Баутин С.П., Медведев Н.В., Титов С.С.

О ПРОБЛЕМЕ РАЗДЕЛЕНИЯ СЕКРЕТА НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Уральский государственный университет путей сообщения

Постановка задачи построения пороговой схемы разделения секрета на произвольных кривых может быть произведена на основе теории интерполяции путем переноса на дискретные модели методов непрерывных моделей, математического анализа и дифференциальных уравнений. В данной работе представлен обзор задач такого направления исследований, придающий единство подходам, которые могут быть применены и для локально компактных полей, таких как поле комплексных чисел C, поле вещественных чисел R, и для бесконечных нигде не плотных (поле рациональных чисел Q), и для конечных полей с целью приложения к математическим методам защиты информации.

В случае многочленов над полем данное построение имеет вид интерполяционного многочлена Лагранжа, что и используется в пороговой схеме разделения секрета Шамира.

Для произвольного многообразия такая постановка предполагает решение ряда специфических задач: будет ли такая схема совершенной? будет ли такая схема идеальной? какие условия существования такой схемы? какие параметры такой схемы? каковы эффективные компьютерные реализации таких схем? в каких ситуациях такие схемы предпочтительнее общепринятых?

В частности, если параметры такой схемы превосходят параметры схемы Шамира, то такие схемы улучшают разделение секрета.

При рассмотрении в качестве многообразия M эллиптической кривой над данным полем возникают специфические и своеобразные конкретные особенности, если в качестве семейства S берется класс многочленов на данной эллиптической кривой, так как: в этом классе отсутствуют многочлены первой степени; нет разложения на множители первой степени; количество корней многочлена совпадает с его степенью только для алгебраически замкнутого поля; отсутствует явная интерполяционная формула.

Однако при всей сложности этой задачи ясна и ее актуальность, поскольку ее решение позволит повысить стойкость схемы разделения секрета не только за счет мощности используемого поля, но и за счет хороших криптографических качеств эллиптических кривых.

При этом могут быть установлены новые связи между различными разделами научной деятельности, связанной с разработкой математических методов защиты информации.

Эллиптические кривые обеспечивают необходимое основание, на котором могут быть построены криптологические алгоритмы. Вместо работы с остатками по простому модулю p мы имеем дело с геометрическими отношениями. Преимуществом эллиптических кривых является то, что в сложных геометрических вычислениях существует более трудный (для раскрытия) аналог проблемы дискретного логарифма (или, по крайней мере, который в данный момент пока еще не так хо-

рошо понятен). Для этой задачи требуются более короткие простые числа p. С более короткими простыми числами криптографические алгоритмы будут работать значительно быстрее.

Для построения схемы разделения секрета Шамира «четыре из семи» рассмотрен вариант пересечения эллиптической кривой с гиперболой. Причем эллиптическая кривая должна быть не монотонной, то есть существуют различные точки с одинаковой ординатой.

Как известно, гиперболу можно однозначно построить по трем точкам, поэтому чтобы эти точки были гарантированно рациональными, мы берем на эллиптической кривой некоторую рациональную точку и путем сложения получаем другие рациональные точки.

Исходя из выбранных точек на эллиптической кривой, можно подсчитать дискриминант и сказать, будут ли остальные две точки рациональными.

Имеется система уравнений, которая описывает разделение секрета:

$$\begin{cases} y^2 = x^3 + ax + b; \\ y = \dfrac{\alpha x + \beta}{x + \delta}, x + \delta \neq 0. \end{cases}$$

Если на кривой есть точки с одинаковой ординатой, то существует $f(P)$, обращающаяся в нуль в четырех точках кривой, то есть на этом пути схему разделения секрета Шамира улучшить нельзя.

Для возможности усовершенствования схемы разделения секрета была выдвинута идея использовать вместо декартовой системы координат эллиптическую кривую.

Литература

1. Введение в криптографию / Под общей ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.

2. Болотов А.А. «Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых»/ А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – Издательство: КомКнига, 2006.

3. «Алгоритмические основы эллиптической криптографии». Учебное пособие / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: Изд-во МЭИ.

4. Н.Коблиц, Введение в эллиптические кривые и модулярные формы. – М.: «Мир» 1988.

5. Кнэпп, Энтони. Эллиптические кривые / Э. Кнэпп; Ф. Ю. Попеленский (пер. с англ.); Ю. П. Соловьев (ред.). — М.: Факториал Пресс, 2004.

6. Журнал "Открытые системы", #07-08, 2002 год Цифровая подпись. Эллиптические кривые.