Мелитопольская школа прикладной геометрии

Мелитопольский государственный педагогический университет

им. Б. Хмельницкого

ГЕОМЕТРИЧЕСКОЕ МОДЕЛИРОВАНИЕ ОБЪЕКТА ШИФРОВАНИЯ НА ОСНОВЕ ТОЧЕЧНОГО ИСЧИСЛЕНИЯ БАЛЮБЫ - НАЙДЫША

Докладчик: В.В. Юрченко,

аспирант

Научный руководитель: И.Г. Балюба,

д.т.н., проф.

Мелитополь 2016

Недостатки использования эллиптических кривых в криптографии:

- Ограничение длины ключа при шифровании на основе кривой Вейерштрасса.
- Появление суперсингулярных кривых.
- Невысокая точность моделирования.
- Сложность последующей программной реализации.

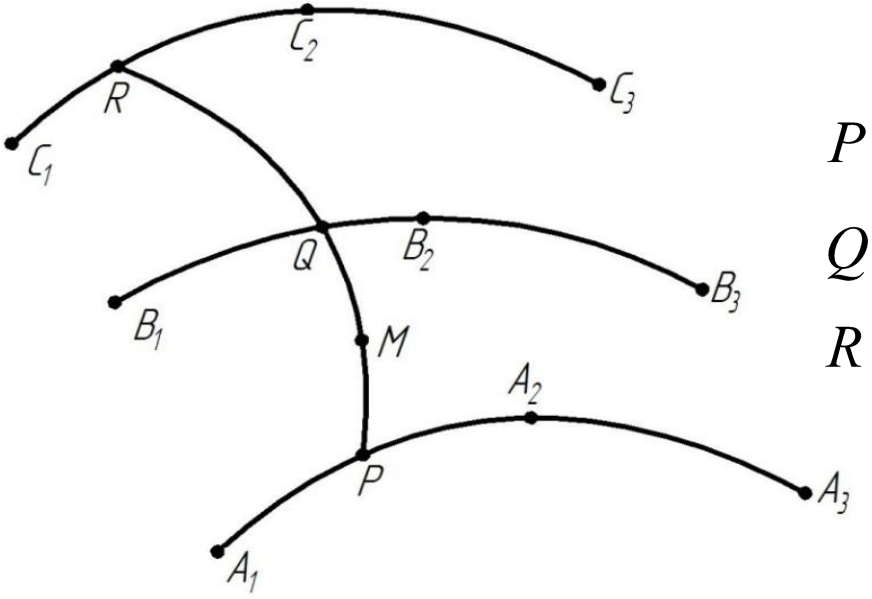
Шифрование с использованием поверхностей имеют следующие преимущества:

- Больший порядок модели
- Двухпараметрический подход моделирования стойкости ключа в комбинации "логин/пароль"
- Простота построения геометрической модели функции криптозащиты
- Эффективность программной реализации за счет использования особенностей БН-моделей

Преимуществами использования геометрических моделей, описаных в терминах БН-исчисления:

- Меньшая длина ключа в сравнении с «классической» асимметричной криптографией.
- Скорость работы алгоритмов шифрования и вычисления гораздо выше, чем у классических.
- Малая длина ключа и высокая скорость работы алгоритмов позволяют использовать модели в смарт-картах и других устройствах с ограниченными вычислительными ресурсами.

Построение поверхности способом «Лупа»



$$P = A_1\bar{u}(1-2u) + 4A_2u\bar{u} + A_3u(2u-1)$$

$$Q = B_1\bar{u}(1-2u) + 4B_2u\bar{u} + B_3u(2u-1)$$

$$R = C_1\bar{u}(1-2u) + 4C_2u\bar{u} + C_3u(2u-1)$$

$$\begin{aligned} M = {} & [A_1\bar{u}(1-2u) + 4A_2u\bar{u} + A_3u(2u-1)]\bar{v}(1-2v) + \\ & + 4[B_1\bar{u}(1-2u) + 4B_2u\bar{u} + B_3u(2u-1)]v\bar{v} + \\ & + [C_1\bar{u}(1-2u) + 4C_2u\bar{u} + C_3u(2u-1)]v(2v-1). \end{aligned}$$

Выводы:

В результате анализа выявлены преимущества и недостатки существующих способов защиты информации с помощью эллиптических кривых. Было предложено использовать геометрические объекты описанных в терминах БН - исчисления; Для шифрования в качестве примера было рассмотрено шифрование способом "Лупа" что нам позволило значительно упростить программную реализацию, увеличить скорость при сохранении точности вычисления и криптостойкости.

СПАСИБО ЗА ВНИМАНИЕ