КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ НА БАЗЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

А.В. Короткевич
Кафедра программного обеспечения информационных технологий,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: ankor91@mail.ru

Рассмотрены основные преимущества криптосистем на базе эллиптических кривых и обоснован их выбор для обеспечения защиты данных. Выделены и оптимизированы основные алгоритмы, требующие максимального быстродействия для эффективной работы криптосистемы. Исследована зависимость времени выполнения основных операций над точками эллиптической группы от размера эллиптической группы. Исследована зависимость времени шифрования от алгоритма разбиения набора шифруемых данных на блоки.

Введение

В современном обществе, в связи с повсеместным распространением информационных технологий и передачи информации на расстояния, безопасность передаваемой информации приобретает огромное значение. Такая безопасность обеспечивается различными криптографическими методами, одним из самых перспективных среди которых является использование криптосистем, основанных на свойствах эллиптических кривых.

В настоящее время в криптографии принято выделять два крупных направления: классическую (одноключевую, симметричную) и современную (двухключевую, асимметричную) криптографию. Основным преимуществом симметричных криптосистем (к примеру, AES, DES, Blowfish) является высокое быстродействие и высокая стойкость при относительно небольшом размере ключей. Однако, использование методов ассиметричной криптографии порождает вторичные проблемы защиты, такие как потребность в защищенном канале связи для передачи секретных ключей участникам взаимодействия. Это означает, что лишь симметричных методов недостаточно в ситуациях, когда отсутствует взаимное доверие сторон.

Ассиметричная криптография возникла относительно недавно — в середине семидесятых годов прошлого века. Она ориентирована на решение иных, более современных задач, перед которыми симметричная криптография оказалась бессильной. Так, протоколы асимметричной криптографии незаменимы в ситуациях отсутствия взаимного доверия между сторонами. Каноническими задачами ассиметричной криптографии являются двухключевое шифрование, распределение секретных ключей по несекретным каналам связи и подпись цифровых документов [1].

Стойкость алгоритмов ассиметричной криптографии базируется на вычислительной невозможности эффективного решения некоторых математических задач. Например, стойкость криптосистемы RSA базируется на сложности задачи факторизации больших чисел, а стойкость современных схем электронной цифровой подписи, большинство из которых являются вариациями обобщенной схемы Эль-Гамаля, – на сложности задачи логарифмирования в конечных полях.

I. Преимущества эллиптических криптосистем

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. Этот факт в совокупности с быстрым устареванием схем ассиметричной криптографии привел к повсеместному переходу на эллиптические кривые в наиболее важных областях применения. Так, старые стандарты электронной цифровой подписи РФ и США, просуществовав около 7 лет (с 1994 по 2001 гг.), практически одновременно были заменены новыми, реализующими прежние криптографические схемы на эллиптических кривых, что позволило существенно увеличить стойкость и сократить размер блоков данных [1]. Старый российский стандарт оперировал 1024-битовыми блоками данных, новый оперирует 256-битовыми. При этом, по оценкам специалистов, трудоемкость взлома нового стандарта выше, чем старого. По указанной причине в настоящее время происходит массовый перевод асимметричных крипто-

систем, основанных на сложности задачи логарифмирования в дискретных полях, на эллиптические кривые. Потому использование эллиптических кривых является хорошим решением при выборе способа защиты важных данных.

II. Производительность алгоритмов

Основным недостатком криптосистем, основанных на эллиптических кривых, 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]. Ускорение каждого из указанных алгоритмов приводит к значительному росту производительности всей системы в целом.

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 (см. рис. 1).

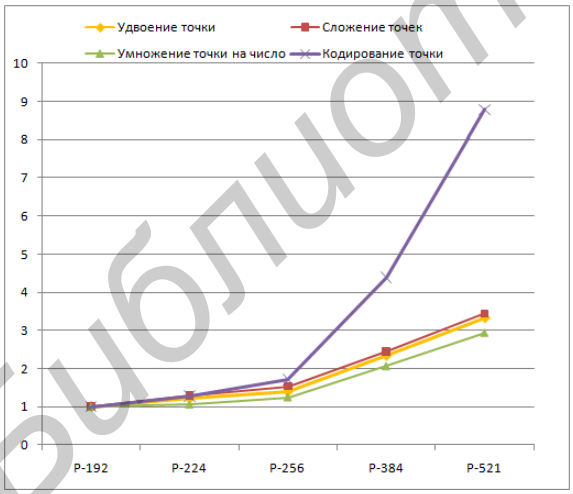

Рис. 1 – Время выполнения операций над точками кривой

Из графика можно заключить, что сложности операций удвоения точки, сложения точек и умножения точки эллиптической кривой на число растут приблизительно в одном темпе с увеличением размера поля, а скорость роста сложности кодирования точки значительно выше. Соответственно, при выборе кривой для шифрования необходимо соблюдать баланс между надежностью криптосистемы и скоростью выполнения операции шифрования. Однако, стоит отметить, что даже минимальной из упомянутых кривых достаточно для обеспечения чрезвычайно высокого уровня безопасности данных.

III. Оптимальный размер шифруемого блока

Схема Менезеса-Ванстоуна предоставляет возможность шифрования точки эллиптической кривой. Т.е. 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 данных представлены на графике (см. рис. 2).

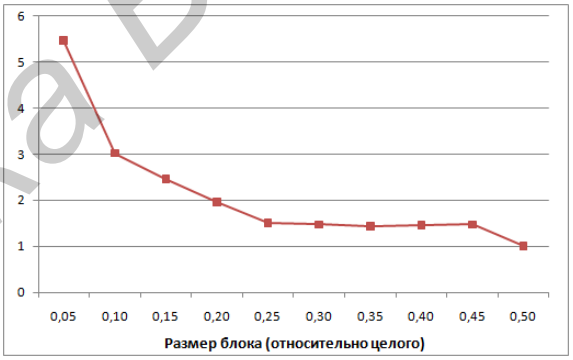

Рис. 2 – Время шифрования в зависимости от размера блока

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).

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.