ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ВЫСШИХ ПОРЯДКОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Авторы: Попова Е.А., Яковлев А.В., Королькова И.К.

ВВЕДЕНИЕ

В большинстве современных продуктов и стандартов криптографии применяются методы с открытым ключом, основанные на проблеме факторизации больших чисел (RSA) и дискретного логарифмирования (Эль-Гамаль). Однако для их надежной защищенности число битов ключа в последние годы резко возросло, что обусловило рост нагрузки на вычислительные системы. Для удобства использования, программная и аппаратная реализация криптографических методов должны, в первую очередь, обеспечивать достаточный уровень криптографической стойкости и при этом высокую скорость преобразований.

Для улучшения свойств криптографических алгоритмов начали применяться эллиптические кривые высших порядков. Поэтому в данной работе рассматривается возможность расширения использования эллиптических кривых высших порядков в криптографических протоколах, с целью обеспечения надежной защиты при меньших длинах ключа.

Криптографические методы защиты информации

Надлежащий уровень защиты данных, передаваемых через открытые каналы связи, может быть обеспечен с помощью криптографических методов. Криптографические методы защиты позволяют решать следующие задачи:

- закрытие данных, хранимых в АС или передаваемых по каналам связи
- контроль целостности и аутентичности данных, передаваемых по каналам связи

Основным достоинством криптографических методов защиты информации является то, что они обеспечивают **гарантированную стойкость защиты**.

Наиболее известные криптосистемы с открытым ключом:

- криптосистема *RSA* (шифрование и электронная подпись);
- криптосистема Эль-Гамаля (трудность вычисления дискретных логарифмов в конечном поле в сравнении с лёгкостью возведения в степень в том же самом поле);
- криптосистема, основанная на свойствах эллиптических кривых (преимущества применения в беспроводных коммуникациях – высокое быстродействие и небольшая длина ключа);
- активно исследуются вопросы реализации криптопреобразований на эллиптических кривых высших порядков.

Применение кубических кривых в криптографических протоколах

В общем случае кубические уравнения для эллиптических кривых имеют вид:

$$y^2 + axy + by = x^3 + cx^2 + dx + e,$$

где a, b, c, d и e являются действительными числами, удовлетворяющими некоторым простым условиям. Определение эллиптической кривой включает также некий элемент, обозначаемый ***O*** и называемый «**несобственным элементом**» («бесконечным элементом», «нулевым элементом», «точкой в бесконечности»). Такие уравнения называются кубическими, или уравнениями эллиптических кривых третьего порядка, поскольку в них наивысший показатель степени равен 3.

Графическое представление кубической кривой в пространстве

То есть внедрение кубической кривой в криптографические протоколы позволяет выбирать эллиптическую кривую из множества возможных, используя параметр Z как уровень для выбора секущей плоскости.

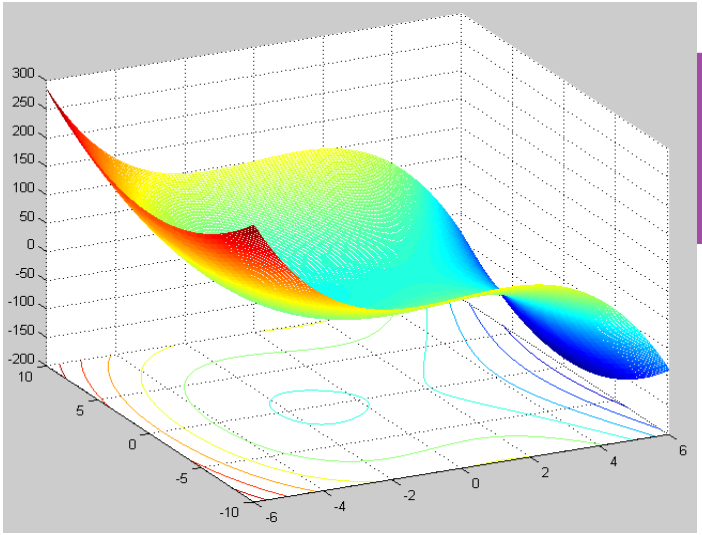
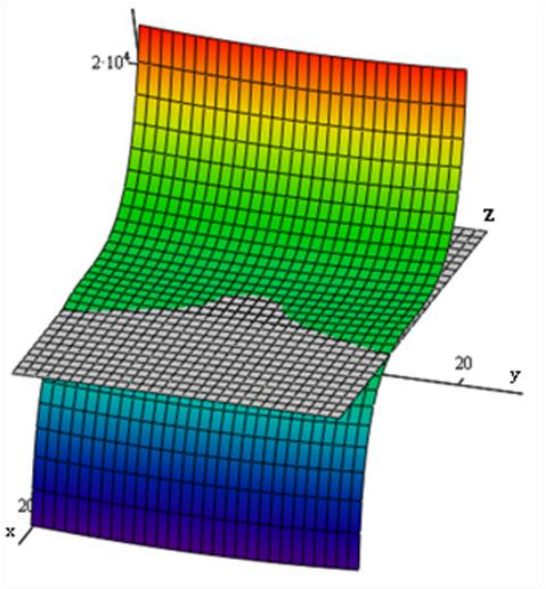
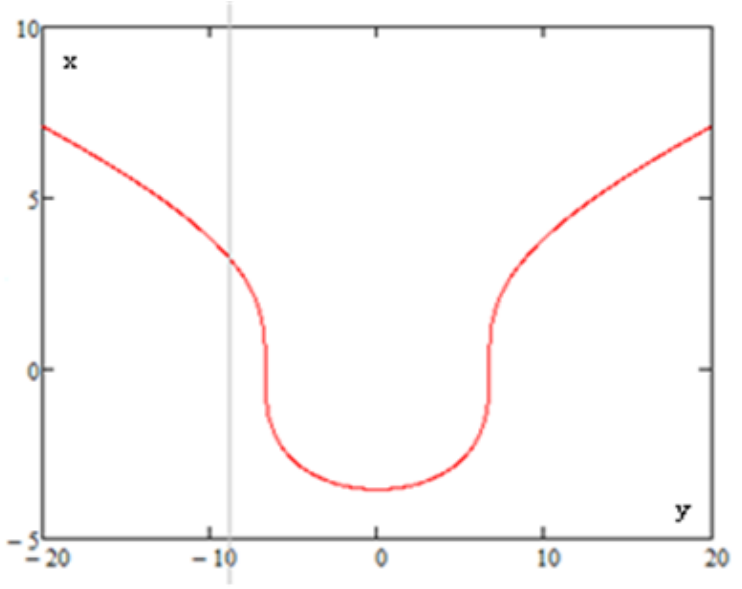


Схема обмена ключами Диффи-Хеллмана, при добавлении в нее кубической кривой в пространстве и уровня секущей плоскости *Z* будет выглядеть так: предположим, что в протокол вшита кубическая кривая $y^2 = x^3 + ax + b$, тогда алгоритм в этом случае будет выглядеть следующим образом:

1. Выбирается уровень *Z*, открытый параметр.
2. Вычисляется эллиптическая кривая .
3. На получившейся эллиптической кривой выбирается генерирующая точка *G*, такая что, при n-кратном сложении точки *G*, где n очень большое простое число, получается *O* – точка на бесконечности.

Кубическая кривая и секущая плоскость в пространстве (справа), эллиптическая кривая на плоскости (слева)





Абонент А:

1. Выбирает целое число n_A, меньшее n. Это число будет личным ключом участника A. Затем участник A генерирует открытый ключ $P_A = n_A G$. Открытый ключ представляет собой некоторую точку из группы точек на эллиптической кривой. Для вычисления $P_A = n_A G$ пользуются правилом сложения точек эллиптической кривой:

$$P = (x_1, y_1); Q = (x_2, y_2)$$

$$x_3 = \lambda^2 - x_1 - x_2;$$
$$y_3 = \lambda (x_1 - x_3) - y_1;$$

где $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, если P ≠ Q или $\lambda = \frac{(3x + a)}{2y}$, если P = Q.

2. Полученный открытый ключ P_A отправляется абоненту В.

Абонент В:

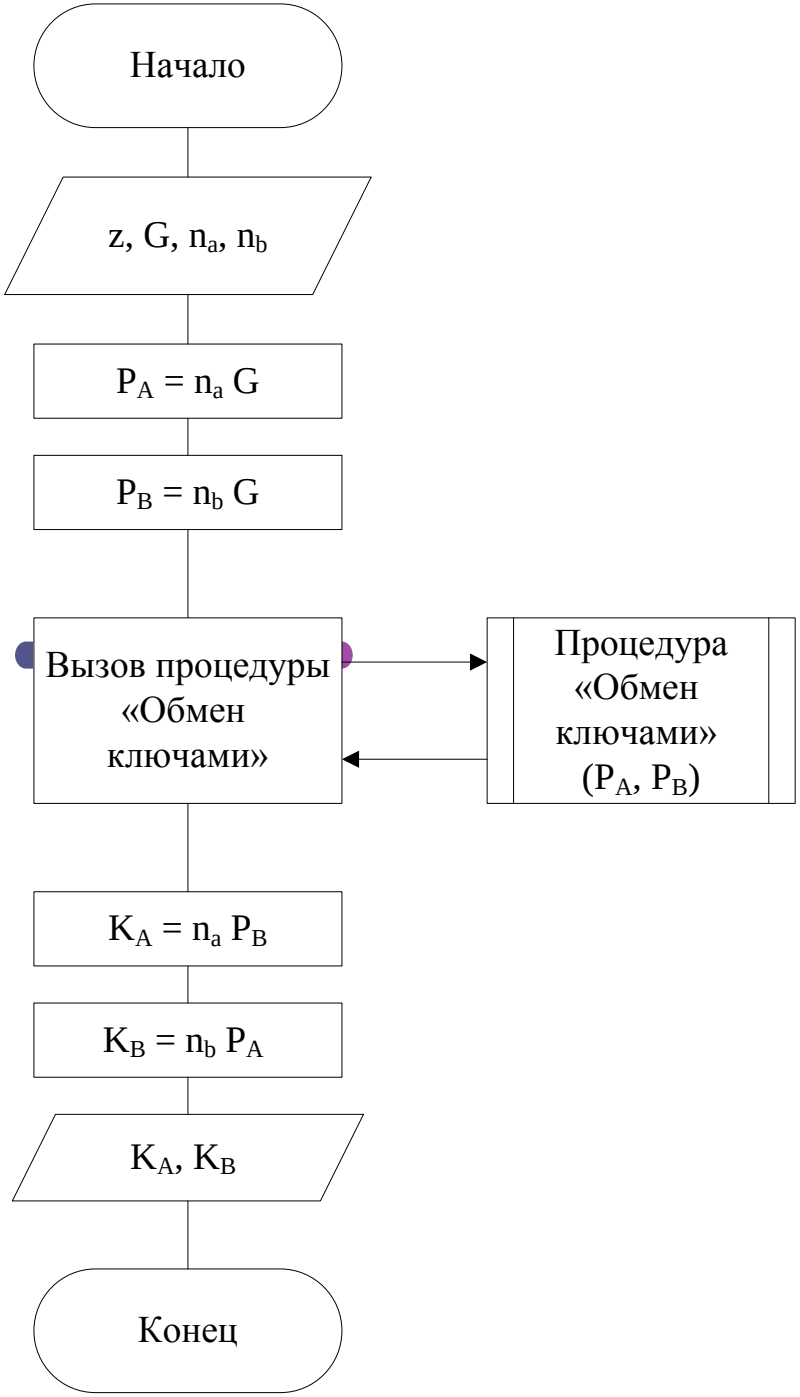
3. Выбирает целое число n_B, меньшее n. Это число будет личным ключом участника В. Затем участник В генерирует открытый ключ $P_B = n_B G$. Открытый ключ представляет собой некоторую точку из группы точек на эллиптической кривой.

4. Полученный открытый ключ P_B отправляется абоненту А.

5. Абонент А вычисляет $K_A = n_A P_B$, абонент В $K_B = n_B P_A$

6. Два последних выражения дают один и тот же результат, поскольку:

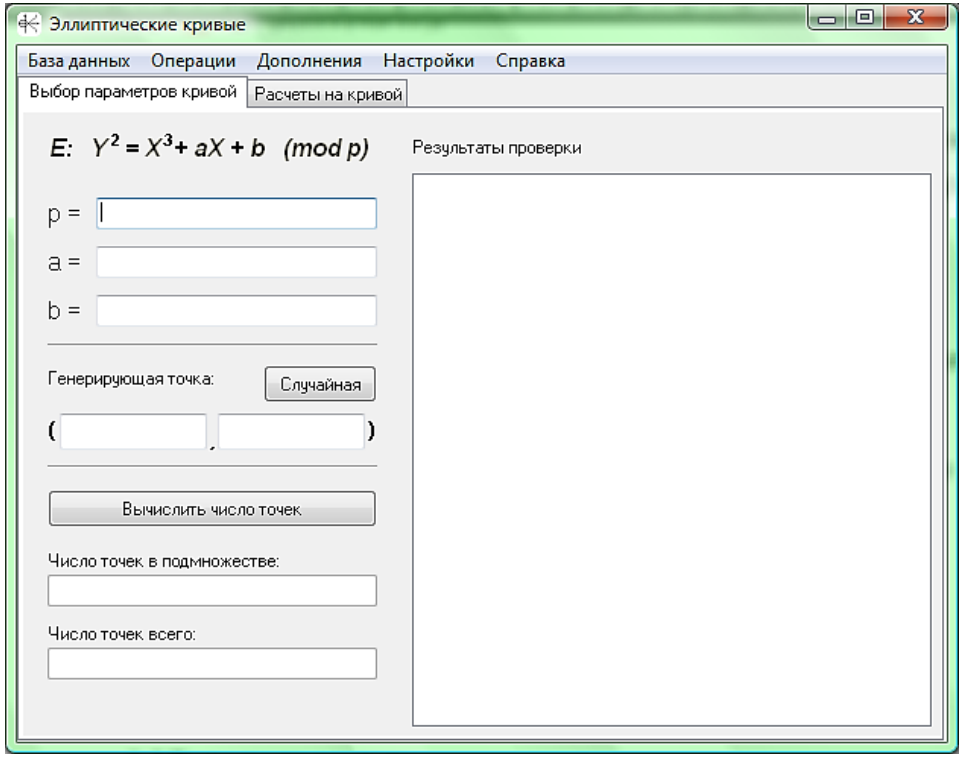
$$n_A P_B = n_A n_B G = n_B n_A G = n_B P_A$$



Структурная схема алгоритма Диффи-Хеллмана с использованием кубической кривой

Реализация схемы обмена ключами с использованием кубической кривой

Приложение «**Эллиптические кривые 1.1**» разработано специально для работы с эллиптическими кривыми.

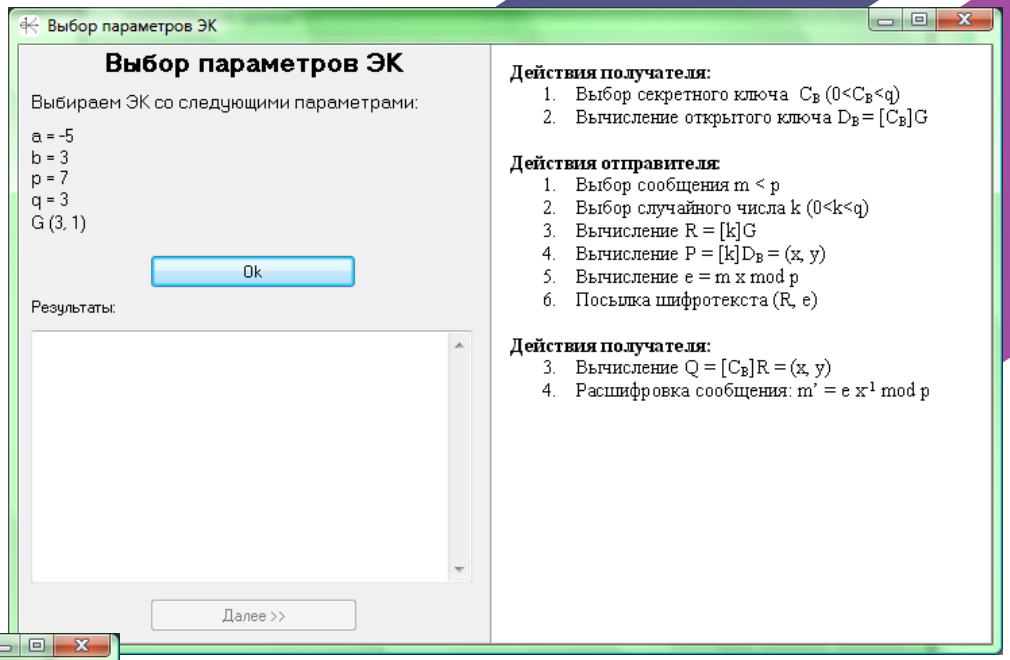


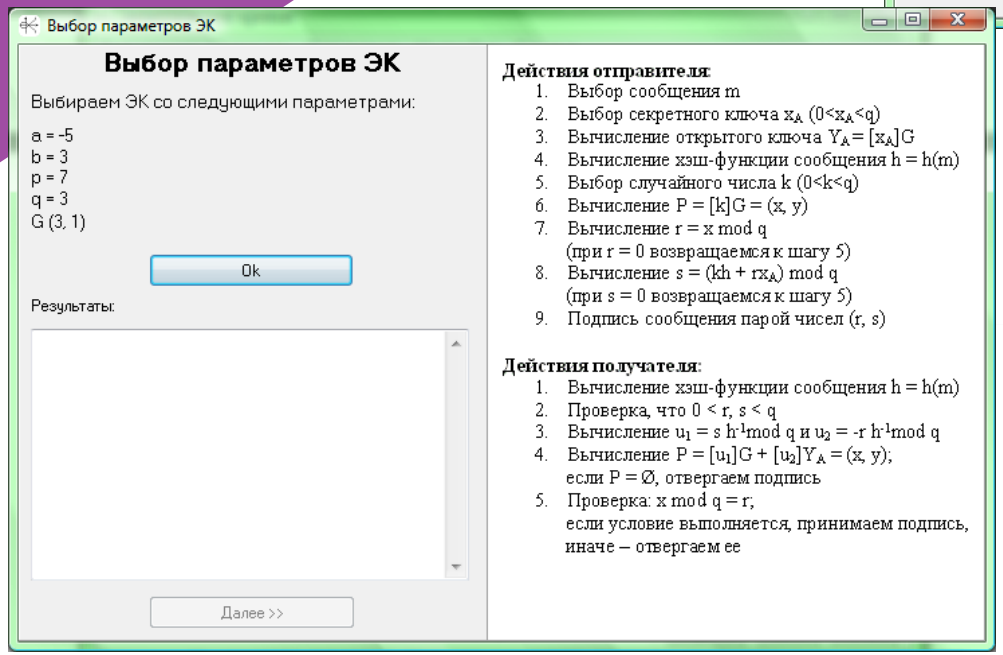
Приложение позволяет работать с эллиптическими кривыми, как из собственной БД, так и введенными вручную. Позволяет случайным образом выбирать генерирующую точку, либо проверять, принадлежит ли заданная вручную точка эллиптической кривой и многое другое.

Еще одной функциональной возможностью данного приложения является возможность подсчета числа точек в подмножестве и общего числа точек.

Помимо всего перечисленного, приложение позволяет:

проиллюстрировать работу алгоритма шифрования Эль-Гамаля

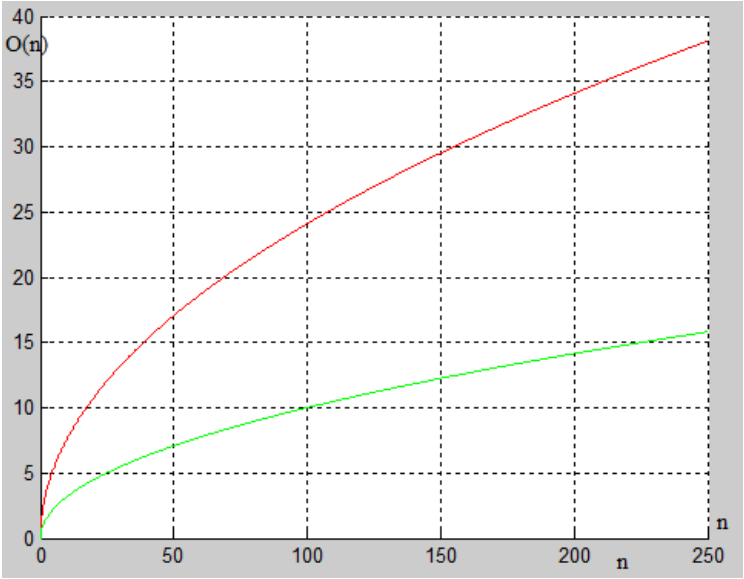




проиллюстрировать работу алгоритма генерации и проверки ЭП

Т.к. в ПО применяются эллиптические кривые высших порядков, то стоит также отметить их значимость перед эллиптическими кривыми второго порядка.

Значимость будет демонстрироваться из сравнения сложности разных порядков эллиптических кривых. Для второго порядка сложность составляет $O(\sqrt{n})$ – алгоритм **Шанкса**, а для высшего порядка – $o\left(\ln^2(n)\left(\sqrt{\frac{\pi n}{2}}\right)\right)$ – алгоритм **Ховитца-Венкатесана**.



Сравнение сложностей алгоритмов на эллиптических кривых второго порядка (нижний график) и на эллиптических кривых высших порядков (верхний график)

Видно, что при одинаковых объемах входных данных, сложность алгоритмов на эллиптических кривых второго порядка меньше сложности алгоритмов на эллиптических кривых высших порядков, из чего можно сделать вывод, что криптосистемы на эллиптических кривых высших порядков обладают большей криптостойкостью, нежели криптосистемы на эллиптических кривых второго порядка.

Заключение

Рассмотрены криптографические методы защиты информации, применение кубических кривых в криптографических протоколах, а также представлено ПО, которое облегчает работу с эллиптическими кривыми, выполняет множество различных операций над точками эллиптической кривой, а также иллюстрирует процесс шифрования, генерации и проверки ЭП на основе схемы Эль-Гамаля с использованием эллиптических кривых.

Таким образом, асимметричные криптосистемы требуют использования более длинных ключей, нежели симметричные, для обеспечения того же уровня криптостойкости, а использование эллиптических кривых высших порядков позволяет обеспечивать необходимый уровень криптостойкости при меньших длинах ключа.