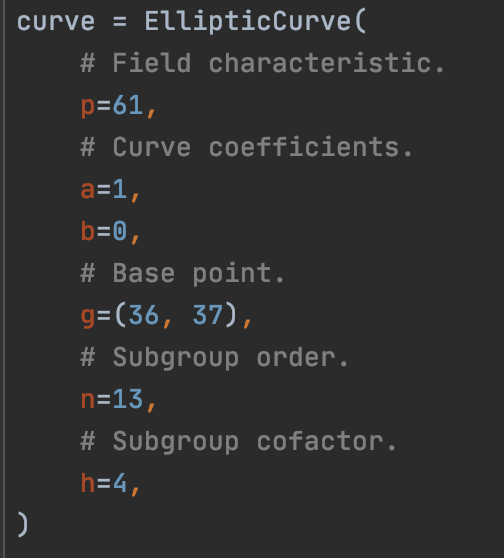
Отчет. Лабораторная работа №3

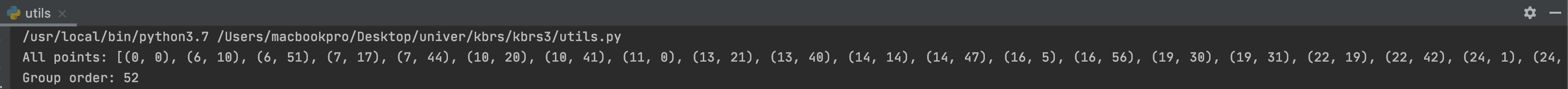
Лобко Артем

4 курс, 12 группа

Подобранные параметры (Вариант 4):



Часть элементов эллиптической группы:



Алгоритм шифрования:

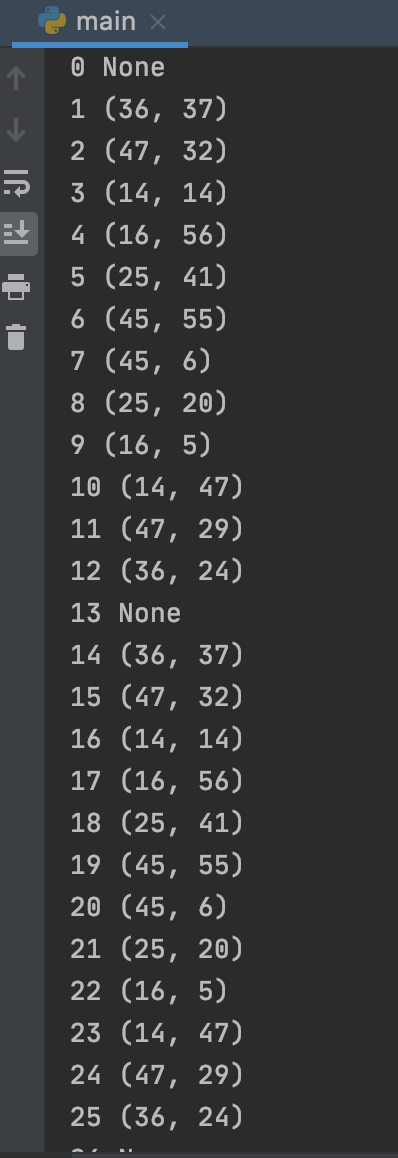
1. Сначала **Алиса и Боб генерируют собственные закрытые и открытые ключи**. У Алисы есть закрытый ключ dA и открытый ключ HA=dAG, у Боба есть ключи dB и HB=dBG
2. **Алиса и Боб обмениваются открытыми ключами**HA**и**HB**по незащищённому каналу**.
3. **Алиса вычисляет**S=dAHB (с помощью собственного закрытого ключа и открытого ключа Боба), **а Боб вычисляет**S=dBHA (с помощью собственного закрытого ключа и открытого ключа Алисы).

Алгоритм, выполняемый Алисой для подписывания сообщения, работает следующим образом:

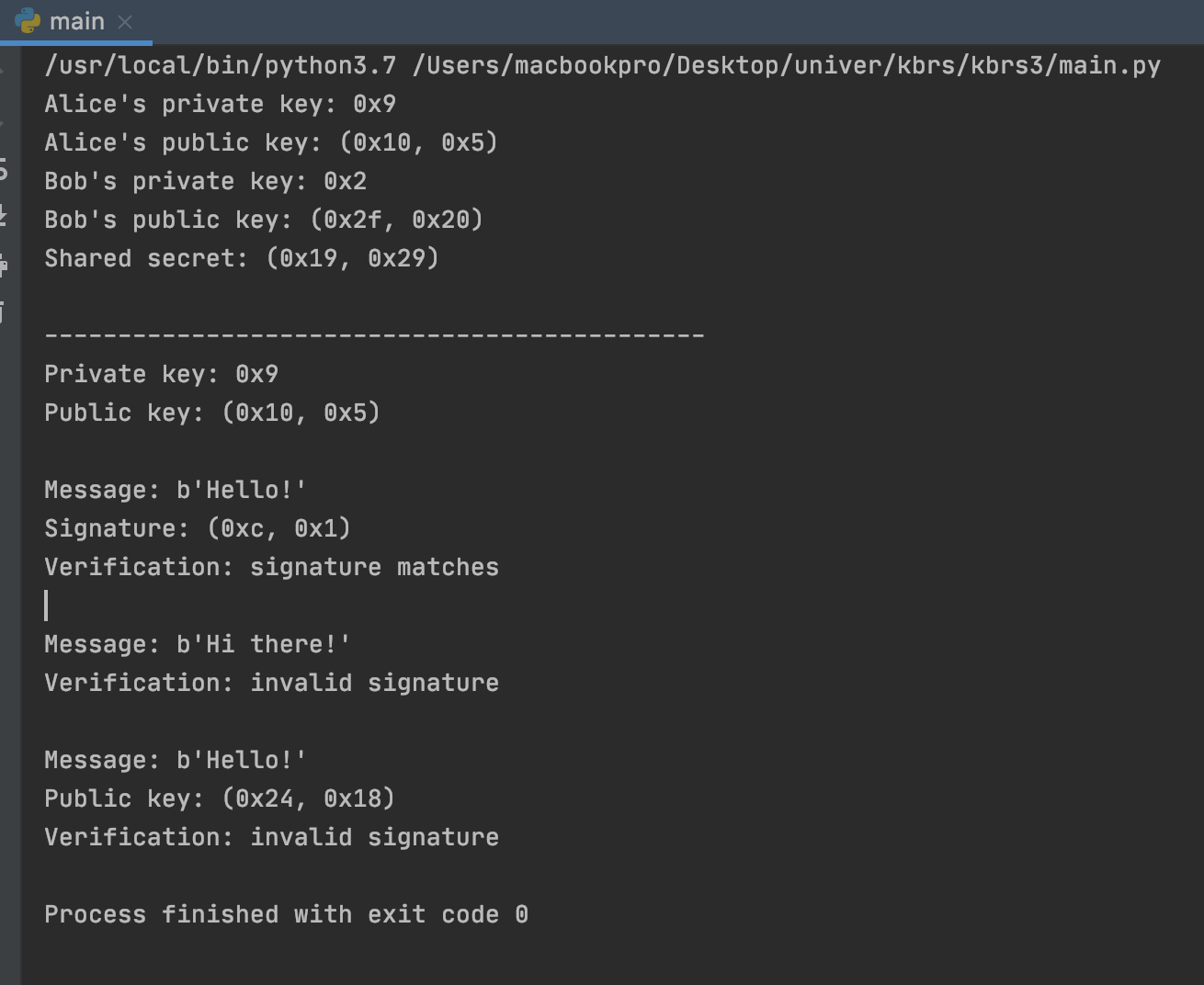
1. Берём **случайное целое**k, выбранное из {1,…,n−1} (где n — порядок группы).
2. Вычисляем точку P=kG (где G — базовая точка подгруппы).
3. Вычисляем число r=xPmodn (где xP — это координата x P).
4. Если r=0, то выбираем другое k и пробуем снова.
5. Вычисляем s=k−1(z+rdA)modn (где dA — закрытый ключ Алисы, а k−1 — мультипликативная инверсия k по модулю n).
6. Если s=0, то выбираем другое k и пробуем снова.

Пара (r,s)**является подписью**.

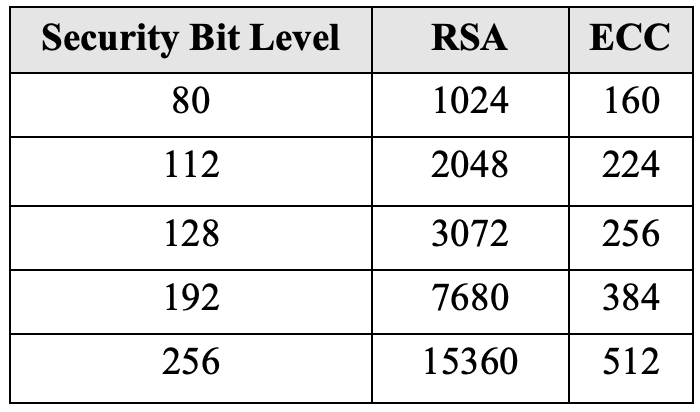
Циклические подгруппы, полученные программой:



Обмен сообщениями:

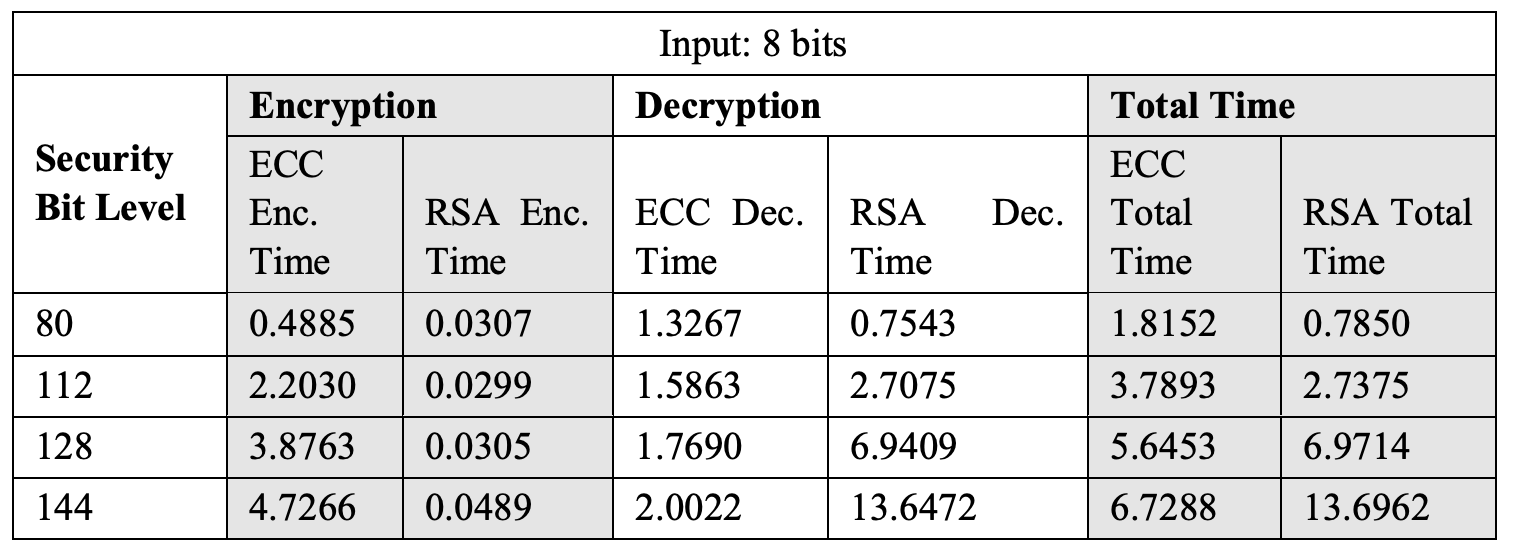


для того же уровня безопасности, в ECC можно использовать значительно меньшие параметры, чем в RSA. Например, для достижения уровня безопасности 112 бит RSA алгоритм требует размер ключа 2048 бит, в то время как ECC требует размер ключа 224 бит.

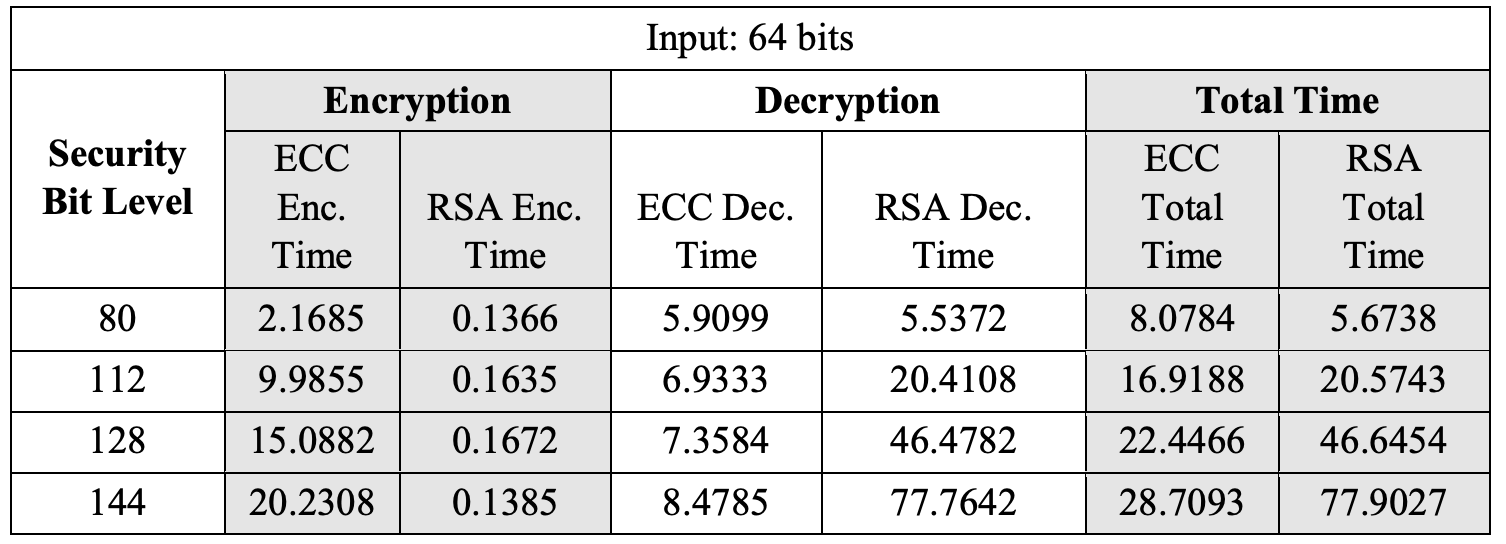


RSA очень эффективен в шифровании, но медленнее в дешифровании, а ECC медленнее в шифровании, но очень эффективен в дешифровании. В целом ECC более эффективен и безопасен, чем RSA.

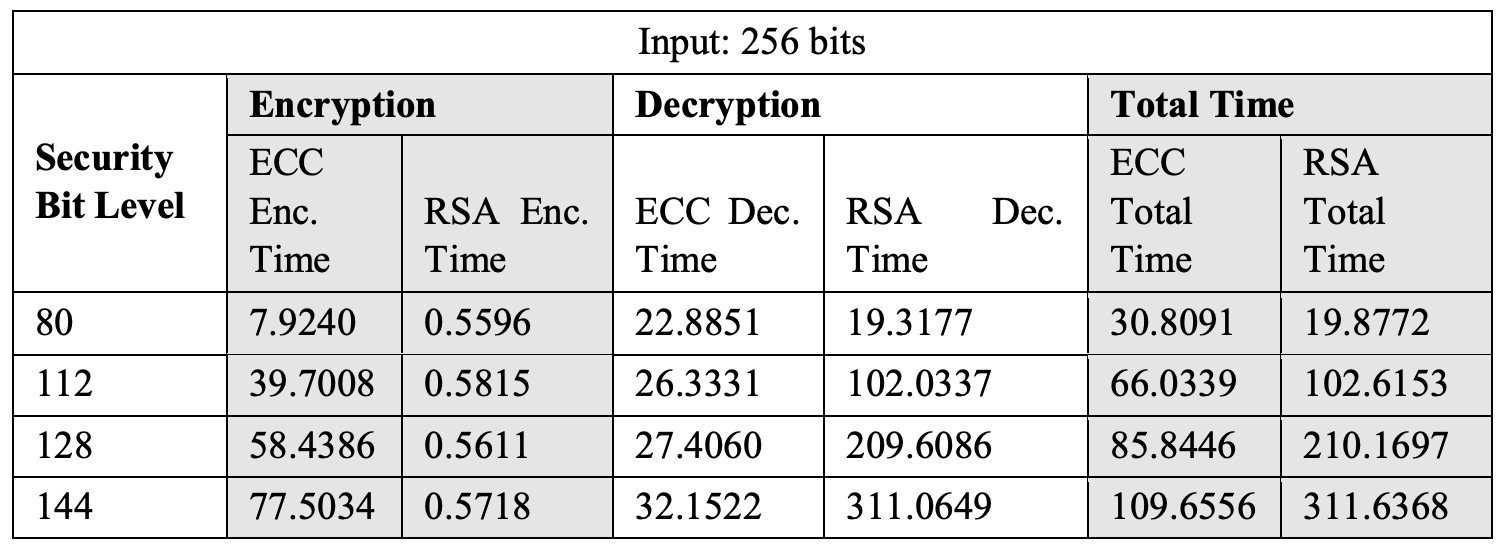
8 bits:



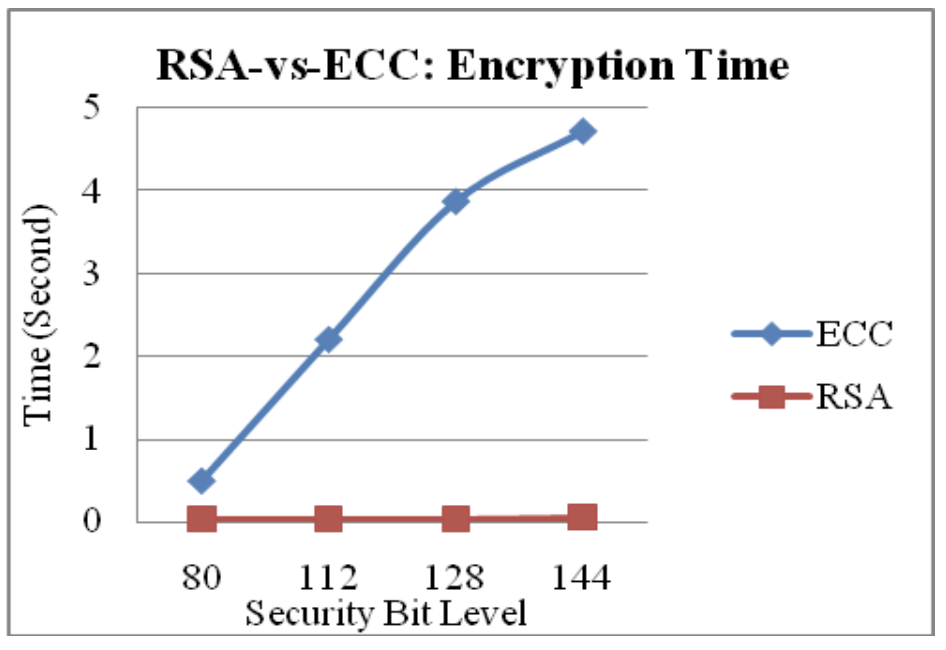
64 bits:



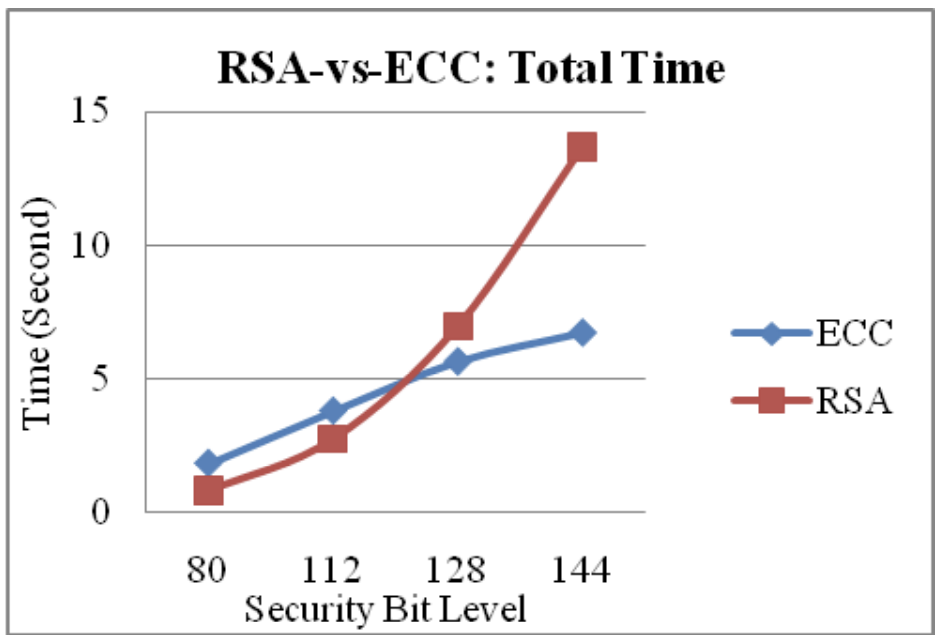
256 bits:



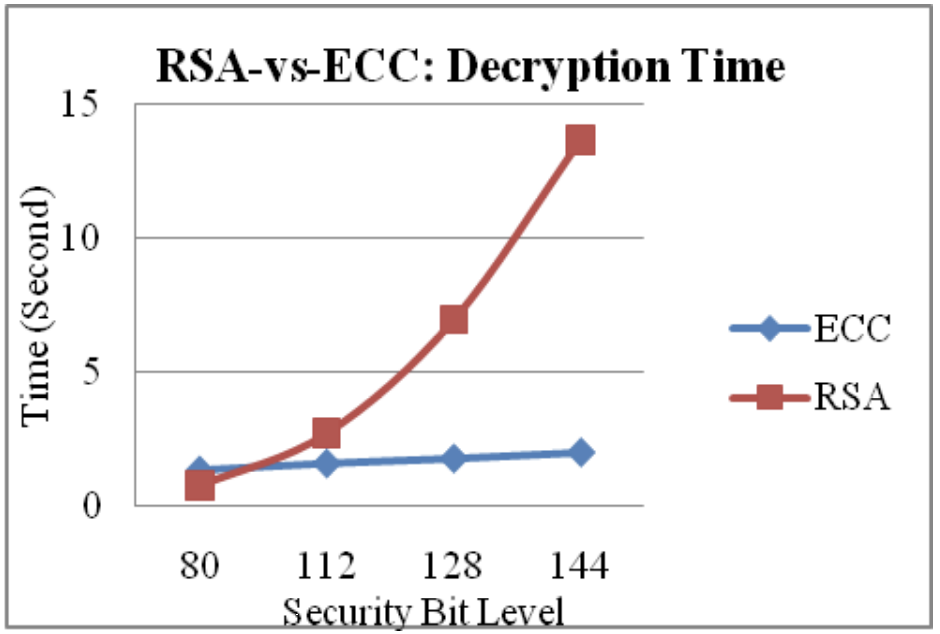
8 bits время шифрования:



8 bits общее время:



8 bits расшифрование:



Для 64 и 256 bits ситуация аналогичная.

**Результат:** ECC превосходит RSA по операционной эффективности и

безопасность с меньшими параметрами.