УДК 681.3

КРИПТОСИСТЕМА РАБИНА, ПОСТРОЕННАЯ НА ТОЧКАХ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Бабенко М.Г., Червяков Н.И.

В статье разрабатывается криптосистема Рабина, в основе которой лежат точки на эллиптической кривой. Предложен способ устранения недостатков криптосистемы Рабина за счет использования свойств хеш-функции.

Ключевые слова: эллиптическая кривая, криптосистема Рабина на точках эллиптической кривой, факторизация чисел.

Введение

Эллиптические кривые – один из самых перспективных инструментов для построения криптографических алгоритмов [1]. Это обусловлено тем, что они обеспечивают максимально возможную для криптосистемы с открытым ключом стойкость на один бит размера задачи [2]. Эллиптическая кривая E задается уравнением в форме Вейерштрассе:

$$E(Z_n): y^2 = x^3 + ax + b\,, \qquad (1)$$

где $n = pq$ и $p\,, q$ — простые числа равной длины.

Для построения криптосистемы Рабина с использованием эллиптической кривой необходимо умение делить в конечном кольце, не зная разложения на простые множители, что является нерешаемой задачей. Таким образом, требуется разработать алгоритм криптосистемы Рабина на точках эллиптической кривой, заданной над конечным кольцом.

Решение задачи

Для того, чтобы выполнять операции с точками на эллиптической кривой, не используя операции деления в конечном кольце, воспользуемся эллиптической кривой, заданной в проективных координатах, в форме Вейерштрассе

$$E(Z_n): Y^2Z = X^3 + aXZ^2 + bZ^3\,. \qquad (2)$$

Связь между координатами точек эллиптических кривых, заданных уравнениями (1) и (2), определяется по следующей формуле:

$$\begin{cases} x = \dfrac{X}{Z}, \\ y = \dfrac{Y}{Z}. \end{cases} \qquad (3)$$

На эллиптической кривой (3) формулой из работы [3] задана операция сложения точек:

$$P_1 = (X_1, Y_1, Z_1) \in E(Z_n);$$
$$P_2 = (X_2, Y_2, Z_2) \in E(Z_n), \quad P_1, P_2 \neq O\,, \quad P_1 \neq \pm P_2;$$
$$P_3 = P_1 + P_2 = (X_3, Y_3, Z_3):$$
$$\begin{cases} X_3 = v\left(Z_2\left(u^2 Z_1 - 2v^2 X_1\right) - v^3\right) \bmod n, \\ Y_3 = Z_2\left(3uv^2 X_1 - v^3 Y_1 - u^3 Z_1\right) + uv^3 \bmod n, \\ X_3 = v^3 Z_1 Z_2 \bmod n, \end{cases} \qquad (4)$$
$$u = \left(Y_2 Z_1 - Y_1 Z_2\right) \bmod n\,,\ v = \left(X_2 Z_1 - X_1 Z_2\right) \bmod n.$$

Удвоение также задается формулой из [3] для $E(Z_n)\,,\ P_3 = 2P_1$:

$$\begin{cases} X_3 = 2Y_1 Z_1 \left(w^2 - 8X_1 Y_1^2 Z_1\right) \bmod n, \\ Y_3 = 4Y_1^2 Z_1 \left(3wX_1 - 2Y_1^2 Z_1\right) \bmod n, \\ Z_3 = 8Y_1^3 Z_1^3 \bmod n, \end{cases} \qquad (5)$$

где $w = \left(3X_1^2 + AZ_1^2\right) \bmod n$.

Таким образом, из (4)-(5) следует подтверждение, что для вычисления сложения и удвоения точек на эллиптической кривой не используется операция деления.

Для построения криптосистемы Рабина на точках эллиптической кривой получатель сообщения выбирает два больших простых числа p и q приблизительно одинакового размера так, чтобы $p \equiv q \equiv 3 (\bmod 4)$. Далее он вычисляет число $n = pq$ и выбирает случайным образом число $a \in [1 \ldots n-1]$, тогда пара (n, a) является публичным ключом, а пара чисел (p, q) – секретным ключом криптосистемы Рабина на точках эллиптической кривой

$$E\,(Z_n)\, y^2 = x^3 + ax. \qquad (6)$$

Алгоритм 1. Шифрования текста в криптосистеме Рабина, построенной на точках эллиптической кривой.

Вход. Текст *M*, открытый ключ числа (n,a).

Выход. Шифротекст, точка $Q \in E(Z_n)$.

1. $P = \text{TextToPint}(M)$.
2. $Q = 2P$.
3. Возвращаем Q.

Функция кодирования алфавита точками эллиптической кривой – TextToPint(P) – описана в [4]. Значение Q. вычисляется с помощью уравнения (5) и передается по открытым каналам связи получателю.

Получатель получил точку Q., теперь перед ним стоит задача решить уравнение

$$2X = Q. \qquad (7)$$

Сформулируем необходимое условие для того, чтобы уравнение имело решение.

Утверждение 1 (необходимое условие). Пусть эллиптическая кривая $E(Z_n)$ задана уравнением (6), где $n = pq$, p, q – простые числа, $p \equiv q \equiv 3(\bmod 4)$, $a > 0$, а точки $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(Z_n)$ такие, что $Q = 2P$ и $P \neq O$, тогда выполняются условия: $\left(\frac{x_Q}{p}\right) = 1$ и $\left(\frac{x_Q}{q}\right) = 1$.

Доказательство.

Так как $P \neq O$, то используем формулу

$$2P = \left(x_P - \frac{3x_P^4 + 6ax_P^2 - a^2}{4y_P^2}, \frac{x_P^6 + 5ax_P^4 - 5a^2x_P^2 - a^3}{8y_P^3} \right),$$

после чего получим

$$x_Q = x_P - \frac{3x_P^4 + 6ax_P^2 - a^2}{4y_P^2} =$$

$$= \frac{4y_P^2 x_P - 3x_P^4 - 6ax_P^2 + a^2}{4y_P^2} =$$

$$= \frac{4\left(x_P^3 + ax_P\right)x_P - 3x_P^4 - 6ax_P^2 + a^2}{4y_P^2} =$$

$$= \frac{x_P^4 - 2ax_P^2 + a^2}{4y_P^2} = \left(\frac{x_P^2 - a}{2y_P}\right)^2.$$

Значит, $\left(\frac{x_Q}{p}\right) = 1$ и $\left(\frac{x_Q}{q}\right) = 1$.

Утверждение доказано.

Сформулируем достаточное условие, чтобы уравнение (7) имело решение.

Теорема 1 [5]. Пусть задана эллиптическая кривая уравнением (6) и $Q(u,v) \in E(Z_n)$ – данная точка. Если уравнение (7) разрешимо и $p = (x_1, y_1)$ – его решение, то координата x_1 удовлетворяет следующим условиям.

1. x_1 – корень уравнения

$$l(x) = x^4 - 4ux^3 - 2ax^2 - 4auX + a^2 = 0. \qquad (8)$$

2. $\left(\frac{2x_1 + u}{p}\right) = 1$ *или* 0. (9)

3. $\left(\frac{2x_1 + u}{q}\right) = 1$ *или* 0. (10)

4. $\left(\frac{x_1^3 + a \cdot x}{p}\right) = 1$ *или* 0. (11)

5. $\left(\frac{x_1^3 + a \cdot x}{q}\right) = 1$ *или* 0. (12)

Обратно, если x_1 – элемент Z_n, удовлетворяющий условиям (8)-(12), то на *E* существует точка $P = (x_1, y_1)$, удовлетворяющая уравнению (7).

Из теоремы 1 следует, что для того, чтобы найти решение уравнения (7), нужно решить уравнение (8) и проверить его на выполнение условий (9)-(10). Для этого будем искать решения уравнения (8) по каждому из модулей в отдельности, а потом восстанавливать искомый корень, используя китайскую теорему об остатках.

Предложим алгоритм, основанный на этой идее, для решения уравнения (7).

Алгоритм 2. Решения уравнения (8) на эллиптической кривой (6).

Вход. Точка $Q = (u,v) \in E(F_p)$, числа a, p.

Выход. Решения уравнения (8).

1. $flag = False$.
2. $D_1 = \sqrt{u^2 + a}$, $D_{21} = 8\left(u^2 - uD_1\right)$.
3. Если $\left(\frac{u^2 + a}{p}\right) = 0$ и $\left(\frac{u^2 - a}{p}\right) = 0$, то
   - 3.1. Вывод $x = 0$.
   - 3.2. $flag = True$.
4. Если $\left(\frac{u^2 + a}{p}\right) = 0$, и $\left(\frac{u^2 - a}{p}\right) = 1$, и $\left(\frac{2}{p}\right) = 1$, и $\left(\frac{3u + 2\sqrt{u^2 - a}}{p}\right) > -1$, то
   - 4.1. Вывод $x = u + \sqrt{u^2 - a}$;
   - 4.2. $flag = True$.

5. Если $\left(\frac{u^2+a}{p}\right)=0$, и $\left(\frac{u^2-a}{p}\right)=1$, и $\left(\frac{2}{p}\right)=1$, и $\left(\frac{3u-2\sqrt{u^2-a}}{p}\right)>-1$, то

5.1. Вывод $x=u-\sqrt{u^2-a}$;

5.2. $flag=True$.

6. Если $u=0$ и $\left(\frac{a}{p}\right)=1$ и $\left(\frac{2\sqrt{a}}{p}\right)=1$, то

6.1. Вывод $x=\sqrt{a}$;

6.2. $flag=True$.

7. Если $u=0$ и $\left(\frac{a}{p}\right)=1$ и $\left(\frac{2\sqrt{a}}{p}\right)=-1$, то

7.1. Вывод $x=p-\sqrt{a}$;

7.2. $flag=True$.

8. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=-1$, и $\left(\frac{D_{21}}{p}\right)=1$, и $\left(\frac{3u-2D_1+2\sqrt{2\left(u^2-uD_1\right)}}{p}\right)>-1$, то

8.1. Вывод $x=u-D_1+\sqrt{2\left(u^2-uD_1\right)}$;

8.2. $flag=True$.

9. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=-1$, и $\left(\frac{D_{21}}{p}\right)=1$, и $\left(\frac{3u-2D_1-2\sqrt{2\left(u^2-uD_1\right)}}{p}\right)>-1$, то

9.1. Вывод $x=u-D_1-\sqrt{2\left(u^2-uD_1\right)}$;

9.2. $flag=True$.

10. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=-1$, и $\left(\frac{D_{21}}{p}\right)=1$, и $\left(\frac{3u+2D_1+2\sqrt{2\left(u^2-uD_1\right)}}{p}\right)>-1$, то

10.1. Вывод $x=u+D_1+\sqrt{2\left(u^2-uD_1\right)}$;

10.2. $flag=True$.

11. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=-1$, и $\left(\frac{D_{21}}{p}\right)=1$, и $\left(\frac{3u+2D_1-2\sqrt{2\left(u^2-uD_1\right)}}{p}\right)>-1$, то

11.1. Вывод $x=u+D_1-\sqrt{2\left(u^2-uD_1\right)}$;

11.2. $flag=True$.

12. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=1$, и $\left(\frac{3u-2D_1+2\sqrt{2\left(u^2-uD_1\right)}}{p}\right)>-1$, то

12.1. Вывод $u-D_1+\sqrt{2\left(u^2-uD_1\right)}$;

12.2. $flag=True$.

13. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=1$, и $\left(\frac{3u-2D_1-2\sqrt{2\left(u^2-uD_1\right)}}{p}\right)>-1$, то

13.1. Вывод $u-D_1-\sqrt{2\left(u^2-uD_1\right)}$;

13.2. $flag=True$.

14. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=1$, и $\left(\frac{D_{21}}{p}\right)=-1$, и $\left(\frac{3u+2D_1+2\sqrt{2\left(u^2+uD_1\right)}}{p}\right)>-1$, то

14.1. Вывод $x=u+D_1+\sqrt{2\left(u^2+uD_1\right)}$;

14.2. $flag=True$.

15. Если $\left(\frac{u^2+a}{p}\right)=1$, и $u\neq 0$, и $\left(\frac{a}{p}\right)=1$, и $\left(\frac{D_{21}}{p}\right)=-1$, и $\left(\frac{3u+2D_1-2\sqrt{2\left(u^2+uD_1\right)}}{p}\right)>-1$, то

15.1. Вывод $x=u+D_1-\sqrt{2\left(u^2+uD_1\right)}$;

15.2. $flag=True$.

16. Если $flag=False$, то вывод «решения нет».

17. Конец алгоритма.

В данном алгоритме $\left(\frac{a}{p}\right)$ обозначает символ Лежандра.

Если α – квадратичный вычет F_p, то для извлечения квадратного корня в F_p, где $p\equiv 3(\mathrm{mod}\,4)$, удобно использовать формулу $\sqrt{a}=a^{\frac{p+1}{4}}(\mathrm{mod}\,p)$.

Алгоритм 3. Дешифровки текста для криптосистемы Рабина, построенной на точках эллиптической кривой.

Вход. Шифротекст (точка) $Q=(u,v,z)$, секретный ключ – пара чисел (p,q) и число a из открытого ключа.

Выход. Исходный текст

1. $zop = z^{p-2} \bmod p.$
2. $zoq = z^{p-2} \bmod q.$
3. $u_p = (u \cdot zop) \bmod p.$
4. $u_q = (u \cdot zoq) \bmod q.$
5. $v_p = (v \cdot zop) \bmod p.$
6. $v_q = (v \cdot zoq) \bmod q.$
7. Используя алгоритм 2, находим множество возможных значений $x_{p,i}$ и $x_{q,j}$.
8. Для всех $i=1$ до $Count(x_p)$ выполнять:

   8.1. Если $\left(\frac{x_{p,i}^3 + a \cdot x_{p,i}}{p}\right) > -1$, то

   8.1.1. $TempY = \left(x_{p,i}^3 + a \cdot x_{p,i}\right)^{\frac{p+1}{4}} \bmod p;$

   8.1.2. $TempYO = TempY^{p-2} \bmod p.$
   $TempV = -TempY +;$

   8.1.3. $+\frac{p+1}{2} \cdot \left(3x_{p,i}^2 + a\right) \cdot TempYO \cdot \left(u_p - x_{p,i}\right);$

   8.1.4. Если $(v_p - TempV) \bmod p = 0$, то
   $y_{p,i} = TempY$ иначе $y_{p,i} = p - TempY.$

9. Для всех $j=1$ до $Count(x_q)$ выполнять:

   9.1.1. $TempY = \left(x_{q,j}^3 + a \cdot x_{q,j}\right)^{\frac{q+1}{4}} \bmod q;$

   9.1.2. $TempYO = TempY^{q-2} \bmod q.$
   $TempV = -TempY +;$

   9.1.3. $+\frac{q+1}{2} \cdot \left(3x_{q,j}^2 + a\right) \cdot TempYO \cdot \left(u_q - x_{q,j}\right).$

   9.1.4. Если $(v_q - TempV) \bmod p = 0$, то
   $y_{q,j} = TempY$ иначе $y_{q,j} = q - TempY.$

10. Вычисляем множество возможных значений точки P:
    $P_{i,j} = \left((x_{p,i}, y_{p,i}), (x_{q,j}, y_{q,j})\right).$
11. Вычисляем возможные значения исходного текста $M_{i,j} = \text{PointToText}(P_{i,j})$.
12. Вывод $M_{i,j}$.

Из алгоритма 3 следует, что исходный текст нужно выбирать из нескольких возможных текстов. Эта проблема присутствовала и в криптосистеме, предложенной автором [6]. Для устранения этой проблемы будем вычислять на стадии шифрования значение хеш-функции для координаты x точки P. Получатель при расшифровке будет вычислять хеш-функции для каждого из претендентов, сравнивать его с исходным значением хеш-функции и выбирать истинное значение точки P из множества претендентов. Это возможно благодаря следующим свойствам хеш-функции[6]:

1. Необратимость хеш-функции – невозможность вычислить значения исходного текста, зная значения хеш-функции;

2. Стойкость к коллизиям первого рода – невозможность подобрать два разных текста, чтобы значения их хеш-функций было равным.

Из свойства 2 хеш-функций следует, что внесение изменений в текст влечет за собой изменение значения хеш-функции. Для n-битной хеш-функции вероятность того, что два разных текста будут иметь равные значения хеш-функции, равна $\frac{1}{2^n}$, при использовании $n=256$ бит получим, что вероятность равна 10^{-77}.

Пример. Используя алгоритм Рабина на точках эллиптической кривой $E(Z_n): y^2 = x^3 + ax$, зашифровать и дешифровать текст:

$$M = (0,0,1,0,0,1,1,0,1,1,1,0,0,0,0,0,1,1,1,0),$$

где $n = p\ q$, $p = 10^{199} + 3267$, $q = 10^{199} + 3307$ и $a = 1495680259\quad 4444322208\quad 0.$

Рассмотрим работу алгоритма шифрования криптосистемы Рабина на точках эллиптической кривой:

1. Используя алгоритм из работы [4], текст M закодируем в точку
$$P = (5095880,504767297520,1).$$
2. Вычисляем значение хеш-функции SHA-2 256 от координат x и y точки P, получаем:
$SHA(P_x) = 087be4bb71ba1ab1ce903d1e1b75f90b \backslash$
ee9991ec724d269faf9e5d202c96a784.
3. Вычисляем значение $Q = 2P$ по формуле (5)
$w = 50051155874494880,$
$X_Q = 25185174206790859148497292233248022 \backslash$
62183936000,
$Y_Q = 260481018001268059080407656856303 06 \backslash$
6267811840000,
$Z_Q = 10288773774034881403187583240560 64000.$
4. Передаем точку Q и $SHA(P_x)$.

Рассмотрим алгоритм дешифровки криптосистемы Рабина на точках эллиптической кривой.

1. Найдем множество значений x_p, воспользуемся для этого алгоритмом 2.

Вычислим $Z_Q^{-1} \bmod p$, получим

$zop = 233913991832622700351164422094970 47 \backslash$
$087694874998017061240973957624428726080 5 \backslash$
$554551227763103032137103318968321144498 2 \backslash$
$462491454094534743370084977545339815095 8 \backslash$
$806408927276869191484052719562187935033 5 \backslash$
6127;
$zoq = 616444353365446013474356966296799 69 \backslash$
$431207912984904896619502043673866754767 2 \backslash$
$411220982628474953848368169448814308159 4 \backslash$
$135215924418648906917209228613009117466 6 \backslash$
$127571030584118508408232967805905231908 9 \backslash$
723.

Вычислим u_p и v_p:

$u_P = X_Q \cdot zop \bmod p = 291102443405813699476 \backslash$
$833590531913354897468970589423492017594 6 \backslash$
$489855168260716841881062825333367713529 9 \backslash$
$138361427625131021756282255770048853402 4 \backslash$
$043435718257508038481697120881005591185 2 \backslash$
610236625096606842;
$v_p = Y_Q \cdot zop \bmod p = 5842873584105639348234 \backslash$
$296444363680416742382942637349324610818 3 \backslash$
$415106911381670603913017142164879762553 7 \backslash$
$585559391846871403476891392573747652795 4 \backslash$
$449088376037312980798352413834877945363 1 \backslash$
35259808564158058.

Вычислим u_q и v_q:

$u_q = X_Q \cdot zoq \bmod q = 24221077401465343319 \backslash$
$690312311378027359773647491181328940537 \backslash$
$963216874241424895115440419794642542674 \backslash$
$835855036893403545365596648765592336116 \backslash$
$211952548647712152325140640359470386125 \backslash$
$4872307527830434402531 4;$
$v_q = Y_Q \cdot zoq \bmod q = 83802774244351565812587 \backslash$
$073717366285056635774426070628142225452 7 \backslash$
$833303046822945060270155672663395723544 7 \backslash$
$331758434793143134048094978496577624326 1 \backslash$
$251438609243442970500938881822036464958 5 \backslash$
0748329976721765;

$Dp_1 = \left(u_p^2 + a\right)^{\frac{p+1}{4}} \bmod p = 291102443405813699 \backslash$
$476833590531913354897468970589423492017 5 \backslash$
$946489855168260716841881062825333367713 5 \backslash$
$299138361427625131021756282255770048853 4 \backslash$
$024043435718257508038481697120881005591 1 \backslash$
$852610236620190759384;$

$Dp_{21} = 8\left(u_p^2 - u_p Dp_1\right) = 96069464117077960336$

$\left(\frac{a}{p}\right) = -1.$

Так как $Dp_1 \neq 0$, $u_p \neq 0$, $\left(\frac{a}{p}\right) = -1$ и $\left(\frac{Dp_{21}}{p}\right) = 1$, то подходят только случаи 8 и 11.

Рассмотрим случай 8. Значение $\left(\frac{3u_p - 2Dp_1 + 2\sqrt{2\left(u_p^2 - u_p Dp_1\right)}}{p}\right) = 1 > -1$, следовательно, $x_{p,1} = 9806599036$.

Случай 9. Значение $\left(\frac{3u_p - 2Dp_1 - 2\sqrt{2\left(u_p^2 - u_p Dp_1\right)}}{p}\right) = 1 > -1$, следовательно, $x_{p,2} = 5095880$.

Случай 10. Значение $\left(\frac{3u_p + 2Dp_1 + 2\sqrt{2\left(u_p^2 - u_p Dp_1\right)}}{p}\right) = 1 > -1$, следовательно,

$x_{p,3} = 582204886811627398953667181063826 7 \backslash$
$097949379411788469840351892979710336521 4 \backslash$
$336837621256506667354270598276722855250 2 \backslash$
$620435125645115400977068048086871436515 0 \backslash$
$160769633942417620111823705220473250188 1 \backslash$
17804.

Случай 11. Значение $\left(\frac{3u_p + 2Dp_1 - 2\sqrt{2\left(u_p^2 - u_p Dp_1\right)}}{p}\right) = 1 > -1$, следовательно,

$x_{p,4} = 164409773623254797907334362127653 41 \backslash$
$958987588235769396807037859594206730428 6 \backslash$
$736752425130133347085411965534457105005 2 \backslash$
$408702512902308019541360961737428730300 3 \backslash$
$215392678848352402236474104409464807732 2 \backslash$
6029.

Теперь найдем множество значений x_q, используя алгоритм 2:

$Dq_1 = 24221077401465343319690312311378027 \backslash$
$359773647491181328940537963216874241 4248 \backslash$
$951154404197946425426748358550368934035 4 \backslash$

536559664876559233611621195254864771215 2 \
325140640359470386125487230752782994381 7 \
7856;

$Dq_{21} = 8\left(u_q^2 - u_q Dq_1\right) = 96069464117077960336$,

$\left(\frac{a}{q}\right) = -1$.

Так как $Dq_1 \neq 0$, $u_q \neq 0$, $\left(\frac{a}{q}\right) = -1$, то подходят только случаи 8-11.

Случай 8. Значение

$$\left(\frac{3u_q - 2Dq_1 + 2\sqrt{2\left(u_q^2 - u_q Dq_1\right)}}{q}\right) = 1 > -1,$$ следовательно, $x_{q,1} = 9806599036$.

Случай 9. Значение

$$\left(\frac{3u_q - 2Dq_1 - 2\sqrt{2\left(u_q^2 - u_q Dq_1\right)}}{q}\right) = 1 > -1,$$ следовательно, $x_{q,2} = 5095880$.

Случай 10. Значение

$$\left(\frac{3u_q + 2Dq_1 + 2\sqrt{2\left(u_q^2 - u_q Dq_1\right)}}{q}\right) = 1 > -1,$$ следовательно,

$x_{q,3} = 484421548029306866393806246227560 54 \backslash$
$719547294982362657881075926433748482849 7 \backslash$
$902308808395892850853496717100737868070 9 \backslash$
$073119329753118467223242390509729542430 4 \backslash$
$650281280718940772250974461505566086829 5 \backslash$
4748.

Случай 11. Значение

$$\left(\frac{3u_q + 2Dq_1 - 2\sqrt{2\left(u_q^2 - u_q Dq_1\right)}}{q}\right) = 1 > -1,$$ следовательно,

$x_{q,4} = 484421548029306866393806246227560 54 \backslash$
$719547294982362657881075926433748482849 7 \backslash$
$902308808395892850853496717100737868070 9 \backslash$
$073119329753118467223242390509729542430 4 \backslash$
$650281280718940772250974461505565988814 5 \backslash$
1592.

Найдем значение $SHA\left(P_{x,i,j} = \left(x_{p,i}, x_{a,i}\right)\right)$ и будем сравнивать его со значением $SHA\left(P_x\right)$:

$m = q\left(q^{-1} \bmod p\right) = 925 \cdot 10^{195} + 3022,$

$k = p\left(p \bmod q\right) = 75 \cdot 10^{195} + 248,$

$P_{x,i,j} = m \cdot x_{p,i} + k \cdot x_{q,j},$

$P_{x,1,1} = 9806599036,$

$SHA\left(P_{x,1,1}\right) = a202c5ffe71423606ee6f458b8173cd \backslash$
$2bcf11fe40733244e6c16198cf9fa6939 \neq SHA\left(P_x\right),$

$P_{x,1,2} = 3 \cdot 10^{396} + 2450395511 \cdot 10^{197} +$
$+ 810347610493,$

$SHA\left(P_{x,1,2}\right) = 895ff7bed3ed858578285af7add4bc5 \backslash$
$32049a5dd8e4f0126ccbd5bb27683eb43 \neq SHA\left(P_x\right)$

$P_{x,1,3} = 387889461299267328340154843844310 9 \backslash$
$863201131762544093355297310183915628792 8 \backslash$
$755244227979010267872866258207248155329 8 \backslash$
$227317201675617203831941894023725676143 9 \backslash$
$238374296798202648069372563846236085028 0 \backslash$
$936972348700647063616872858748393639923 0 \backslash$
$780974682315529917563123708523592663243 3 \backslash$
$828928074265451406540655630797234625308 6 \backslash$
$452978742414049189541677755117839621991 7 \backslash$
$688276397280512426401660856532897965845 6 \backslash$
7846.

$SHA\left(P_{x,1,3}\right) = bf5320fdef323284a59761dd764c8a \backslash$
$6445fddcd131803e92ac89404bc3a52fa1 \neq SHA\left(P_x\right)$

$P_{x,1,4} = 687889461299267328340154843844310 \backslash$
$986320113176254409335529731018391562879 \backslash$
$287552442279790102678728662582072481553 \backslash$
$298227317201675617203831941894023725676 \backslash$
$143923837429679820264806937256384623608 \backslash$
$527313324833487006470636168728587483936 \backslash$
$399230780974682315529917563123708523592 \backslash$
$663243382892807426545140654065563079723 \backslash$
$462530864529787424140491895416777551178 \backslash$
$396219917688276397280512426401660856532 \backslash$
90597125579303,

$SHA\left(P_{x,1,4}\right) = e3b0c44298fc1c149afbf4c8996fb92 \backslash$
$427ae41e4649b934ca495991b7852b855 \neq SHA\left(P_x\right)$

$P_{x,2,1} = 7 \cdot 10^{397} - 2450329771 \cdot 10^{197} -$
$- 800525111608,$

$SHA\left(P_{x,2,1}\right) = 8159db4adad129289d66539b7be447 \backslash$
$6df30df85af98267eef0d5c7b2b6776d9d \neq SHA\left(P_x\right)$

$P_{x,2,2} = 5095880,$

$SHA\left(P_{x,2,2}\right) = 087be4bb71ba1ab1ce903d1e1b75f9 \backslash$
$0bee9991ec724d269faf9e5d202c96a784 = SHA\left(P_x\right).$

Значит, искомое значение $P_x = 5095880$.

Найдем искомое значение P_y. Так как y_p равно 504767297520 или $p - 504767297520$, проверка на равенство $2\left(x_p, y_p\right) = \left(u_p, v_p\right)$. Так как выполняет-

ся равенство $2(5095880,504767297520) = (u_p, v_p)$, то $y_p = 504767297520$.

Аналогично находим, что $y_q = 504767297520$, следовательно,

$$P_y = (m \ \ y_p + k \ \ y_q) \bmod n = 504767297520.$$

Значит, искомая точка имеет координаты $P = (5095880,\ 504767297520)$

Восстанавливаем исходное сообщение из точки, используя алгоритм [4], получаем

$$M = (0,0,1,0,0,1,1,0,1,1,1,0,0,0,0,0,1,1,1,0).$$

Выводы

В статье предложен вариант построения криптосистемы Рабина на точках эллиптической кривой. Разработан алгоритм, эффективно вычисляющий значения исходного текста. Устранен недостаток криптосистемы Рабина, построенной над числовым конечным кольцом, за счет применения хеш-функций.

Литература

1. Menezes A., Van Oorchot P., Vanstone S. Handbook of applied cryptography. CRC Press, 1997. – 816 p.
2. Ростовцев А.Г., Маховенко Е.Б. Два подхода к логарифмированию на эллиптической кривой. http://www.ssl.stu.neva.ru/ssl/archieve/lift1.pdf
3. Koblitz N. A Course in Number Theory and Cryptography. Berlin: Springer-Verlag, 1987. – 208 p.
4. Червяков Н.И., Бабенко М.Г. Алгебраические подходы к разработке алгоритмов кодирования алфавита точками эллиптической кривой // Нейрокомпьютеры: разработка и применение. №9, 2010. – С. 16-26.
5. Тараканов В.Е. Свойства делимости точек эллиптических кривых над конечным полем // Труды по дискретной математике. №4, 2001. – С. 243-258.
6. Шнайер Б. Прикладная криптография: Протоколы. Алгоритмы. Исходные тексты на С. М.: Триумф, 2002. – 408 с.

RABIN'S CRYPTOSYSTEM WHICH BUILT ON THE POINTS OF ELLIPTIC CURVES

Chervaykov N.I., Babenko M.G.

Rabin's cryptosystem based on points on an elliptic curve is elaborated in the article. A method for elimination of deficiencies Rabin cryptosystem by using the properties of the hash function is suggested in this article.

Keywords: *elliptic curve, cryptosystem of Rabin on the points of an elliptic curve, factoring numbers.*

Бабенко Михаил Григорьевич, аспирант Кафедры «Высшая алгебра и геометрия» Ставропольского государственного университета (СГУ). Тел (8-8652) 38-80-84. E-mail: whbear@yandex.ru

Червяков Николай Иванович, д.т.н., профессор, заведующий Кафедрой «Прикладная математика и информатика» СГУ. Тел. (8-8652) 35-68-32, доб. 1154; 8 (8652) 35-48-61.

Поздравляем!

Члена редакционного совета, Заслуженного деятеля науки и техники Российской Федерации, доктора технических наук, профессора Николая Ивановича Червякова с 75-летием со дня рождения.

Профессор Н.И. Червяков более сорока лет отдал преподавательской деятельности – в Ставропольском высшем военном командном училище связи (впоследствии – Ставропольский военный институт связи ракетных войск), в настоящее время – в Ставропольском государственном университете, где он заведует Кафедрой «Прикладная математика и информатика». Автор более 600 научных и методических работ, основатель и бессменный руководитель научной школы «Параллельные нейрокомпьютерные технологии», которая является признанным лидером в области исследования модулярных алгебраических структур. Пятеро его учеников стали докторами, более 60 – кандидатами технических и физико-математических наук.

Почетный работник высшего профессионального образования РФ, почетный профессор СГУ, действительный член Международной академии информатизации. Награжден орденом и медалями СССР и России, является многократным победителем конкурсов на участие в Федеральных целевых программах.

Уважаемый Николай Иванович!

Желаем Вам и всем Вашим близким, а также многочисленным ученикам и последователям, крепкого здоровья, творческих успехов, семейного счастья, финансового благополучия, выполнения всех проектов и планов!

Редакционный совет и редколлегия журнала ИКТ