ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 621.391

НОВАЯ КРИПТОСИСТЕМА НА ТОЧКАХ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ, ОСНОВАННАЯ НА ПРОБЛЕМЕ УПАКОВКИ РЮКЗАКА

Бабенко М.Г., Ляхов П.А., Червяков Н.И.

В статье разрабатывается криптосистема на точках эллиптической кривой, основанная на задаче упаковки рюкзака. Для построения криптосистемы используется операция спаривания точек эллиптической кривой, заданной над конечным кольцом. Все арифметические операции выполняются в системе остаточных классов.

Ключевые слова: криптосистема на точках эллиптической кривой, система остаточных классов, спаривание точек эллиптической кривой

Введение

Современные информационные системы требуют особого подхода к сохранению секретной информации. Это обусловлено развитием технических возможностей потенциальных нарушителей, а также появлением новых алгоритмов криптографии и криптоанализа. Криптосистемы, основанные на использовании вычислительно сложной задачи упаковки рюкзака, обладают высокой скоростью шифрования информации, однако у них есть существенный недостаток. В большинстве случаев такие криптосистемы уязвимы для анализа с помощью алгоритма LLL, который аппроксимирует решение, являющееся кратчайшим вектором, содержащимся в решетке предполагаемых решений. Цель статьи – разработка криптосистемы упаковки рюкзака на точках эллиптической кривой над кольцом вычетов.

Билинейное спаривание

Для построения криптосистемы введем операцию спаривание на эллиптической кривой аналогичную работе [1]. Для любой точки $P \in E\left(GF\left(p_i\right)\right)$ выполняется следующие равенство $\left(n_i+1\right)P = O$, где O – точка в бесконечности. Обозначим за $E\left(\overline{Z}_q\right)$ множество точек эллиптической кривой, которая задана уравнением $y^2 = x^3 + ax + b$, над расширенными полями $GF\left(p_i^k\right)$. Для построения спаривания важно знать структуру группы точек эллиптической кривой. Ниже приведена теорема, описывающая структуру группы, когда эллиптическая кривая задана над полем $GF\left(p_i^k\right)$, где p_i – простое число, $k \geq 1$ и порядок группы точек эллиптической кривой выражается формулой $\#E\left(GF\left(p_i^k\right)\right) = p_i^k + 1 - t$.

Теорема 1 [2]. Если $t^2 = p_i^k, 2p_i^k, 3p_i^k$, то группа циклическая. Если $t^2 = 4p_i^k$, то группа изоморфна $Z_{\sqrt{p_i^k}-1} \oplus Z_{\sqrt{p_i^k}-1}$ в случае $t = 2\sqrt{p_i^k}$ или изоморфна $Z_{\sqrt{p_i^k}+1} \oplus Z_{\sqrt{p_i^k}+1}$ в случае $t = -2\sqrt{p_i^k}$. Если $t = 0$, $p_i^k \neq 3 \pmod 4$, то группа циклическая. Если $t - 0$, $p_i^k \equiv 3 \pmod 4$, то группа или циклическая, или изоморфна $Z_{\frac{p_i^k+1}{2}} \oplus Z_2$.

Из теоремы 1 следует, что в случае, когда $t^2 = 4p_i^k$ и r – четное число, группа точек $E\left(GF\left(p_i^k\right)\right)$ представляется в виде прямой суммы $Z_{\sqrt{p_i^k}-1} \oplus Z_{\sqrt{p_i^k}-1}$ или $Z_{\sqrt{p_i^k}+1} \oplus Z_{\sqrt{p_i^k}+1}$. Обозначим эти группы $E\left[l_i\right]$, где $l_i = \sqrt{p_i^k} - 1$ или $l_i = \sqrt{p_i^k} + 1$.

Так как $E\left[l_i\right]$ представляется в виде прямой суммы циклических групп, то можно зафиксировать некоторую образующую пару точек G_i и H_i таким образом, чтобы любую точку в $E\left[l_i\right]$ можно было представить с помощью них. Рассмотрим точки $P_i = a_{1,i}G_i + b_{1\,i}H_i$ и $Q_i = a_{2.i}G_i + b_{2.i}H_i$, принадлежавшие $E\left[l_i\right]$, где $a_{1,i}, a_{2,i}, b_{1,i}, b_{2,i} \in \left[0, l_i - 1\right]$. Для некоторых зафиксированных целых $\alpha_i, \beta_i \in \left[0, l_i - 1\right]$ определим функцию следующим образом

$$L_{\alpha_i,\beta_i} : E\left[l_i\right] \times E\left[l_i\right] \to E\left[l_i\right],$$
$$L_{\alpha_i,\beta_i}\left(P_i, Q_i\right) = \left(a_{1,i}, b_{1,i} - a_{2,i}b_{2,i}\right)\left(\alpha_i G_i + \beta_i H_i\right),$$

исключая тривиальный случай, когда α_i и β_i одновременно равны нулю.

Пусть G_1, G_2 и G_3 – три Абелевы группы. Билинейное спаривание является отображением $e : G_1 \times G_2 \to G_3$ среди этих трех групп, и отображение должно удовлетворять свойству билинейности: для

$$\alpha,\beta \in G_1,\ \gamma,\delta \in G_2,$$
$$e(\alpha+\beta,\gamma)=e(\alpha,\gamma)+e(\beta,\gamma),$$
$$e(\alpha,\gamma+\delta)=e(\alpha,\gamma)+e(\alpha,\delta).$$

Следующая теорема показывает, что функция L_{α_i,β_i} задает билинейное спаривание.

Теорема 2 [1]. Функция L_{α_i,β_i} обладает следующими свойствами.

1. Тождественность:
для всех $P_i \in E[l_i]$, $L_{\alpha_i,\beta_i}(P_i,P_i)=O$.

2. Билинейность:
для всех $P_i,Q_i,R_i \in E[l_i]$,
$L_{\alpha_i,\beta_i}(P_i+Q_i,R_i)=L_{\alpha_i,\beta_i}(P_i,R_i)+L_{\alpha_i,\beta_i}(Q_i,R_i)$ и
$L_{\alpha_i,\beta_i}(P_i,Q_i+R_i)=L_{\alpha_i,\beta_i}(P_i,Q_i)+L_{\alpha_i,\beta_i}(P_i,R_i)$.

3. Антисимметричность:
для любых $P_i,Q_i \in E[l_i]$,
$L_{a_i,\beta_i}(P_i,Q_i)=-L_{\alpha_i,\beta_i}(Q_i,P_i)$.

4. Невырожденность:
для всех $P_i \in E[l_i]$, $L_{\alpha_i,\beta_i}(P_i,O)=O$, кроме того, если $L_{\alpha_i,\beta_i}(P_i,Q)=O$ для всех $Q_i \in E[l_i]$, тогда $P_i=O$.

L_{α_i,β_i} называется спариванием, поскольку оно отображает $E[l_i]\times E[l_i]$ в $E[l_i]$ (аналогично традиционным спариваниям Вейля и Тейта).

Пусть $L_{\alpha,\beta}(P,Q)=L \in E(Z_{q^k})$ и $L_{\alpha_i,\beta_i}(P_i,Q_i)=L_i \in E(GF(p_i^k))$. Зададим спаривания $L_{\alpha.\beta}(P,Q)$ как $X_{L_i} \equiv X_L \bmod p_i$, $Y_{L_i} \equiv Y_L \bmod p_i$, $Z_{L_i} \equiv Z_L \bmod p_i$ с помощью множества точек G_i, H_i и целых чисел

$$\alpha_i,b_i \in [1,...,l_i-1], \text{ где } L=(X_L:Y_L:Z_L),$$
$$L_i=(X_{L_i}:Y_{L_i}:Z_{L_i}),\ P=(X_P:Y_P:Z_P),$$
$$Q=(X_Q:Y_Q:Z_Q)\in Z_{q^k},\ P_i(X_{P_1}:Y_{P_i}:Z_{P_i}),$$
$$Q(X_{Q_i}:Y_{Q_i}:Z_{Q_i})\in GF(p_i^k),\ X_{P_i} \equiv X_P \bmod p_i,$$
$$Y_{P_i} \equiv Y_p \bmod p_i,\ Z_{P_i} \equiv Z_P \bmod p_i,$$
$$X_{Q_i} \equiv X_Q \bmod p_i,\ Y_{Q_i} \equiv Y_Q \bmod p_i,$$
$$Z_{Q_i} \equiv Z_Q \bmod p_i \text{ и } i=1..s$$

Замечание. Значения X_L, Y_L, Z_L представляются в системе остаточных классов числами X_{L_i}, Y_{L_i}, Z_{L_i} по основаниям p_i.

Приведем пример построения билинейного спаривания.

Пример 1. Пусть задана эллиптическая кривая $E(F_5)$: $y^2=x^3+3x+4$ и $F_{5^2}=F_5/(\alpha^2+\alpha+1)$, тогда $\#E(F_{p^2})=27$ имеет восемь торсионных точек третьего порядка: $(-1,\pm(\alpha+3))$, $(2,\pm 2)$, $(\alpha,\pm\alpha)$, $(4\alpha+4,\pm(\alpha+1))$. Билинейное спаривание можно задать с помощью следующих точек $G=(2,2)$ и $H=(\alpha,\alpha)$,

$$0G+0H=0;\quad 1G+0H=(2,2);$$
$$2G+0H=(2,-2);\quad 0G+1H=(\alpha,\alpha);$$
$$1G+1H=(4+4\alpha,1+\alpha);$$
$$2G+1H=(-1,-\alpha-3);\quad 0G+2H=(\alpha,-\alpha);$$
$$1G+2H(-1,\alpha+3);\quad 2G+2H=(4+4\alpha,4+4\alpha),$$

что изоморфно $Z_3 \otimes Z_3$. Из определения следует что $e(P,Q)=e(Q,P)^{-1}$.

Процесс генерации ключей

Пусть E, заданной уравнением в форме Вейерштрассе $y^2=x^3+ax+b$, над Z_q, где $a,b \in Z_q$, $q=\prod_{i=1}^{s} p_i$, p_i – различные простые числа и для всех $i=1,...,s$ выполняется следующее условие: $3<p_i<10^6$ и $q>2^{1024}$.

Числа p_i выбираются так, чтобы было большое простое число n в 160 бит или более в факторизации на простые числа порядка эллиптической кривой $\#E(F_q)$.

Далее, мы выбираем случайное число k $k \in N$. Однако следующая супервозрастающая последовательность $a_i=k\cdot 2^{i-1}$, $(i=1,2,3,...,ur)$, k выбирается так, чтобы удовлетворяла следующему условию $\sum_{i=1}^{ur}(k\cdot 2^{i-1})<\frac{n-1}{2}$.

Рациональные точки $a_iP(i=1,2,3,...,ur)$ являются открытым публичным вектором рюкзака. Однако, как описано ниже, расшифровка эффективна, сообщаем каждому шифротексту u сумму r рациональных точек a_iP. Следовательно, количество a_i равно ur. Здесь мы имеем $ur>100$, так что шифротексты могут иметь допуск достаточно грубой силы нападения.

Затем рациональные точки a_1P, … , $a_{ur}P$, эллиптической кривой $E(F_n)$, произвольная точка $R(\neq a_1P,...,a_{ur}P)\in E(F_p)[n]$ и $S=dR$, где $d \in Z_n$ случайно взятое публичное открытое.

Затем для каждого $C_i(i=1,...,u)$, которое передается в качестве шифротекста, функция расшифровки задается следующим образом. Сначала вычисляется $b_{11}=e(P,Q)^k$ и вычисляем $b_{1j}=(e(P.Q)^k)^j$ $(j=2,3,...,2^{r-1})$. В дальнейшем b_{ij} вычисляется по схеме:

$$b_{2j}=(b_{1j})^{2^r}=\left((e(P,Q)^k)^j\right)^{2^r}=\left((e(P,Q)^k)^{2^r}\right)^j,$$

$$b_{3j} = \left(b_{2j}\right)^{2^r} = \left(\left(\left(e(P,Q)^k\right)^{2^r}\right)^j\right)^{2^r} = \left(\left(e(P,Q)^k\right)^{2^{2r}}\right)^j,$$

$$b_{uj} = \left(b_{u-1,j}\right)^{2^r} = \left(\left(e(P,Q)^k\right)^{2^{(n-1)r}}\right)^j.$$

Процедура вычислений: сначала определяются $b_{i1} = b_{i-1,i}^{2^r} \quad (i = 2,3,...,u)$, затем $b_{ij} = b_{i,j-1}b_{i1}$ $\left(i = 1,..., u,\ j = 2,3,..., 2^{r-1}\right)$. В завершение мы находим многочлен как

$$f(x) = (x - b_{i1})\cdots(x - b_{i2^{r-1}})(x-1)\ \ (i = 1,...,n).$$

Публичный ключ и секретный ключ задаются следующим образом.

Публичный ключ:

$$a_1P,\ldots,a_{ur}P,\ E(F_p),\ R,\ S,\ r$$

Секретный ключ:

$$d,\ f_1(x),\ e(P,Q),\ a_0,\ \ldots,\ a_{ur},\ Q$$

Алгоритм 1. Шифрования для криптосистемы упаковки рюкзака на эллиптической кривой

Вход. Двоичный вектор $M = (m_1, m_2, ..., m_{ut})$, $m_i \in (0,1)$, $(i = 1,2,...,ur)$, Публичный ключ $a_1P,\ldots,a_{ur}P$, $E(F_p)$, R, S, r.

Выход. Шифротекст C, C, C_{11}, C_{12}, …, $C_{u-1,1}$, $C_{u-1,2}$.

1. $C = O$

2. Для $i = 1$ до ur выполнять следующие действие:

2.1. $C = C + m_i(a_iP)$.

3. Для $i = 0$ до $u-2$ выполнять следующие действие:

3.1 $C_i = O$.

3.2. Для $j = 1$ до r выполнять следующие действия: $C_{i+1} = C_i + m_{r\cdot i+j}(a_{r\cdot i}P)$.

4. Генерируются случайно числа $t_1, t_2, ..., t_{u-1}$.

5. Для $i = 1$ до $u-1$ выполнять следующие действия:

5.1. $C_{i.1} = t_iR$,

5.2. $C_{i,2} = C_1 + t_1S$ ..

6. Вывод C, C_{11}, C_{12}, …, $C_{u-1,1}$, $C_{u-1,2}$

Алгоритм 2. Дешифрование для криптосистемы упаковки рюкзака на эллиптической кривой.

Вход. Шифротекст C, C_{11}, C_{12}, …, $C_{u-1,1}$, $C_{u-1,2}$ и d, $f_1(x)$, $e(P,Q)$, a_0, , a_1, …, a_{ur}.

Выход. Двоичный вектор M

1. Для $i = 1$ до $u-1$ выполнять следующие действия: $C_i = C_{i,2} - dC_{i,1}$.

2. $y = e(C,Q)$,

3. Для $i = 1$ до $u-1$ выполнять следующие действия:

3.1. $x = e(C_i, Q)$,

3.2. $y = y / x$.

3.3. Для $j = 0$ до $r-1$ выполнять следующие действия:

3.3.1.Если $f_1\left(x / e(P,Q)^{a_{ri-j}}\right) = 0$, то $m_{ri-j} = 1$, $x = x / e_i^{a_{ri-j-1}}$, иначе $m_{ri-j} = 0$

4. Для $j = 0$ до $r-1$ выполнять следующие действия:

4.3.1.Если $f_1\left(y / e(P,Q)^{a_{ur-j}}\right) = 0$, то

4.3.1.1. $m_{ur-i} = 1$,

4.3.1.2 $x = x / e_i^{a_{ur-j-1}}$,

иначе $m_{ur-j} = 0$.

5. Вывод M.

Действие расшифровки

Во-первых, объясним расшифровку C_1: пусть

$$\begin{aligned}
&Y = e(C_1,Q)/e(P,Q)^{a_r} = \\
&= e\left(m_1(a_1P) + \ldots + m_r(a_rP), Q\right)/e(a_rP,Q) = \\
&= e\left(m_1(a_1P) + \ldots + m_r(a_rP) - a_rP, Q\right) = \\
&= e\left((m_1a_1 + \ldots + m_ra_r - a_r)P, Q\right) = \\
&= e\left(k\left(m_1 + \ldots + m_r2^{r-1} - 2^{r-1}\right)P, Q\right) = \\
&= \left(e(P,Q)\right)^{\left(m_1+\ldots+m_r2^{r-1}-2^{r-1}\right)}.
\end{aligned}$$

Если $m_1 + \ldots + m_r2^{r-1} - 2^{r-1} \geq 0$, мы называем это положительное значение спариванием. В противном случае мы называем его отрицательным значением спаривания. В уравнении $b_{ij} = \left(e(P,Q)^k\right)^j \quad \left(j = 1,2,3,...,2^{r-1}\right)$ b_{1j} все значения различны потому, что $k\cdot 2^{r-1} < \frac{n-1}{2} < n$, и значение спаривания определяется единственным образом. C вида $1,2,...,2^{r-1}$ «супервозрастает», так как $1 + 2 + \ldots + 2^{r-2} < 2^{r-1}$, следовательно, $m_1 + \ldots + m_r2^{r-1} - 2^{r-1} < 2^{r-1}$.

Если $m_r = 1$, тогда $f_1(Y) = 0$, потому что спаривание имеет положительное значение, равное одному b_{1j}. В противном случае $f_1(Y) \neq 0$, потому что спаривание Y имеет отрицательное значение, не равное любому b_{1j}. Повторяя процесс, мы дешифруем C_i от m_r к m_1.

Аналогичным образом мы можем расшифровать C_i. Пусть

$$\begin{aligned}
&Y = e(C_i,Q)/e(P,Q)^{a_{ir}} = \\
&= e\left(m_{(i-1)r+1}\left(a_{(i-1)r+1}P\right) + \ldots + m_{ir}(a_{ir}P), Q\right)/e(a_{ir}P,Q) = \\
&= e\left(m_{(i-1)r+1}\left(a_{(i-1)r+1}P\right) + \ldots + m_{ir}(a_{ir}P) - a_{ir}P, Q\right) = \\
&- e\left(\left(m_{(i-1)r+!}a_{(i-1)r+1} + \ldots + m_{ir}a_{ir} - a_{ir}\right)P, Q\right) = \\
&e\left(k\left(m_{(i-1)r+1}2^{(i-1)r} + \ldots + m_{ir}2^{ir-1} - 2^{ir-1}\right)P, Q\right) = \\
&= \left(e(P,Q)^k\right)^{m_{(i-1)r+1}2^{(i-1)r}+\ldots+m_{ir}2^{ir-1}-2^{ir-1}} = \\
&= \left(e(P,Q)^k\right)^{2^{(i-1)}\left(m_{(i-1)r+1}+\ldots+m_{ir}2^{r-1}-2^{r-1}\right)}.
\end{aligned}$$

Поскольку $b_{ij} = \left(\left(e(P,Q)^k \right)^{2^{(i-1)r}} \right)^j$, то $\left(j = 1, 2, 3, ..., 2^{r-1} \right)$. Если $m_{ir} = 1$, то $f_i(Y) = 0$, потому что Y является положительным значением спаривания и равно одному из b_{ij}. В противном случае $f_i(Y) \neq 0$, потому что Y есть отрицательное значение спаривания и не равно любому b_{ij}. Повторяя этот процесс, дешифруем C_i из m_{ir} с $m_{(i-1)r+1}$. В итоге получим

$$X_u = e(C,Q)/(e(C_1,Q)...e(C_{u-1},Q)) =$$
$$= e(C - C_1 - ... - C_{u-1}, Q) = e(C_u, Q),$$

то есть мы расшифровываем C_u аналогичным образом с расшифровкой C_i.

Вычислительная сложность

Вычислительная сложность спаривания равна $\log p$. В шифровании вычислительная сложность сложения на эллиптической кривой тоже полиномиальная $\log p$. В дешифровании сложность вычисления частного значения спаривания также имеет полиномиальное время, так как они вычисляются по $\bmod p$. Хотя мы судим о том, что значение спаривания положительно или отрицательно путем расшифровки функции, оно вычисляется за полиномиальное время, поскольку вычитание и умножение по $\bmod p$ рассчитывается за константу.

Исследования выполнены при поддержке гранта РФФИ 12-07-00482-а.

Заключение

Рюкзачная криптосистема на эллиптической кривой обладает следующими преимуществами относительно криптосистемы рюкзака над числами. Криптосистема не расшифровывается LLL-алгоритмом за счет использования эллиптической кривой. Шифротексты – это точки эллиптической кривой. Вычислительная сложность расшифровки – полиномиальное время с помощью функции расшифровки. Все арифметические операции с точками эллиптической кривой можно эффективно выполнять в системе остаточных классов с использованием приближенного метода [3].

Литература

1. Lee H.-S. A self-pairing map and its applications to cryptography // Applied Mathematics and Computation. 151, 2004. – P. 671-678.
2. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2006. – 328 с.
3. Червяков Н.И., Бабенко М.Г., Ляхов П.А., Лавриненко И.Н. Приближенный метод ускоренного обнаружения и локализации неисправного вычислительного канала ЭВМ, функционирующей в системе остаточных классов // Нейрокомпьютеры: разработка, применение. №10, 2011. – С. 13-19.

NEW CRYPTOSYSTEMS ON ELLIPTIC CURVE POINTS BASED ON THE PACKAGE KNAPSACKS DIFFICULTY

Babenko M.G., Lyakhov P.A., Chervyakov N.I.

In the paper we develop a cryptosystem on the points of an elliptic curve, based on the package knapsacks difficulty. To construct a cryptosystem uses the pairing operation of the elliptic curve defined over a finite ring. All arithmetic operations are performed in the residue number system.

Keywords: *cryptosystem on the elliptic curve points, residue number system, pairing of the elliptic curve points.*

Бабенко Михаил Григорьевич, к.ф-м.н., доцент Кафедры «Высшая алгебра и геометрия» (ВАГ) Северо-Кавказского федерального университета (СКФУ). Тел. (8-865) 238-80-84. E-mail: whbear@yandex.ru

Ляхов Павел Алексеевич, старший преподаватель Кафедры ВАГ СКФУ. Тел. (8-879) 377-89-27; 8-962-028-72-14. E-mail: ljahov@mail.ru

Червяков Николай Иванович, Заслуженный деятель науки и техники РФ, доктор технических наук, профессор Кафедры «Прикладная математика и информатика» Ставропольского государственного университета. Тел. (8-865) 275-35-64. E-mail: kfmf-primath@stavsu.ru