А.В. Короткевич (УО «БГУИР», Минск)
Науч. рук. **В.Н. Ярмолик**, д-р техн. наук, профессор

ПРОИЗВОДИТЕЛЬНОСТЬ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА БАЗЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В современном информационном обществе безопасность информации приобретает огромное значение. Такая безопасность может обеспечиваться различными криптографическими методами, одним из самых перспективных среди которых является использование криптосистем, основанных на свойствах эллиптических кривых.

Практически любая ассиметричная криптосистема может быть переложена на эллиптические кривые, однако не для всех схем это дает выигрыш в стойкости [1]. Например, для системы RSA и родственных ей систем, основанных на сложности задачи факторизации, это не усиливает схему. Но в то же время для криптосистем, базирующихся на сложности задачи логарифмирования в дискретных полях, переход на эллиптические кривые позволяет существенно увеличить стойкость схемы. Это возможно благодаря тому, что при надлежащем выборе параметров кривой задача логарифмирования в группе точек кривой существенно сложнее задачи логарифмирования в мультипликативной группе исходного поля. Потому эллиптических кривые являются хорошим решением при выборе способа защиты важных данных.

Основным недостатком эллиптических криптосистем, как и других ассиметричных криптосистем, является их высокая вычислительная сложность. Как следствие, необходимо тщательно оптимизировать все используемые при шифровании данных алгоритмы. Используя схему Менезеса-Ванстоуна на базе эллиптических кривых, можно выделить следующие оптимизируемые алгоритмы: умножение точки эллиптической группы на число, мультипликативная инверсия числа по модулю, возведение в степень по модулю [2].

Схема Менезеса-Ванстоуна предоставляет возможность шифрования точки эллиптической кривой. То есть точка эллиптической кривой является минимальным шифруемым блоком данных. Потому появляется проблема оптимального разбиения шифруемого набора данных на блоки. Очевидно, что исходный набор данных можно представить в виде одного блока данных; в таком случае первая половина набора определяет координату X точки, вторая – координату Y. При делении исходного набора данных на максимальное число блоков код каждого символа будет являться координатой точки (X или Y). Результаты исследования оптимального размера шифруемого блока представлены на рисунке 1.

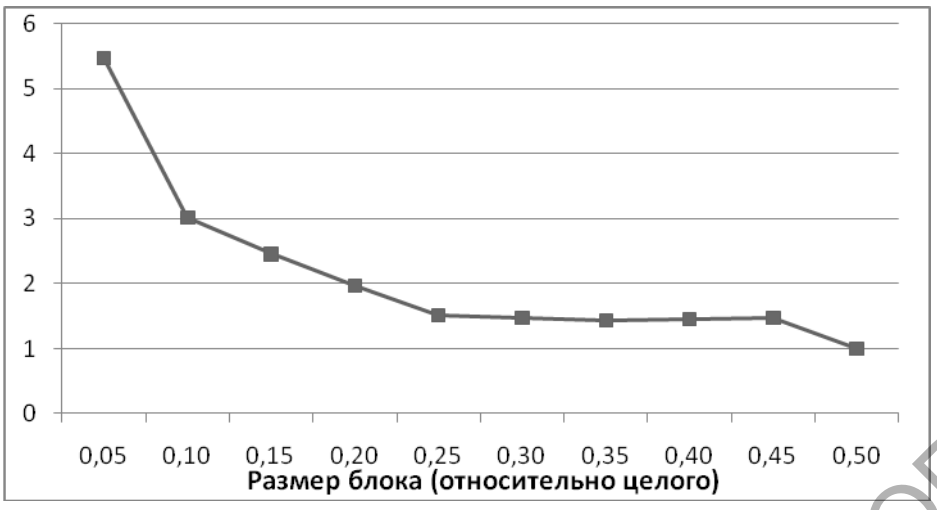

Рисунок 1 – Время шифрования в зависимости от размера блока

Как видно из графика, оптимальная скорость шифрования наблюдается при разбиении шифруемого набора данных на одну точку. Однако, тут можно столкнуться с ограниченным размером эллиптического поля. Координаты X и Y точки не должны выходить за пределы поля, следовательно, стратегия представления всего набора данных в виде одной точки будет неприменима при шифровании больших объемов информации. Таким образом, оптимальной стратегией разбиения набора данных на блоки будет выделение минимального числа точек, координаты которых не выходят за пределы поля эллиптической группы (т.е. меньше модуля данной группы).

После оптимизации алгоритмов были проведены исследования времени выполнения операций над точками эллиптической кривой в зависимости от размера эллиптической группы. В качестве кривых для анализа были выбраны рекомендованные NIST (Национальным институтом стандартов и технологий) кривые P-192, P-224, P-256, P-384, P-521 (число в названии обозначает размер эллиптического поля в битах). Результаты исследования представлены на графике рисунка 2.

Как видно из результатов исследований, времена выполнения операций сложения точек и удвоения точки растут медленнее всего с увеличением размера поля и увеличиваются для кривой P-521 по сравнению с кривой P-192 примерно в 3 раза. Сложность умножения точки на число растет быстрее и именно ее вклад в кодирование точки максимален, что подтверждается схожей формой этих графиков. Сложность умножения точки на число и кодирования точки для кривой P-521 приблизительно в 9 раз выше, чем для кривой P-192.

Сложность шифрования строки растет медленнее сложности кодирования точки. Это объясняется тем, что оптимальной стратегией разбиения шифруемого блока данных на точки является выделение минимального

числа точек, размеры которых максимальны и при этом не выходят на пределы эллиптического поля, т. е. для большего размера эллиптического поля можно выделить меньшее количество точек, потому для шифрования строки такого же размера понадобится меньшее число операций кодирования точки.

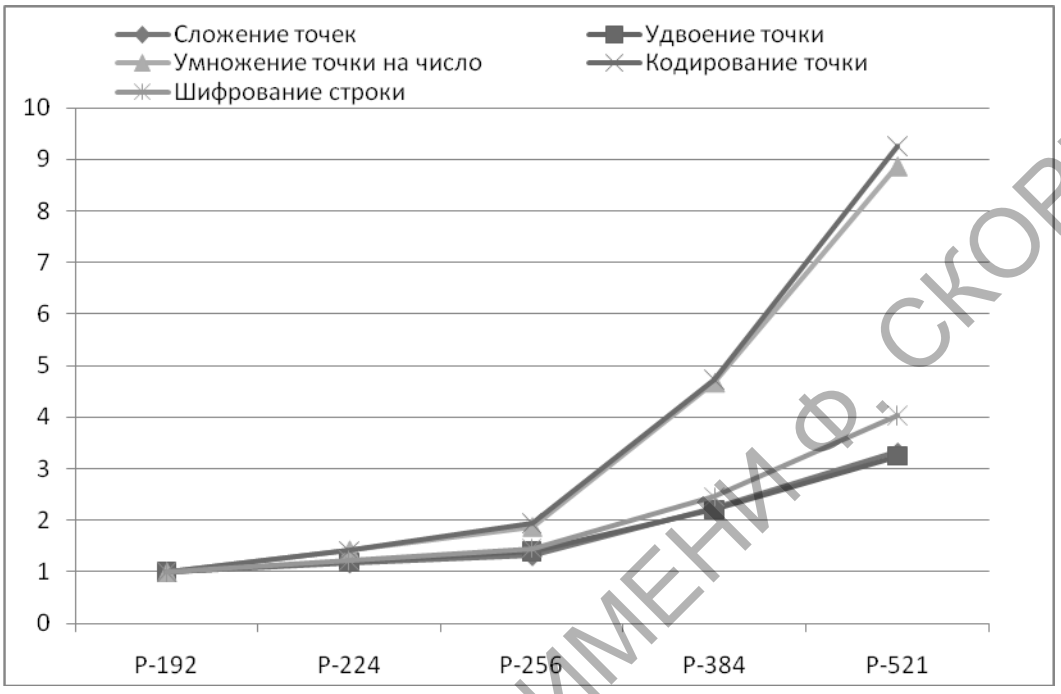

Рисунок 2 – Время выполнения основных криптографических операций

Были рассмотрены основные преимущества криптосистем на базе эллиптических кривых. Выделены и оптимизированы основные алгоритмы, требующие максимального быстродействия для эффективной работы криптосистемы. Исследованы зависимости времени шифрования от алгоритма разбиения набора шифруемых данных на блоки и времени выполнения основных операций над точками эллиптической группы от размера эллиптической группы.

Литература

1. Применко, Э. А. Эллиптические кривые: новый этап развития современной криптографии / Э. А. Применко, А.Ю. Винокуров // Каталог «Пожарная безопасность». – 2004 – с.164-168.

2. Hankerson, D. Guide to elliptic curve cryptography / D. Hankerson, A. Menezes, S. Vanstone – Springer-Verlag New York, Inc, 2004 – P. 188–196.