ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ В ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Коминч В.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Станкевич А.В. – к.т.н.,доцент

В век технологий, когда электронный документооборот, если не преобладает над бумажным, то составляет ему большую конкуренцию, особенно важно задуматься об идентификации и сохранности важных данных. Множество предприятий, перешедших на электронную документацию, всячески пытаются обезопасить себя от подделок каких-либо ценных бумаг и попадания их «в руки» конкурентов. Ученые и специалисты всего мира для этих целей разрабатывают всё новые алгоритмы электронной цифровой подписи. В данном докладе рассматривается алгоритм электронной цифровой подписи на эллиптических кривых, описанном в белорусском стандарте СТБ 34.101.45 – 2013, а также его аппаратная реализация на базе ПЛИС.

Для работы алгоритма необходимы несколько параметров: входное сообщение, имеющее произвольную длину, личный ключ и параметры эллиптической кривой, необходимые для формирования подписи. Длина личного ключа зависит от уровня стойкости, который зависит от алгоритма хэширования, использующегося в процессе генерации ЭЦП.

Уравнение эллиптической кривой над конечным полем Fp выглядит следующим образом:

$$y^2 = x^3 + a * x + b \ (mod\ p) \quad (1),$$

где p - большое простое число.

Оно представляет собой кривые Вейерштрасса, обладающие некоторыми свойствами. Кривая имеет характеристику 0, поэтому является плоской. Она не имеет самопересечений, что достигается выполнением условия дискриминта.

Множество точек, являющихся решением данного уравнения, образуют конечное поле. В данном поле определена одна особая точка, расположенная на бесконечности и представляющая аналог нуля для чисел, и некоторые операции над точками кривой, такие как сложение и умножение точки на константу. Также определен обратный элемент, который получается вычитанием из ординаты координаты точки.

Операция сложения определена как алгебраически, так и геометрически. Геометрический смысл сложения заключается в пересечении прямой, образующейся двумя слагаемыми точками, с кривой и отражении полученной точки относительно вертикальной прямой. Алгебраическая форма имеет две формулы для равных и разных точек.

Операция умножения представляется через сложение точки N раз. Таким образом, напрямую операцию невозможно выполнить. В работе рассматриваются некоторые возможные реализации данной операции.

С операцией умножения на константу связана основная задача по взлому эллиптических кривых. Она носит название задачи дискретного логарифмирования. Её суть заключается в подборе того коэффициента, на который умножали базовую точку. Именно этот коэффициент является закрытым ключом.

Также определена операция умножения двух чисел по модулю. Так как числа имеют большую длину(минимально 128 бит), то для их реализации необходимо использовать некоторые схемы ускоренного умножения. Принципиальная разница заключается лишь в способе вычисления, так как возможно найти результат умножения, а затем найти остаток от деления, а можно проводить последовательные упрощения, сокращая разрядность промежуточного результата.

Кроме того, нетипичную реализацию имеет операция деления. Она определена таким образом, чтобы заменить деление умножением с взаимно простым числом. Данная операция представляет собой нахождение взаимно простых чисел.

Вместе с тем, большую роль выполняет реализация операции умножения на константу, так как она подвержена, так называемым, атакам по времени. В зависимости от значения личного ключа, время работы алгоритма может отличаться. Поэтому, чтобы обезопасить устройство, на практике алгоритмы “уравновешивают”, делая атаки по времени сложно достижимыми.

На практике одним из самых распространённых алгоритмов является алгоритм Монтгомери, позволяющий выполнять умножение точки на константу за константное время. Другим способом безопасного вычисления является использование оконной функции, с подобранным размером окна.

На рисунке 1 представлена структурная схема устройства для генерации цифровой подписи. В случае использования эллиптической кривой из стандарта схему можно упростить, убрав генератор параметров эллиптической кривой и подавая на вход блоков электронной подписи соответствующие параметры. Кроме того генератор ключей также является необязательным блоком в схеме, так как

пользователь может иметь уже сгенерированный ключ. Сообщение для устройства подаётся блоками, так как изначально алгоритм может работать с данными произвольной длины.

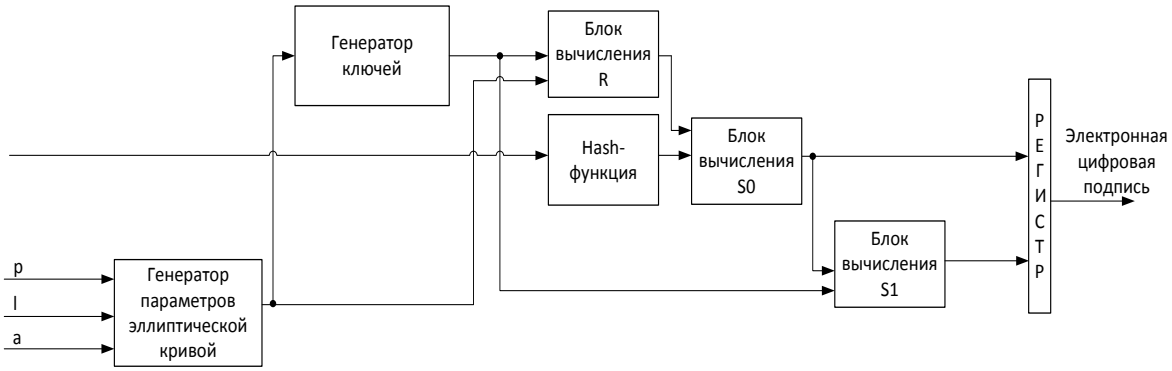

Рисунок 1 – Структурная схема устройства для выработки электронной цифровой подписи

$R = k * G$, где G – базовая точка, являющаяся выходом генератора параметров эллиптической кривой. Блоки S0 и S1 являются частями итоговой подписи и выражаются следующими формулами:

$S_0 =< belt - hash(OID(h)|| < R >_{2l} ||H) >_l$,

$S_1 =< (k - \bar{H} - (\bar{S}_0 + 2^l)d \bmod q) >_{2l}$, где belt-hash – функция хэширования, H – выход блока хэш-функции, OID – идентификатор функции($06092A7000020022651F51_{16}$), R – выход блока вычисления R, d – личный ключ, q – порядок группы точек из поля Fp.

Идентификатор функции для алгоритмов, не представленных в стандарте, может быть вычислен по алгоритму из стандарта.

Уровень стойкости равен 128. Длина итоговой подписи равна 384 бита.

Одним из блоков алгоритма электронной цифровой подписи является блок вычисления функции хэширования. По умолчанию, в стандарте используется функция из стандарта СТБ 34.101.31-2011, в основе вычисления которой лежит алгоритм блочного шифрования из того же стандарта. При использовании данной хэш-функции в алгоритме электронной цифровой подписи на ее вход подается сообщение фиксированной длины. На выходе функции получается хэш-значение длиной 256 бит. Данный алгоритм используется в настоящей подписи. При выборе другого значения в качестве уровня стойкости данный алгоритм будет некорректным и необходимо выбрать другой.

Алгоритм шифрования, приведённый в стандарте, имеет множество архитектурных решений. В настоящей работе рассматриваются различные реализации и приводится их сравнение. Основными критериями сравнения были производительность и расход ресурсов.

Рассматриваются различные архитектурные решения операций в конечном поле, которые являются модулярными и должны удовлетворять временным ограничениям для невозможности реализации атаки по времени. Кроме того, они должны иметь приемлемый расход ресурсов для того, чтобы всё устройство можно было разместить в кристалле.

Также при реализации алгоритма рассматриваются несколько систем координат, упрощающих аппаратную реализацию либо усложняющих взлом подписи. Они, напрямую, влияют на реализацию операций по модулю, делая их сложнее, но избегая операции деления.

Наконец, для проверки правильности генерации подписи используется алгоритм проверки, приведённый в стандарте и реализованный аппаратно. Он включает в себя те же операции, что и устройство формирования подписи.

Сильной стороной устройств на основе эллиптических кривых несомненно защищённость информации от кражи. Вместе с тем, наличие у злоумышленника личного ключа пользователя

Приведенное устройство реализуется на базе FPGA семейства Virtex 7 фирмы Xilinx.

Аппаратную реализацию цифровой подписи можно использовать для проверки транзакций криптовалют, цифровых операций с валютами (платежами), подписи на электронные документы и любые другие файлы.

Список использованных источников:

1. Информационные технологии. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых : СТБ 34.101.45–2013. – Введ. 30.08.2013. – Минск : Госстандарт, 2013. – 41 с.

2. Информационные технологии. Криптографические алгоритмы шифрования и контроля целостности : СТБ 34.101.31–2011. – Введ. 31.01.2011. – Минск : Госстандарт, 2011. – 32 с.

3. https://ru.wikipedia.org/wiki/ Эллиптическая_кривая

4. https://ru.wikipedia.org/wiki/ Дискретное_логарифмирование_на_эллиптической_кривой

5. http://wiki.ru/wiki/Алгоритм_Монтгомери(эллиптические_кривые)