УДК 681.3

АНАЛИЗ ПОРОГОВЫХ КРИПТОСИСТЕМ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Н. И. ЧЕРВЯКОВ
М. Г. БАБЕНКО

Ставропольский государственный университет

e-mail: whbear@yandex.ru

В статье рассмотрены методы построения пороговых криптосистем на эллиптической кривой (ЭКК-ПК). Проведен сравнительный анализ скорости шифрования и дешифрования при реализации ЭКК-ПК, использующей эллиптическую кривую, рекомендованную NIST и ЭКК-ПК, построенную с использованием СОК.

Ключевые слова: пороговые криптосистемы на эллиптической кривой, система остаточных классов.

Современные информационные системы требуют особого подхода к передаче электронных документов по открытым каналам связи и сохранению секретных сведений. Для этих целей используются криптографические средства защиты информации.

Эллиптические кривые – один из самых перспективных инструментов для построения криптографических алгоритмов [1].

В работе [2] предлагается использовать для передачи данных в уязвимых к атакам беспроводным сетям пороговую криптосистему на эллиптической кривой, позволяющую доставлять сообщение от отправителя к получателю при условии, что ряд пользователей сети недоступны по техническим или каким-либо другим причинам. Это обусловлено тем, что эллиптическая кривая обеспечивает максимально возможную для криптосистемы с открытым ключом стойкость на один бит размера задачи [3]. В работе [2] представлена табл. 1 о размерах ключей для эквивалентных уровней безопасности.

Таблица 1

Размер ключей в битах для эквивалентных уровней безопасности

Симметричный	ECC	DH/DSA/RSA
128	283	3072
192	409	7680
256	571	15360

Эллиптическая кривая E над простым полем F_p, где $p>3$, задана уравнением в форме Вейерштрассе:

$$E(F_p): y^2 = x^3 + ax + b,\ \text{где}\ 4a^3 + 27b^2 \neq 0\ \text{и}\ a,\ b \in F_p. \tag{1}$$

Решение уравнения (1) совместно с бесконечно удаленной точкой задают множество точек эллиптической кривой. При использовании самого быстрого универсального алгоритма SEA для нахождения $\#E(GF(q))$ требуется 283^6 операций, что приблизительно равно 5×10^{14}, а так как современная вычислительная техника может выполнять 10^{10} операций в секунду, то потребуется 13 часов для нахождения порядка одной эллиптической кривой. Это делает данный алгоритм неприемлемым для использования его в практических целях.

Альтернативным решением этой проблемы является построение криптосистемы на эллиптической кривой с использованием системы остаточных классов.

Сложность генерации может быть уменьшена при использовании эллиптической кривой над кольцом Z_q, где $q=\prod_{i=1}^{n} p_i$, p_i – попарно различные простые числа и для каждого $i \in \{1,2,..,n\}$ $p_i > 3$.

Пусть эллиптическая кривая над кольцом задана уравнением

$$E(Z_q): y^2 = x^3 + ax + b \text{ над } Z_q, \tag{2}$$

где $q=\prod_{j=1}^{n} p_j$ и p_j – попарно простые числа и $p_i > 3$.

Приведем алгоритм нахождения мощности множества эллиптической кривой, заданной уравнением (2).

Алгоритм нахождения мощности множества точек на эллиптической кривой.

Рассмотрим сравнение

$$y^2 \equiv x^3 + ax + b (\bmod p_i). \tag{3}$$

1. Найдем количество решений n_i сравнения (3), используя формулу $n_i = p_i + \sum_{x \in F_{p_i}} \left(\frac{x^3+ax+b}{p_i}\right)$, где $\left(\frac{x^3+ax+b}{p_i}\right)$ – символ Лежандра.
2. Вычислим порядок по формуле.

$$\# E(Z_q) = \prod_{i=1}^{s} n_i + 1.$$

При соответствующем выборе простых чисел p_i мощность множества точек эллиптической кривой, заданной уравнением (2), при $\lfloor \log_2 q \rfloor = 283$ вычисляется с использованием вышеприведенного алгоритма за 1 секунду, что гораздо меньше, чем время у алгоритма SEA.

Поставим задачу сравнить скорость шифрования и дешифрования данных криптосистемы, построенной с помощью пороговой криптосистемы на точках эллиптической кривой, заданной уравнением (2) и использующей операции в СОК с пороговой криптосистемой, построенной на точках эллиптической кривой, из работы [4].

Рассмотрим основные методы из работы [2] для построения пороговой криптографии на точках эллиптической кривой.

1. Для разбиения перед кодированием: отправитель S генерирует частичные сообщения, используя интерполяцию Шамира-Лагранжа из сообщения M, затем шифрует эти частичные сообщения в точки.

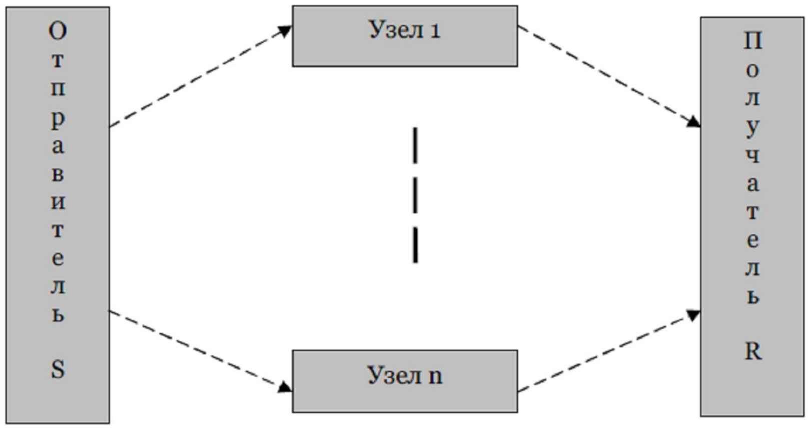
Для разбиения после кодирования отправитель S сначала шифрует сообщение в точки, затем зашифрованные точки разбивает на частичные сообщения, используя интерполяцию Лагранжа.

2. S распространяет частичные сообщения $C_i s$ наряду с передачей x_i, s надежно ко всем соседним узлам по разным несвязным маршрутам.

3. Доступные узлы на этих маршрутах выполняют задачу отправления частичных пакетов сообщения, пока это не достигает получателя R. Ни один из этих узлов не является или акционером или объединителем в реализации ЭКК-ПК.

4. Когда R получает t или больше $C_i s$ и $x_i s$, используя сначала t x_i значения, тогда вычисляет соответствующий зашифрованный текст C. В случае разбиения перед кодированием эти частичные сообщения сначала расшифровываются с исполь-

зованием алгоритма ЭКК-ПК, а затем, используя интерполяцию Лагранжа, оригинальное сообщение восстанавливается. Для разбиения после кодирования частичные сообщения сначала объединяют, используя интерполяцию Лагранжа, чтобы возвратить оригинальный C, затем, используя алгоритм ЭКК-ПК для расшифровки, оригинальное сообщение M восстанавливают.



Мультиперелет вовлекает больше, чем 2 узла,
на единственном несвязном маршруте

Рис. 1. Модель протокола, базирующегося на ЭКК-ПК

Приведем методы построения ЭКК-ПК с разбиением на части до и после кодирования. Для уменьшения времени вычисления скалярного умножения точки на эллиптической кривой все операции с точками будем производить в проективной системе координат.

Метод 1. **Шифрование данных с разбиением на части перед кодированием.**

1) Алиса разбивает сообщение M на n частей секрет M_t, $1 \le t \le n$;

2) Алиса преобразовывает каждую часть M_t в точку $P_t(X_t : Y_t : Z_t)$;

3) Алиса выбирает случайное число $r < |H|$ и вычисляет $rn_BG = (X_k : Y_k : Z_k)$;

4) Алиса сообщает $(rG,, X_kX_t \bmod p, Y_kY_t \bmod p, Z_kZ_t \bmod p)$.

Метод 2. **Дешифрования данных с разбиение на части перед кодированием.**

1) Боб вычисляет $n_BrG = rn_BG = (X_k : Y_k : Z_k)$;

2) Боб восстанавливает X_t и Y_t, используя $X_k^{-1}X_kX_t \bmod p$, $Y_k^{-1}Y_kY_t \bmod p$ и $Z_k^{-1}Z_kZ_t \bmod p$;

3) Если есть t и больше частей P_M, то Боб восстанавливает P_M и преобразует P_M в секрет M.

Метод 3. **Шифрование данных с разбиением на части после кодирования.**

1) Алиса конвертирует сообщение M в точку $P_M(X : Y : Z)$;

2) Алиса выбирает случайное число $r <| H |$;

3) Алиса вычисляет $rn_B G = (X_k : Y_k : Z_k)$, $u = X_k X \bmod p$, $w = Y_k Y \bmod p$ и $v = Z_k Z \bmod p$;

4) Алиса разбивает u, w, v на n частей u_t, w_t и v_t соответственно, $1 \le t \le n$;

5) Алиса передает rG и n части u_t, w_t и v_t Бобу.

Метод 4. **Дешифрование данных с разбиением на части после кодирования.**

1) Боб комбинирует t части u_t, w_t, v_t и вычисляет каждое значение отдельно u, w, v;

2) Боб вычисляет $n_B rG = rn_B G = (x_k, y_k)$;

3) Боб восстанавливает P_M, используя X_k $X_k^{-1}u = X_k^{-1} X_k X \bmod p$ и $Y_k^{-1}w = Y_k^{-1} Y_k Y \bmod p$, $Z_k^{-1}w = Z_k^{-1} Z_k Z \bmod p$;

4) в конечном счете, Боб конвертирует P_M в секрет M.

Реализуя приведенные алгоритмы для рекомендованной эллиптической кривой из работы [4]:

кривая $P-256$;

$\mathrm{p} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$;

$a = -3$;

b = 5ac635d8 aa3a93e7 b3ebbd55769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b.

И эллиптической кривой $Q-281$:

$q = \prod_{i=1}^{32} p_i$, где $p_1 = 271$, $p_2 = 277$, $p_3 = 281$, $p_4 = 283$, $p_5 = 293$, $p_6 = 307$, $p_7 = 311$, $p_8 = 313$, $p_9 = 317$, $p_{10} = 331$, $p_{11} = 337$, $p_{12} = 347$, $p_{13} = 349$, $p_{14} = 353$, $p_{15} = 359$, $p_{16} = 367$, $p_{17} = 373$, $p_{18} = 379$, $p_{19} = 383$, $p_{20} = 389$, $p_{21} = 397$, $p_{22} = 401$, $p_{23} = 409$, $p_{24} = 419$, $p_{25} = 421$, $p_{26} = 431$, $p_{27} = 433$, $p_{28} = 439$, $p_{29} = 443$, $p_{30} = 449$, $p_{31} = 457$, $p_{32} = 461$;

$a = -3$;

b = 5ac635d8 aa3a93e7 b3ebbd55769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b.

Для тестирования методов разделения секрета на точках эллиптических кривых было сгенерировано 1000 случайных сообщений. После запросили системное время T_{start} – время начала, T_{end} – время окончания выполнения алгоритма, а среднее время работы алгоритма вычисляем по формуле $\frac{T_{end} - T_{start}}{1000}$. Результаты, полученные при тестировании, представлены в табл. 2.

Таблица 2

Среднее время работы методов в миллисекундах

	Кривая $P-256$	Кривая $Q-281$
Метод 1	638	325
Метод 2	701	400
Метод 3	647	327
Метод 4	698	401

Мы видим, что шифрование в СОК приблизительно в два раза быстрее, чем шифрование, использующее алгоритмы из работы [4], а дешифрование – на треть быстрее. Это происходит вследствие того, что выполнение модулярных операций в СОК быстрее, что позволяет использовать криптосистемы на точках эллиптической кривой, построенные на базе СОК с большей эффективностью.

Литература

1. Menezes, A. Handbook of applied cryptography [текст] / A. Menezes, P. van Oorchot, S. Vanstone – CRC press, 1997. – 816 p.

2. Ertaul, L. Elliptic Curve Cryptography based Threshold Cryptography Implementation for MANETs [текст] / L. Ertaul, N. J. Chavan // IJCSNS International Journal of Computer Science and Network Security. – 2007. – Vol. 7. – No. 4. P. 48–61.

3. Ростовцев А. Г. Два подхода к логарифмированию на эллиптической кривой [текст] / А. Г. Ростовцев, Е. Б. Маховенко // http://www.ssl.stu.neva.ru/ssl/archieve/lift1.pdf

4. Recommended Elliptic Curves for Federal Government Use [текст]. – NIST. http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf.

AN ANALYSIS THRESHOLD IN ELLIPTIC CURVE CRYPTOGRAPHY

N. I. CHERVAYKOV
M. G. BABENKO

Stavropol State University

e-mail: whbear@yandex.ru

The methods for constructing threshold in Elliptic Curve Cryptography (ECC-TC) are described in article. We researched a comparative analysis of the speed encryption and decryption in the implementation of ECC-TC, and used elliptic curves recommended by NIST and the ECC-TC built with the use of SRC.

Key words: threshold cryptosystem on an elliptic curve, system of residual classes.