Эссе по курсу «Информационная безопасность»
студента 014 гр. Гапона А.В.

Elliptic Curves Cryptography.
Криптография на эллиптических кривых.

Цифровая подпись.

Общеизвестно, что цифровая подпись файлов или электронных почтовых сообщений выполняется с использованием криптографических алгоритмов, использующих несимметричные ключи: собственно для подписи используется «секретный ключ», а для проверки чужой подписи — «открытый». Ключи представляют собой числа достаточно большой длины (от 512 до 4096 бит), математически связанные между собой.

Цифровая подпись сообщения — это последовательность бит фиксированной длины, формирующаяся по тексту сообщения с использованием секретного ключа его создателя. Корректность подписи проверяется с помощью открытого ключа. Цифровая подпись отправляется вместе с сообщением, и, обычно, становится неотъемлемой его частью. Получатель сообщения должен располагать копией открытого ключа отправителя. Схемы распространения открытых ключей могут быть разными: от простого личного обмена ключами до сложной многоуровневой «инфраструктуры открытых ключей» (Public Key Infrastructure — PKI). Если при проверке цифровой подписи получатель устанавливает ее корректность, то может быть уверен не только в неизменности и «актуальности» сообщения, но — что самое важное — и в том, что сообщение «подписал» действительно его автор или отправитель.

Криптографическим алгоритмом для цифровых подписей и шифрования симметричными ключами (для целей распространения) является RSA (Rivest, Shamir и Adleman). Хотя RSA имеет высокую степень защиты и широко применяется, его применение связано с некоторыми проблемами. Рассмотрим альтернативную технологию, основанную на математическом методе эллиптических кривых, которая в некоторых случаях дает существенные преимущества перед RSA.

Еще в 1998 году ISO, в 1999-м ANSI, а в 2000 году IEEE и NIST приняли новый стандарт для цифровой подписи ECDSA (Elliptic Curve Digital Signature Algorithm), основанный на использовании эллиптических кривых. С принятием алгоритма Национальным институтом стандартов США он получил статус федерального стандарта. Рассмотрим математические принципы, лежащие в основе этого стандарта.

Некоторые сведения из математики.

В алгоритмах цифровой подписи активно используются вычисления в конечных полях. Обратимся к некоторым математическим понятиям, связанным с полями Галуа.

Будем говорить, что целое положительное число *a сравнимо с b по модулю p* ($a \equiv b \mod p$), если остаток от деления b на p равен a.

Можно ввести операции сложения и умножения «по модулю p». А именно, результатом сложения двух чисел по модулю p будем считать остаток от деления их суммы на число p. Аналогичным образом определим и произведение. Нетрудно заметить, что результаты операций сложения или умножения пары произвольных неотрицательных целых чисел по модулю p не будут превосходить число p. В результате, можно ограничится рассмотрением множества чисел 0, 1… p–1 с заданными на нем операциями сложения и умножения по модулю p. Множество 0, 1… p–1 с заданными операциями сложения и умножения, подчиняющимися обычным школьным законам сложения, умножения и раскрытия скобок, образуют «кольцо классов вычетов по модулю p».

Элемент b называется *обратным* к элементу a, если ab = 1. Обратный элемент обозначается a^{-1}. Оперируя только целыми неотрицательными числами, нетрудно ввести операцию деления как умножение на обратный элемент, операцию вычитания и даже «отрицательные» числа. Оказывается, если p — простое число, то обратный элемент существует для всех элементов кольца (кроме, естественно, числа 0). Кольцо классов вычетов, для каждого элемента которого (кроме 0) существует обратный элемент, называют *простым полем* (или *конечным полем*, или *полем Галуа*) и обозначается GF(p).

Эллиптические кривые.

Эллиптической кривой называют множество пар точек (X,Y), удовлетворяющих уравнению:

$$y^2 = ax^3 + bx + c$$

Можно наложить ограничения на множество значений переменных x, y, и коэффициентов a, b, c. Ограничивая область определения уравнения значимым для приложений числовым множеством (полем) мы получим эллиптическую кривую, заданную над рассматриваемым полем. На рис. 2 изображен общий вид эллиптической кривой, определенной на множестве действительных чисел.

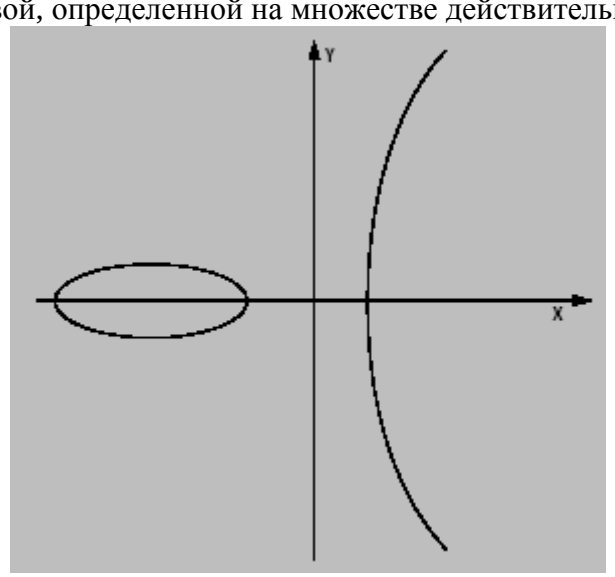

Рис.1. Общий вид эллиптической кривой.

В приложении к криптографии (и в новом стандарте на цифровую подпись) эллиптическая кривая над конечным простым полем GF(p) определяется как множество пар (x,y), таких что x,y ≡ GF(p), удовлетворяющих уравнению:

$$y^2 = x^3 + ax + b \mod p, \quad a, b \equiv GF(p)$$

Пары (x,y) будем называть *точками*. Точки эллиптической кривой можно складывать. Сумма двух точек, в свою очередь, тоже лежит на эллиптической кривой.

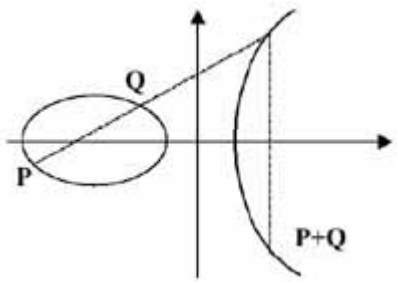

Рис.2. Сложение точек на эллиптической кривой.

Математическое свойство, которое делает эллиптические кривые полезными для криптографии, состоит в том, что если взять две различных точки на кривой, то соединяющая их хорда пересечет кривую в третьей точке (так как мы имеем кубическую кривую). Зеркально отразив эту точку по оси X, мы получим еще одну точку на кривой (так как кривая симметрична относительно оси X). Если мы обозначим две первоначальных точки как P и Q, то получим последнюю – отраженную – точку P+Q. Это «сложение» удовлетворяет всем известным алгебраическим правилам для целых чисел.

Кроме точек, лежащих на эллиптической кривой, рассматривается также *нулевая точка*. Считается, что сумма двух точек – A с координатами (X_A, Y_A) и B с координатами (X_B,Y_B) – равна 0, если $X_A = X_B$, $Y_A = -Y_B$ (mod p). Нулевая точка не лежит на эллиптической кривой, но, тем не менее, участвует в вычислениях. Ее можно рассматривать как бесконечно удаленную точку.

Таким образом, мы можем определить конечную абелеву группу на точках кривой, где нулем будет являться бесконечно удаленная точка. В частности если точки P и Q совпадут, то можно вычислить P+P, т.е. 2P. Развивая эту идею, можно определить kP для любого целого числа k, и следовательно, определить значение P и значение наименьшего целого числа k, такого, что kP = F, где F – бесконечно удаленная точка. Теперь можно сформулировать *«Проблему дискретного логарифма эллиптической кривой»* (Elliptic Curve Discrete Logarithm Problem – ECDLP), на которой основана рассматриваемая система:

«Даны “базовая точка” P и расположенная на кривой точка kP; найти значение k». Для эллиптических кривых и базовых точек решение таких уравнений представляет весьма и весьма большую трудность! С точки же зрения криптографии мы имеем возможность определить новую криптографическую систему на основе эллиптических кривых. Учтите, что любая стандартная система, основаная на проблеме дискретного логарифма, аналогична системе основанной на ECDLP. Например, Эллиптическая Кривая DSA (ECDSA) уже стандартизированна (ANSI X9.62) и на ее основе может быть реализован протокол открытого обмена ключами Diffie-Hellman.

Для каждой эллиптической кривой число точек в группе конечно, но достаточно велико. Оценка порядка (числа элементов) группы точек эллиптической кривой m такова:

$$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p},$$

где p — порядок поля, над которым определена кривая. Если в схеме Эль-Гамаля рекомендуется использовать число p порядка 2^{512}, то в случае эллиптической кривой достаточно взять $p > 2^{255}$.

Использование эллиптических кривых для создания стандарта цифровой подписи.

Кратные точки эллиптической кривой являются аналогом степеней чисел в простом поле. Задача вычисления кратности точки эквивалентна задаче вычисления дискретного логарифма. Собственно, на сложности вычисления кратности точки эллиптической кривой и основана надежность цифровой подписи. Хотя эквивалентность задачи дискретного логарифмирования и задачи вычисления кратности и доказана, вторая имеет большую сложность. Именно поэтому при построении алгоритмов подписи в группе точек эллиптической кривой оказалось возможным обойтись более короткими ключами по сравнению с простым полем при обеспечении большей стойкости.

Секретным ключом, как и раньше, положим некоторое случайное число x. Открытым ключом будем считать координаты точки на эллиптической кривой P, определяемую как P = xQ, где Q — специальным образом выбранная точка эллиптической кривой («базовая точка»). Координаты точки Q вместе с коэффициентами уравнения, задающего кривую, являются параметрами схемы подписи и должны быть известны всем участникам обмена сообщениями.

Выбор точки Q зависит от используемых алгоритмов и весьма непрост. Так, стандарт ГОСТ 34.10-2001 определяет, что точка Q должна иметь порядок q, где q — простое число с «хорошими алгебраическими свойствами». Число q довольно велико ($2^{254} < q < 2^{256}$). При построении конкретного алгоритма, реализующего вычисление цифровой подписи, американский стандарт предполагает использование алгоритма DSA. Новый российский стандарт использует модифицированную версию старого ГОСТ Р 34.10-94. Оказалось, оба они хорошо подходят для реализации в группе точек эллиптической кривой без особых модификаций. Некоторые специалисты отмечают даже, что описание алгоритма цифровой подписи Эль-Гамаля на эллиптической кривой «проще и естественней».

Из-за очевидной трудности взлома алгоритм ECDLP можно применять для высоко защищенных систем; обеспечивая сопоставимый уровень безопасности, алгоритм имеет значительно меньшие размеры ключа, чем, например, алгоритмы RSA или DSA. В приведенной ниже таблице сравниваются приблизительные размеры параметров эллиптических систем и RSA, обеспечивающих одинаковую стойкость шифра, которая рассчитывается на основе современных методов решения ECDLP и факторинга (поиска делителей) для больших целых чисел.

Система на основе эллиптической кривой (базовая точка P)	RSA (длина модуля n)
106 бит 132бит 160бит 224бит	512бит 768бит 1024бит 2048бит

Следовательно, использование эллиптических кривых позволяет строить высоко защищенные системы с ключами явно меньших размеров по сравнению с аналогичными “традиционными” системами типа RSA или DSA. В частности такие системы менее требовательны к вычислительной мощности и объему памяти оборудования и потому хорошо подходят, например, для смарт-карт или портативных телефонов.

Разумеется существуют и проблемы, которые ограничивают повсеместное распространение криптографических систем на основе эллиптических кривых.

Некоторые проблемы и трудности в использовании систем на основе эллиптических кривых.

1) Реальная безопасность таких систем все еще недостаточно осознана.

Главная проблема состоит в том, что истинная сложность ECDLP ещё не осознана полностью. Недавнее исследование показало, что некоторые использовавшиеся для отработки алгоритмов шифрования эллиптические кривые, фактически не подходят для таких операций. Например, если координаты базовой точки P равны положению p, то ECDLP имеет простое решение. Такие кривые являются “аномальными” кривыми.

Исследования в этой области продолжаются по сей день, но потенциальные пользователи все еще проявляют осторожность и выжидают.

2) Трудность генерации подходящих кривых.

При определении системы эллиптической кривой требуются сама кривая и базовая точка (P). Обратите внимание на то, что эти элементы не являются тайной и могут быть одинаковыми для всех пользователей системы. Для данной кривой и точки несложно сгенерировать открытые и частные ключи для пользователей (частный ключ – просто случайное целое число k, а открытый ключ –точка kP на кривой). Однако, чрезвычайно трудно создать подходящую кривую и точку. Главная проблема – подсчитать количество точек на кривой. Для этого необходимо выбрать подходящую базовую точку P, координаты которой должны иметь достаточно большое значение, чтобы гарантировать трудность взлома ECDLP. Но координаты P должны делиться на количество точек на кривой (помните, что точки на кривой вместе с бесконечно удаленной точкой образуют конечную группу). И весьма вероятно, что, найдя число точек на кривой, мы не сможем найти базовую точку.

Подводя итог вышеизложенному, можно утверждать, что создание кривых – непростая задача. Пользователи могут использовать «стандартные» кривые, используя специальное программное обеспечение (типа THALES “Elliptic Curve Generation Bureau”), либо создавать собственные кривые, что занимает много времени.

3) Относительно медленная проверка цифровой подписи.

Как уже было упомянуто, системы на основе эллиптической кривой используют ключи малых размеров. Это снижает требования к вычислительным мощностям по сравнению с требованиями систем на основе RSA. Как это влияет на скорость обработки? Следующая таблица показывает сравнительные характеристики алгоритмов RSA и ECDSA (нечетный) при создании и проверки подписей; оба алгоритма выполнялись на параллельных процессорах Motorola 56303 DSP (66 МГЦ). Обратите внимание, что функция проверки подписи RSA использует при проверке подписи e = 65537.

	Создание подписи	Проверка подписи
RSA (1024 бита)	25 ms	< 2 ms
ECDSA (160 бит)	32 ms	33 ms
RSA (2048 битов)	120 ms	5ms
ECDSA (216 битов)	68 ms	70 ms

Ясно, что различные способы выполнения покажут различное время, но примерная скорость ясна. При увеличении размеров ключа создание подписей с помощью ECDSA производится значительно быстрее чем в аналогичных RSA системах. Это различие в ещё большей степени проявляется для однопроцессорных систем. С другой стороны проверка

подписи с помощью ECDSA производится намного медленнее чем эта же процедура в системах RSA и опять же это различие усиливается для систем с одним процессором. Обратите внимание, что обработка ECDSA несколько ускориться в “четном” случае. Мощность процессора затраченная на проверку подписи при использовании, скажем, ECDSA, может замедлить выполнение других приложений в системе. Множество систем имеют большое количество удаленных устройств, соединенных с центральным сервером и время, затраченное удаленным устройством для создания подписи – несколько секунд – не влияет на производительность системы в целом, но сервер должен также и подтверждать подписи причем очень быстро и в некоторых случаях системы RSA (даже использующие большие ключи) возможно, будут более приемлемы для использования, чем криптосистемы на основе эллиптической кривой.

Заключение.

Криптосистемы на основе эллиптической кривой получают все большее распространение скорее как альтернатива, а не замена системам на основе RSA, поскольку системы на основе ECDLP имеют некоторые преимущества, особенно при использовании в устройствах с маломощными процессорами и/или маленькой памятью. Типичные области применения:

- m-commerce (мобильная торговля) (например, WAP сотовые телефоны, карманные компьютеры);
- смарт-карты (например, EMV);
- e-commerce (электронная торговля) и банковские операции (например, SET);
- интернет-приложения (например, SSL).

Ссылки:

1. Семенов.Г. «Цифровая подпись. Эллиптические кривые». http://www.morepc.ru/security/crypt/os200207010.html?print
2. Dr. Michael Ganley, THALES eSECURITY Ltd. «Метод эллиптических кривых». http://www.racal.ru/rsp/eliptic_curve_cryptography.htm