КРИПТОГРАФИЧЕСКАЯ ПЕРЕДАЧА ИНФОРМАЦИИ НА БАЗЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

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

Короткевич А. В.

Ярмолик В. Н. – д-р. техн. наук, профессор

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.

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 ЭЦП, большинство из которых являются вариациями обобщенной схемы Эль-Гамаля, – на сложности задачи логарифмирования в конечных полях.

Практически любая ассиметричная криптосистема может быть переложена на эллиптические кривые, однако не для всех схем это даёт выигрыш в стойкости. Например, для системы RSA и родственных ей систем, основанных на сложности задачи факторизации, это не усиливает схему. В то же время для схем, основанных на сложности задачи логарифмирования в дискретных полях, переход на эллиптические кривые позволяет существенно увеличить стойкость. Обусловлено это тем, что при надлежащем выборе параметров кривой задача логарифмирования в группе точек кривой существенно сложнее задачи логарифмирования в мультипликативной группе исходного поля. Этот факт в сочетании с быстрой "инфляцией" схем ассиметричной криптографии привел к повсеместному переходу на эллиптические кривые в "чувствительных" областях применения. Так, старые стандарты ЭЦП 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. 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 криптосистем, основанных на сложности задачи логарифмирования в дискретных полях, на эллиптические кривые. Потому эллиптические кривые являются хорошим решением при выборе способа защиты передаваемых данных.

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. Ускорение каждого из указанных алгоритмов приводит к значительному росту производительности всей системы в целом.

Таким образом, были рассмотрены основные преимущества криптосистем на базе эллиптических кривых и обоснован их выбор для защиты передаваемых данных, а также выделены и оптимизированы основные алгоритмы, требующие оптимальной реализации для эффективного решения поставленной задачи.

Список использованных источников:

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., Menezes A., Vanstone S. Guide to elliptic curve cryptography – Springer-Verlag New York, Inc, 2004.