ISSN 2079-8490

Электронное научное издание
«Ученые заметки ТОГУ»
2018, Том 9, № 3, С. 1445 – 1447

Свидетельство
Эл № ФС 77-39676 от 05.05.2010
http://pnu.edu.ru/ru/ejournal/about/
ejournal@pnu.edu.ru

УДК 519.719.2

© 2018 г. **В. Я. Прудников**, канд. физ.-мат. наук,
А. А. Новиков
(Тихоокеанский государственный университет, Хабаровск)

ИСПОЛЬЗОВАНИЕ МЕТОК СОВМЕСТНО С ПРОТОКОЛОМ МЕССИ-ОМУРЫ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В работе рассмотрен алгоритм использования меток на примере асимметричного протокола Месси-Омуры на эллиптических кривых.
Ключевые слова: протокол Месси-Омуры, эллиптические кривые, метки

V. Y. Prudnikov, A. A. Novikov

USING OF MARKS WITH A MESSEY-OMURA PROTOCOL ON ELLIPTIC CURVES

The paper discusses an algorithm of using of marks on the example of the asymmetric Messey-Omura protocol on elliptic curves.
***Keywords*:** Messey-Omura protocol, elliptic curves, zeropoint.

При использовании стандартного протокола Месси-Омуры на эллиптических кривых существует вероятность компрометации диалога путем подмены злоумышленником сообщения одного из легитимных участников диалога сообщением, отправленным ранее, без расшифровки сообщения третьей стороной. В некоторых случаях это может привести к недопониманию сторон, либо же просто к срыву сеанса обмена сообщениями.

Данной проблемы можно избежать, используя метки, содержащие в себе информацию, например, о порядковом номере отправленного сообщения.

Рассмотрим один из возможных способов использования подобных меток. Напомним некоторые определения эллиптической криптографии.

Определение 1. *Нулевым элементом на эллиптической кривой* E *принято называть точку «в бесконечности», являющуюся результатом сложения двух противоположных точек эллиптической кривой, и обозначаемую как* O.

Определение 2. *Обозначим две точки эллиптической кривой, как* $P_1 = (x_1, y_1)$, *либо* $P_1 = O$ *и* $P_2 = (x_2, y_2)$, *либо* $P_2 = O$. *Операция сложения* $P_3 = P_1 + P_2$ *в группе точек эллиптической кривой определяется следующим образом:*

Если $P_1 = -P_2$, *то* $P_3 = O$,
если $P_1 = O$, *то* $P_3 = P_2$,
если $P_2 = O$, *то* $P_3 = P_1$,
если $x_1 \neq x_2$, *то* $P_3 = -(x_3, y_3)$,
в остальных случаях (когда $P_1 = P_2$), $P_3 = 2P_1 = -(x_3, y_3)$.

Точки вида $-(x_3, y_3)$ вычисляются по определенным формулам, в зависимости от вида эллиптической кривой и условия совпадения или различия точек. [1]

Определение 3. *Умножение целого числа на точку эллиптической кривой определяется следующим образом. Если* n – *целое число, то, как и в любой абелевой группе,* nP *обозначает сумму* n *точек* P *при* $n > 0$ *и сумму* $|n|$ *точек* $-P$, *если* $0 \leq n$.[2]

Определение 4. *Противоположной к* $P = (x, y) \neq O$ *точкой называется точка* $-P = (x, -y)$. [1]

Основываясь на определениях 1-4, опишем алгоритм протокола Месси-Омуры на эллиптических кривых, добавив к нему использование меток.

Криптосистема Месси-Омуры является улучшением протокола Шамира. Эллиптический вариант данного протокола основан на невозможности решения задачи дискретного логарифмирования в группе точек эллиптической кривой.

Изначально, два абонента Аи В, желающие обменяться некоторыми данными, договариваются в выборе некоторой эллиптической кривой Eнад конечным полем F_q (q *при этом берется достаточно большим*)с определенным числом N точек на ней, определяется алфавит, который будет использоваться для представления сообщений в виде точек выбранной кривой. Так же выбирается набор меток в виде точек кривой E, использование которых позволяет однозначно понять, что получено именно то сообщение, которое отправлялось (это может быть метка порядка сообщения, временная метка, либо же идентификатор абонента, отправляющего сообщение).Далее каждый из абонентов выбирает для себя некоторое случайное целое число e между 1 и N, удовлетворяющее условию $НОД(e, N) = 1$. Данное число будет шифрующим секретным ключом каждого абонента. Затем они вычисляют число d, являющееся обратным числу eпо модулю N, удовлетворяющее условию $ed = 1\ (mod N)$.

1. Абонент А, желающий послать Внекоторое сообщение, представляет его в виде точки эллиптической кривой E, *которую обозначим, как* P_m.

2. Адобавляет к своему сообщению метку M_1: $P_{m1} = P_m + M_1$.

3. А шифрует получившуюся точку, умножая ее на свое число e_a*, получая точку* $e_a P_{m1}$*, которую он передает абоненту В.*

4. В, получив сообщение с точкой $e_a P_{m1}$*, не пытаясь ее расшифровать, умножает ее на свое число* e_b*, получая точку* $e_b e_a P_{m1}$*, и передает ее обратно А.*

5. А снимает свой шифр, умножая полученную точку на свой расшифровывающий ключ d_a*, получая тем самым точку* $e_b e_a P_{m1} d_a = e_b P_{m1}$*, передает точку далее абоненту В.*

6. Втаким же образом снимает свой шифр ключом d_b*, получая точку* $e_b e_a P_{m1} d_a d_b = P_{m1}$.

7. Для проверки легитимности сообщения, В, заранее зная, какая именно метка должна использоваться в данном сообщении, вычисляет точку, противоположную M_1*, и складывает результат с полученной от А и уже расшифрованной точкой* P_{m1}*:* $P_m = P_{m1} + (-M_1)$*. Если полученная точка находится в наличии в заранее оговоренном алфавите, сообщение принимается, как легитимное, в противном случае, сообщение отклоняется и канал считается скомпрометированным.*

Теорема 1. *Пусть имеется точка* P *некоторой эллиптической кривой точка* $-P$*, противоположная ей.*

Некоторая точка N *этой кривой, входящая в сумму* $S = P + N$*, может быть выделена из данной суммы путем сложения точки, являющейся суммой и точки, являющейся противоположной точкой для* P*, следующим образом*

$$N = S + (-P) = (P + N) + (-P).$$

Доказательство. Воспользуемся свойствами сложения точек эллиптической кривой, описанных в определении 1.

Если $P_1 = -P_2$, то $P_3 = O$, а так же, если $P_1 = O$, то $P_3 = P_2$, поэтому имеем

$$N = S + (-P) = (P + N) + (-P) = P + (-P) + N = O + N = N.$$

Теорема 2. *Пусть эллиптическая кривая* E *имеет* N *точек, точка* P *принадлежит* E*, а некоторое целое число* e*, лежащее между 1 и* N *и имеющее противоположную по модулю* N *точку* $d = e^{-1}$*, удовлетворяет условию* $ed = 1\ (mod N)$.

Точка P*, входящая в произведение* $M = eP$*, может быть выделена из данного произведения следующим образом*

$$P = Md = ePd.$$

Доказательство. Согласно теореме точки e и d удовлетворяют условию $ed = 1\ (mod N)$, поэтому

$$P = Md = ePd = edP = 1 * P = P.$$

Список литературы

[1] Болотов, А. А. ГашковС. Б., . Фролов А.Б. Элементарное введение в эллиптическую криптографию. М.: КомКнига, 2006. .

[2] Жданов О. Н. Чалкин Т. А. Применение эллиптических кривых в криптографии: учеб. пособие. Красноярск: СибГАУ, 2011.

E-mail:
Прудников В. Я. – prudnickov.vit@yandex.ru,
Новиков А. А. – novikowtosha@yandex.ru