Применение эллиптических кривых высших порядков для защиты информации

Е.А. Попова, email: elena.popova2001@yandex.ru,
А.В. Яковлев, email: yava73@bk.ru,
И.К. Королькова, email: irishka-korolkova@mail.ru

ФГБОУ ВО «Тамбовский государственный технический университет»

Аннотация. *Реализация схемы обмена ключами с использованием кубической кривой для обеспечения необходимого уровня криптостойкости при меньших длинах ключа.*

Ключевые слова: *криптография, эллиптические кривые высшего порядка, криптостойкость.*

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. Стойкость криптографических преобразований напрямую зависит от размеров значений параметров криптосистемы, главным среди которых является длина секретного ключа. Поэтому развитие математической базы алгоритмов двухключевой криптографии направлено, главным образом, на поиск компромисса между показателями «скорость-стойкость» [1].

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.

1. 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, которую можно рассчитать и выразить в числовой форме (средним числом операций или количеством времени, необходимого для раскрытия зашифрованной информации или вычисления ключей) [2].

В связи с большой протяженностью каналов связи, невозможно обеспечить их полную физическую защиту от попыток снятия информации. Криптографические методы направлены на защиту передаваемых через эти каналы данных, что делает раскрытие конфиденциальной информации затруднительным процессом. Конфиденциальность и целостность данных, передаваемых по локальной сети или через Интернет, обеспечивается при помощи как симметричных (с секретным ключом), так и асимметричных алгоритмов (с открытым ключом).

Наиболее известный и широко распространенный протокол открытого распределения ключей был разработан У. Диффи и М. Хеллманом в 1976 г. Протокол позволяет двум пользователям обмениваться частным ключом по уязвимым каналам, не имея никаких предварительных договоренностей. Безопасность протокола Диффи-Хеллмана основана на трудности вычисления дискретного логарифма в конечном поле [3].

Наиболее известные криптосистемы с открытым ключом:

– криптосистема RSA (шифрование и электронная подпись);

– криптосистема Эль-Гамаля – EGCS (El Gamal Cryptosystem) (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 – ECCS (Elliptic Curve Cryptosystems) (преимущества применения в беспроводных коммуникациях – высокое быстродействие и небольшая длина ключа);

– активно исследуются вопросы реализации криптопреобразований на эллиптических кривых высших порядков.

Криптосистемы на основе эллиптических кривых высших порядков. Программная реализация современных стандартов электронной подписи, основанных на арифметике в группах точек эллиптических кривых над конечными полями, для обеспечения достаточной стойкости требует подключения специализированных библиотек длинных чисел. Их использование связано с дополнительными накладными расходами на поддержку внутренних механизмов представления и обработки длинных чисел в форматах библиотек длинной арифметики.

Возможность уйти от этой проблемы обеспечивается использованием кривых более высокого порядка. Точки таких эллиптических кривых не образуют группу, однако в качестве групповой структуры используется якобиан кривой – факторгруппа дивизоров нулевой степени по подгруппе главных дивизоров [4].

Таким образом, особенность криптопреобразований на эллиптических кривых высших порядков состоит в том, что для достижения достаточного уровня стойкости можно определить кривую над конечным полем с элементами меньшего размера, что делает их возможной альтернативой криптопреобразованиям на эллиптических кривых [5].

2. 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.

Изобразив эту кубическую кривую в пространстве (рис. 1), получим в любом сечении эллиптическую кривую. То есть внедрение кубической кривой в криптографические протоколы позволяет выбирать эллиптическую кривую из множества возможных, используя параметр Z как уровень для выбора секущей плоскости.

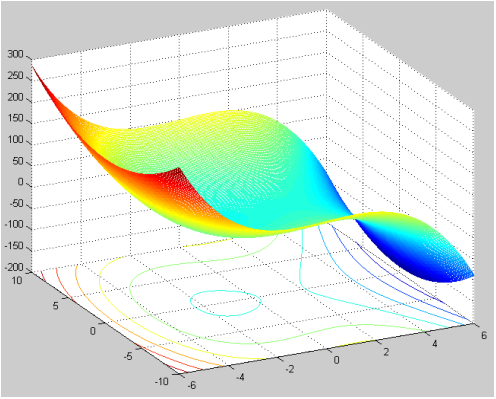

Рис. 1. Графическое представление кубической кривой в пространстве

В случае криптографии с использованием кубических кривых приходится иметь дело с редуцированной формой кривой, которая определяется над конечным полем. Кубическая кривая над конечным полем задаётся уравнением $y^2 = x^3 + ax + b$.

Для обеспечения надежной защиты кубическую кривую предлагается использовать как секретный параметр протокола, известный только его разработчикам.

Параметр Z, обозначающий уровень секущей плоскости, открытый, известный всем участникам. Разработчики могут также установить ограничения на его выбор. Таким образом, задавая конкретное значение уровня секущей плоскости, пользователи получают эллиптическую кривую, с помощью которой будут производить дальнейшие вычисления.

Добавление подобного действия в криптографические протоколы увеличивает количество используемых в нем эллиптических кривых, увеличивается количество точек и число возможных вариантов выбора, а, следовательно, возрастает и криптостойкость системы.

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 $y^2 = x^3 + ax + b + Z$.

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.

На рис. 2 показано графическое представление кубической кривой в пространстве, секущей плоскости Z и получаемая при этом эллиптическая кривая на плоскости.

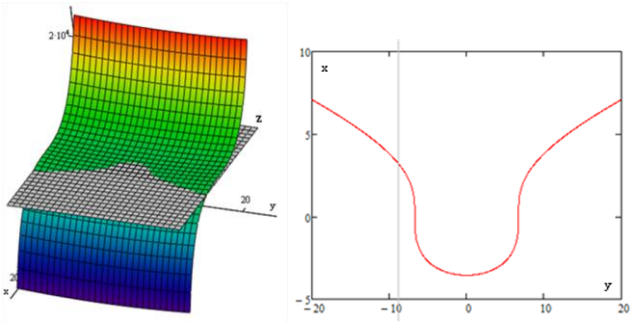

Рис. 2. Кубическая кривая и секущая плоскость в пространстве (справа), эллиптическая кривая на плоскости (слева)

Абонент A:

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 B.

Абонент B:

3. Выбирает целое число n_B, меньшее n. Это число будет личным ключом участника B. Затем участник B 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 изображена на рис. 3.

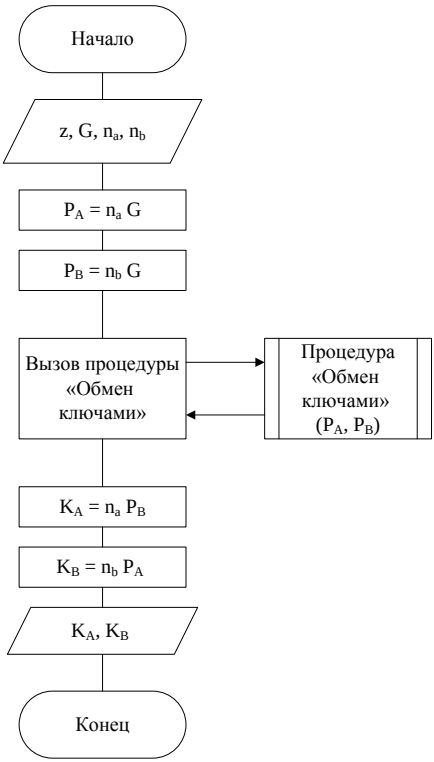

Рис. 3. Структурная схема алгоритма Диффи-Хеллмана с использованием кубической кривой

3. Реализация схемы обмена ключами с использованием кубической кривой

Приложение «Эллиптические кривые 1.1» разработано специально для работы с эллиптическими кривыми. Внешний вид приложения представлен на рис. 4.

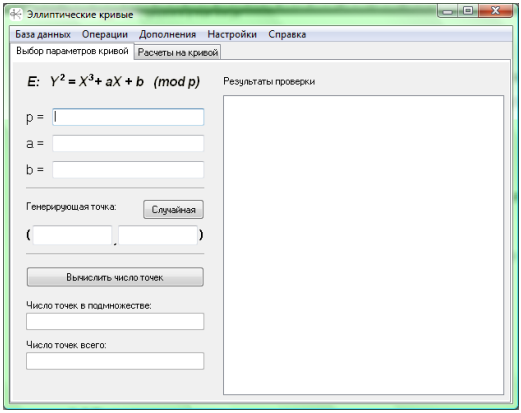

Рис. 4. Внешний вид приложения «Эллиптические кривые 1.1»

Оно 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.

Выбор кривой из БД происходит следующим образом:

1. Взять эллиптическую кривую из БД.
2. Выбрать значение p.
3. Выделить в предлагаемом списке строку и нажать «Выбрать».

После выбора эллиптической кривой, ее числовые параметры будут отражены в левой части главного окна, а результаты проверки выполнения условий в правой.

Возможно задание параметров эллиптической кривой вручную, а также возможно случайным образом выбрать генерирующую точку или проверить, принадлежит ли заданная точка эллиптической кривой.

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

Помимо всего, данное приложение позволяет проиллюстрировать работу алгоритма шифрования Эль-Гамаля (рис. 5) и работу алгоритма генерации и проверки ЭП (рис. 6).

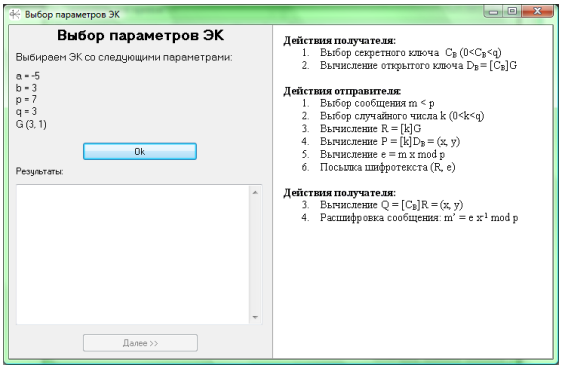

Рис. 5. Окно алгоритма шифрования Эль-Гамаля

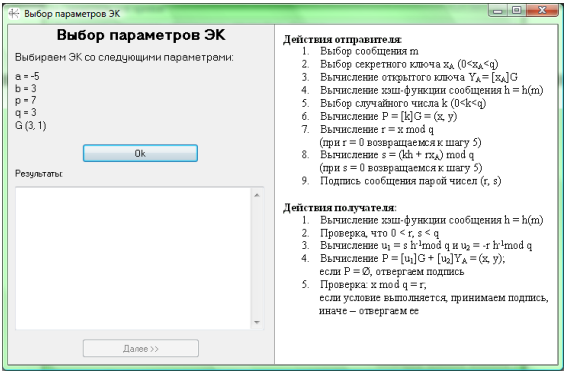

Рис. 6. Окно алгоритма генерации и проверки ЭП

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.

Для определения изменения сложности при внедрении в криптосистемы эллиптических кривых высших порядков на рис. 7

изображены графики сложностей для алгоритмов на эллиптических кривых второго порядка и высших порядков.

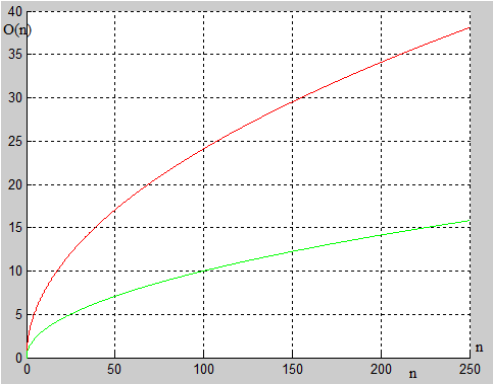

Рис. 7. Сравнение сложностей алгоритмов на эллиптических кривых второго порядка (нижний график) и на эллиптических кривых высших порядков (верхний график)

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

В статье 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.

Список литературы

1. Тилборг, ван Х.К.А. Основы криптологии: учебное пособие/ Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.

2. ГОСТ Р ИСО/МЭК 7498-1. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. –М.: ИПК Издательство стандартов, 2000. – 62 с.

3. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2004. – 328 с.

4. Элементарное введение в эллиптическую криптографию: учебное пособие / А. А. Болотов [и др.]. – М.: КомКнига, 2006. – 280 с.

5. Коломийцева, С.В. Введение в эллиптическую криптографию: учебное пособие / С.В. Коломийцева. – Хабаровск: ДВГУПС, 2012. – 35 с.