ЭПГОСТ Р 34.10-2001

Аметов Имиль, гр. М07-903

1 июня 2020 г.

Задача:

Соображения о сложности вычислений с очень большими числами для стандарта ЭПГОСТ Р 34.10-2001.

Решение:

Вначале выполняется выбор простого числа $p > 2^{255}$, задаются значения для эллиптической кривой.

Нахождение ранга эллиптической кривой по алгоритму Шуфа с использованием быстрых операций с многочленами и целочисленной арифметикой позволяет добиться сложности алгоритма в $O(\log^5 p)$.

После определения ранга эллиптической кривой нужно искать точку с нужным порядком. Здесь для определения порядка точки можно применять метод со скалярным умножением через удвоение-сложение. Для удвоения-сложения нужно будет в худшем случае выполнить $\log_2 q$ умножений на 2 и столько же сложений, здесь q — это искомый порядок точки.

После нахождения подходящей точки P нужно выбрать случайное число d и вычислить точку $Q = dP$. Это ещё $2 \log_2 d$ операций.

На этом заканчивается формирование закрытого и открытого ключа. Всего на генерацию ключей приходится $\log^5 p + 2 \log_2 q + 2 \log_2 d$ операций.

Для создания подписи основную алгоритмическую нагрузку создают вычисление хеша от сообщения и вычисление точки $C = kP$, где k — это случайное число, а P — генератор группы.

Для проверяющей подпись стороны алгоритмическую нагрузку создаёт вычисление хеша сообщения, нахождение обратных значений для $(h(M) \mod q)^{-1} \mod q$, где $h(M)$ — функция вычисления хеша для сообщения M. И вычисление $aP + bQ$.