МЕТОД КРИПТОГРАФИЧЕСКОЙ ПЕРЕДАЧИ 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

Выделены основные преимущества и недостатки ассиметричных криптосистем. Изучен метод обмена криптографическими ключами в криптосистемах на основе свойств эллиптических кривых. Исследован метод передачи информации с помощью криптосистемы на базе эллиптических кривых, выделены его недостатки. Изучен метод Менезеса-Ванстоуна для передачи криптографической информации на базе эллиптических кривых, выделены его недостатки. Предложена модификация метода Менезеса-Ванстоуна для удовлетворения целей исследования, выделены основные направления для дальнейшего анализа.

Введение

Ассиметричные криптосистемы имеют свои особенности по сравнению с симметричными. Так, они обладают большей вычислительной сложностью и, соответственно, меньшей скоростью работы. Однако, для задачи распределения криптографических ключей одних симметричных криптосистем оказывается недостаточно и данная задача эффективно решается при помощи ассиметричных алгоритмов. Одними из самых современных и востребованных среди современных ассиметричных криптосистем являются криптосистемы, основанные на свойствах эллиптических кривых. Именно о таких криптосистемах и решении с их помощью основных задач, поставленных перед ассиметричной криптографией, и пойдет речь далее.

I. Обмен криптографическими ключами

Прежде всего, необходимо определиться с общими параметрами криптосистемы и пользовательскими открытым и секретным ключами. До начала обменом зашифрованными сообщениями собеседники должны узнать открытые ключи друг друга. Обмен ключами с использованием эллиптических кривых может быть выполнен следующим образом. Сначала выбирается простое число p и параметры a и b для уравнения эллиптической кривой. Это задает множество точек $E_p(a,b)$. Затем в $E_p(a,b)$ выбирается генерирующая точка $G = (x_1, y_1)$. При выборе G важно, чтобы наименьшее значение n, при котором $n \cdot G = 0$, оказалось очень большим простым числом. Параметры $E_p(a,b)$ и G криптосистемы являются параметрами, известными всем участникам.

Обмен ключами между пользователями A и B производится по следующей схеме [1]:

1. Участник A выбирает целое число n_A, меньшее n. Это число является закрытым ключом участника A. Затем участник A вычисляет открытый ключ $P_A = n_A \cdot G$, который представляет собой некоторую точку на $E_p(a,b)$.
2. Точно так же участник B выбирает закрытый ключ n_B и вычисляет открытый ключ P_B.
3. Участники обмениваются открытыми ключами, после чего вычисляют общий секретный ключ K. Участник A вычисляет $K = n_A \cdot P_B$. Участник B вычисляет $K = n_B \cdot P_A$.

Следует заметить, что общий секретный ключ представляет собой пару чисел. Если данный ключ предполагается использовать в качестве сеансового ключа для алгоритма симметричного шифрования, то из этой пары необходимо создать одно значение.

II. Шифрование данных

Существуют различные методы шифрования данных на основе эллиптической криптосистемы. Рассмотрим самый простой подход к шифрованию/дешифрованию с использованием эллиптических кривых. Задача состоит в том, чтобы зашифровать сообщение M, которое может быть представлено в виде точки на эллиптической кривой $P_m(x,y)$.

Как и в случае обмена ключом, в системе шифрования/дешифрования в качестве параметров рассматривается эллиптическая кривая $E_p(a,b)$ и точка G на ней. Участник B выбирает закрытый ключ n_B и вычисляет открытый ключ $P_B = n_B \cdot G$. Чтобы зашифровать сообщение P_m используется открытый ключ получателя B – P_B. Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение $C_m = (k \cdot G, P_m + k \cdot P_B)$, являющееся точкой на эллиптической кривой [2].

Чтобы дешифровать сообщение, участник B умножает первую координату точки на свой закрытый ключ и вычитает результат из второй координаты: $P_m + k \cdot P_B - n_B \cdot (k \cdot G) = P_m + k \cdot (n_B \cdot G) - n_B \cdot (k \cdot G) = P_m$.

Участник А зашифровал сообщение P_m добавлением к нему $k \cdot P_B$. Никто не знает значения k, поэтому, хотя P_B и является открытым ключом, никто не знает $k \cdot P_B$. Злоумышленнику для восстановления сообщения придется вычислить k, зная G и $k \cdot G$. Сделать это будет нелегко.

Получатель также не знает k, но ему в качестве подсказки посылается $k \cdot G$. Умножив $k \cdot G$ на свой закрытый ключ, получатель получит значение, которое было добавлено отправителем к незашифрованному сообщению. Тем самым получатель, не зная k, но имея свой закрытый ключ, может восстановить незашифрованное сообщение [3].

Однако, такой метод шифрования не является недостаточно удобным, т.к. исходное сообщение должно быть представлено в виде точек эллиптической группы, что не всегда бывает возможным. Решением данной проблемы может быть использование криптосистемы Менезеса-Ванстоуна, которая является вариацией схемы Эль-Гамаля.

III. Метод Менезеса-Ванстоуна

Криптосистема Менезеса-Ванстоуна предполагает согласование взаимодействующими сторонами параметров эллиптической кривой a, b и p, что задает множество точек эллиптической группы $E_p(a, b)$, а также генерирующей точки G, имеющей порядок, являющийся очень большим простым числом. После этого участники А и В выбирают случайные целые числа n_A и n_B, меньшие периода точки G, и вычисляют свои открытые ключи $P_A = n_A \cdot G$ и $P_B = n_B \cdot G$ соответственно. Теперь, для посылки сообщения участнику В, участник А узнает открытый ключ P_B и выполняются следующие действия [4]:

1. Участник А выбирает целое число k, меньшее n, где n – порядок генерирующей точки G.
2. Вычисляется $k \cdot P_B = (x_2, y_2)$.
3. Вычисляется $C_0 = k \cdot G$.
4. Вычисляются $C_1 = x_1 x_2 (mod\ p)$ и $C_2 = y_1 y_2 (mod\ p)$, где x_1 и y_1 – произвольные целые числа, которые и являются исходным сообщением.
5. Участник А высылает участнику В зашифрованное сообщение в виде набора $C = (C_0,\ C_1,\ C_2)$.

Участник В, получив такое зашифрованное сообщение, должен выполнить следующую последовательность действий для вычисления исходного сообщения:

1. Вычисляется $n_B \cdot C_0 = k \cdot P_B = (x_2, y_2)$.
2. Составляются уравнения $C_1 = x_1 x_2 (mod\ p)$ и $C_2 = y_1 y_2 (mod\ p)$, в которых неизвестны x_1 и y_1, после решения которых участник В получит исходное сообщение.

IV. Модифицированный метод Менезеса-Ванстоуна

Таким образом, криптосистема Менезеса-Ванстоуна позволяет безопасно передавать сообщения, которые можно представить в виде пары чисел. Однако, размер реальных сообщений может быть настолько велик, что представление сообщения в виде пары чисел будет невозможным, т.к. эти числа будут превышать величину модуля эллиптической группы.

Потому для решения проблемы передачи криптографической информации на базе эллиптических кривых можно предложить модификацию метода Менезеса-Ванстоуна. Пусть оптимальный размер координаты передаваемой точки равен l байт. Тогда исходное сообщение будет представлено в виде набора точек, где количество байт в каждой точке составляет $2l$. Очевидно, что размер исходного сообщения скорее всего не будет кратен $2l$, потому будем дополнять сообщение случайными байтами до необходимого размера, предварительно запомнив изначальный размер сообщения. Случайность добавляемых байтов необходима для лучшей защиты от потенциальных злоумышленников. При дешифровании сообщения понадобится знать его реальную длину в байтах, потому она должна быть включена в набор передаваемых данных (например, в качестве первых байт первой точки). При дешифровании первым делом вычитывается исходная длина сообщения, а затем полное сообщение восстанавливается путем отбрасывания лишних случайных байт.

В описанном модифицированном методе переменным параметром является размер точки в байтах l. Нахождение оптимального l для наибольшей производительности криптографической системы является одной из важнейших задач исследования, т.к. именно высокое время выполнения является слабостью ассиметричных криптографических алгоритмов. Для решения данной задачи необходимо произвести анализ производительности метода в зависимости от различных допустимых значений l (от 1 до значения, при котором максимальный размер точки не будет превышать величины модуля эллиптической группы).

1. Мао, В. Современная криптография: теория и практика / В. Мао – М. : «Вильямс», 2005. – 678 с.
2. Коблиц, Н. Введение в эллиптические кривые и модулярные формы / Н. Коблиц. – М. : «Мир», 1998. – 313 с.
3. Henk, C.A. van Tilborg Encyclopedia of Cryptography and Security / C.A. van Tilborg Henk. – Springer, 2007. – 784 с.
4. Hankerson, D. Guide to elliptic curve cryptography / D. Hankerson, A. Menezes, S. Vanstone – Springer-Verlag, New York, Inc, 2004 – P. 188-196.