корректность алгоритма может быть осуществлена как:

$$s_1 = s^{-1}(mod\ n) = (k^{-1}(h + r * d))^{-1}(mod\ n) = k(h + r * d)^{-1}(mod\ n),$$
$$R' = (hs_1) * G + (rs_1) * Q = (hs_1) * G + (rs1) * d * G =$$
$$= (h + rd) * s1 * G = (h + rd) * k * (h + rd)^{-1} * G(mod\ n) =$$
$$= k * G => \text{сравниваем } R' \text{ и } R.$$

Важно так же учитывать, что для избежания известных атак, необходимо выбрать a и $b : D \neq 0$ так, чтобы порядок N группы точек, образованной такой элиптической кривой имел достаточно большой простой делитель n (по крайней мере $n > 2^{160}$ и $n > 4\sqrt{p}$). Так же $p^j - 1$ не должно являться делителем n для всех $j \in [1; 100]$ и $n \neq p$. Дополнительно при использовании алгоритма важно понимать, что если параметр k является предсказуемым, а не случайным, то атакующий может определить закрытый ключ.

4.4 Преимущества и распространение

Кау уже упоминалось ранее, преимуществом ECC по сравнению с большинством алгоритмов шифрования с открытым ключом, является использование меньших ключей. Это означает, что более надежное шифрование может быть достигнуто с меньшей пропускной способностью сети.

Если же говорить про сложность вычислений, то все обстоит несколько сложнее. В случае алгоритма RSA для операций шифрования, расшифрования и проверки подписи основную вычислительную сложность представляет вычисление $h^e mod\ n$, где (e, n) - открытый ключ. При использовании алгоритма быстрого возведения в степень требуетсы $O(log\ e)$ умножений по модулю. Причем чем больше нулевых бит в двоичном представлении числа e, тем быстрее скорость шифрования. Умножения же в случае ECC и применения алгоритма удвоения-сложения имеет сложность O(log n). Так, RSA оказывается быстрее при проверке подписи, а ECDSA при подписании (уже до 10 раз быстрее при 128-битном уровне безопасности). Но RSA имеет худшую длину и худшую масштабируемость длины ключей. Так, постоянное повышение требований безопасности увеличивает перевес в сторону ECDSA.

Такие преимущества делают алгоритмы на базе ECC привлекательными для маломощных мобильных устройств и устройств Интернета вещей. Помимо этого системы на эллиптических кривых используются в таких стандартах как, например, ANSI, IEEE, ISP, SEGG и протоколах TLS и SSH.

5 Заключение

На этом обзорная статья заканчивается. На основе всего вышесказанного можно сказать, что использование такой математической абстракции, как эллиптические кривые, позволяет благодаря сложности решения задачи дискретного логарифмирования перейти к алгоритмам, обладающим эквивалентной стойкостью при гораздо меньших длинах ключей и затратах на вычисление по сравнению с аналогами, основанными на сложности задачи факторизации. Еще раз заметим, что хотя на текущий момент эллиптическая криптография достаточно широко распространена, ничто не запрещает найти алгоритмы, из-за которых придется отказаться от вычислений по крайней мере на некоторых классах кривых.

6 Используемая литература

1. Alfred J.Menezes, PaulC.van Oorschot and Scott A.Vanstone. Handbook of applied cryptography — CRC Press, 1997.

2. Standards for Efficient Cryptography Group (SECG), SEC 1: Elliptic Curve Cryptography, Version 1.0, 2000.

3. А. Болотов, С. Гашков, А. Фролов, А. Часовских — Элементарное введение в эллиптическую криптографию, 2006.

4. D. Brown. Generic groups, collision resistance, and ECDSA, 2002.

5. RSA vs. ECC Comparison for Embedded Systems. RSA vs. ECC Comparison for Embedded Systems, 2020

6. $https://cryptobook.nakov.com/asymmetric-key-ciphers/$

7. $https://en.wikipedia.org/wiki/Elliptic_curve$

8. $https://avinetworks.com/glossary/elliptic-curve-cryptography$

9. $https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction$

10. $https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography$