УДК 621.391

КАСКАДНЫЙ АЛГОРИТМ LWE-E АЛГЕБРАИЧЕСКИХ РЕШЕТЧАТЫХ КОДОВ И ЭЛЛИПТИЧЕСКИХ КРИВЫХ

М.А. АЛИСЕЕНКО, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 7 ноября 2020

Аннотация. Рассмотрены алгебраические решетки, криптосистема обучения с ошибками и свойства эллиптических кривых. Показан алгоритм кодирования на основе криптосистемы обучения с ошибками и эллиптических кривых. Приведено моделирование алгоритма LWE-E.

Ключевые слова: алгебраические решетки, криптосистема обучения с ошибками, эллиптические кривые.

Введение

Одной из задач разработки алгоритмов защиты данных является их потенциальная способность противостоять различного вида атакам, в том числе на основе пост-квантовых и параллельных вычислений.

Одним их методов решения задач такого рода является применение алгоритмов теории решеток, позволяющих создавать пространственно- временные многообразия кодовых структур и криптографию эллиптических кривых [1–5]. В настоящей работе рассматривается каскадная схема LWE-E, сочетающая алгоритмы с обучением на основе теории решеток и кодированием алфавита точками эллиптической кривой.

Криптосистема обучения с ошибками LWE

N-мерная целочисленная решетка $\mathbb{Z}^m$ – это решетка в евклидовом пространстве $\mathbb{R}^n$, точки которой являются *n*-кортежами целых чисел. Целочисленная решетка является нечетной унимодулярной решеткой [1–3].

Решетка может быть выражена через порождающую матрицу и целочисленный коэффициент аналогично линейным кодам. Под кратчайшим вектором решетки понимается наименьший радиус окружности, которая соединяет ближайшие точки от выбранной центральной точки. Решетчатая криптография относится к набору криптографических конструкций, которые относятся к дискретной аддитивной подгруппе. Среди особенностей решетчатой криптографии – квантовая безопасность, полностью гомоморфное шифрование.

Для того, чтобы решетки с высоким коэффициентом выигрыша от кодирования были применимы на практике, они должны удовлетворять ограничению по мощности [3]. В области решетки ограничение по мощности обеспечивается выбором набора кодирующих точек решетки, которые находятся в области формирования. Сложность области формирования возрастает с увеличением размерности решетки.

Криптосистема строится на основе решеток, поддерживается теоретическим доказательством безопасности. LWE (Learning with errors) параметризуется целыми числами n, m, l, t, r, q и распределением вероятностей χ над $\mathbb{Z}_q$. Функция χ обычно принимается как округленное нормальное распределение.

1. Алгоритм генерация ключа LWE.

Вход: $LWE = n,\ m,\ l,\ q$ – целые числа.

1.1. Выбрать $S \in \mathbb{Z}_q^{n\times l}$ случайным образом.

1.2. Выбрать $A \in \mathbb{Z}_q^{m\times n}$ случайным образом.

1.3. Выбрать $E \in \mathbb{Z}_q^{m\times l}$ согласно χ.

1.4. Вычислить $P = AS + E(\mathrm{mod}\, q)$, где $P \in \mathbb{Z}_q^{m\times l}$.

Выход: закрытый ключ S и открытый ключ $(A;P)$.

2. Алгоритм шифрования.

Вход: целые числа $n,\ m,\ l,\ t,\ r,\ q$, открытый ключ $(A;P)$, открытый текст $M \in \mathbb{Z}_t^{l\times 1}$.

2.1. Выбрать $a \in [-r,r]^{m\times 1}$ случайным образом.

2.2. Вычислить $A^T a(\mathrm{mod}\, q) \in \mathbb{Z}_q^{n\times 1}$.

2.3. Вычислить $c = P^T a + [Mq/t](\mathrm{mod}\, q) \in \mathbb{Z}_q^{l\times 1}$.

Выход: шифротекст (u,c).

3. Алгоритм расшифрования.

Вход: целые $n,\ m,\ l,\ t,\ r,\ q$, секретный ключ S, шифротекст (u,c).

3.1. Вычислить $v = c - S^T u$ и $M = [tv/q]$.

Выход: открытый текст M.

Криптосистемы на основе эллиптических кривых

Применение эллиптических кривых обеспечивает существенно более высокую стойкость при равной трудоемкости или существенно меньшую трудоемкость при равной стоимости. Для вычисления обратных функций на эллиптических кривых известны только алгоритмы с экспоненциальным ростом трудоемкости [2–5].

Эллиптические кривые, заданные в канонической форме, имеют вид $y^2 = x^3 + ax^2 + bx + c$, где a, b, и c – целые коэффициенты.

Полином $P(x) = x^3 + ax^2 + bx + c$ не имеет кратных корней. Многочлен третьей степени (без кратных корней), может иметь либо один, либо три вещественных корня. По предположению, будем считать, что все эти корни различны.

Операция сложения точек на эллиптической кривой E определяется, отправляясь от графического изображения эллиптической кривой рис. 1.

На кривой E берутся две точки P и Q и проводится через них прямая. Эта прямая имеет третью точку пересечения с кривой E. Отражение этой точки от оси x образует новую точку, называемую суммой точек $(P+Q)$.

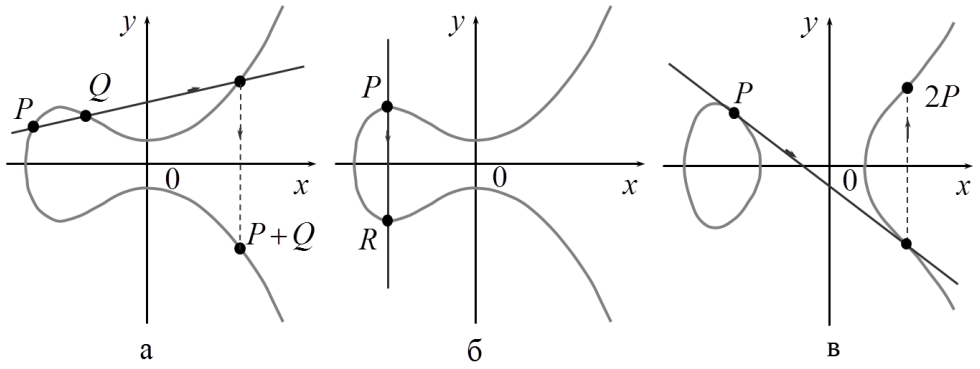

Рис. 1. Графическое изображение точек эллиптической кривой

Пусть точка P имеет координаты (x,y). Точку с координатами $(x,-y)$ будем обозначать как $-P$. Считаем, что вертикальная прямая, проходящая через P и $-P$, пересекает кривую в

бесконечно удаленной точке O, т.е. $[P+(-P)]=O$. По соглашению $P+O=O+P=P$. Точка O играет роль нуля в операциях на эллиптической кривой.

Представим, что точки P и Q сближаются друг с другом, и наконец сливаются в одну точку $P=Q$. Тогда композиция $R=P+Q=P+P$ будет получена путем проведения касательной в точке P и отражения ее второго пересечения с кривой R относительно оси абсцисс $R=P+P=2P$.

Для простого конечного поля Галуа, уравнение Вейерштрасса имеет вид $y^2=x^3+ax+b(\mathrm{mod}\,p)$, где a и b есть целые числа над конечным полем, но такие, что справедливо выражение $4a^3+27b^2\neq 0(\mathrm{mod}\,p)$.

Основной характеристикой эллиптической кривой есть ее порядок $\#E$. Под порядком эллиптической кривой понимается число различных точек на E, включая точку 0, который обозначается как $n=\#E(GF(p))$.

Ниже описаны свойства точек.

1. Сложение с нулем $P+O=O+P=P$, для всех точек $P=E(GF(p))$.

2. Для каждой точки P, существует точка $Q=E(GF(p))$, $P=(x,-y)$, такая что $P+O=O$. Точка Q называется обратным элементом и обозначается как $(-P)$.

3. Если $P=(x,-y)$, $Q=E(GF(p))$, то $(x,y)+(x,-y)=O$.

4. Абелевы группы точек, которые строятся по эллиптическим кривым, имеют одно значительное преимущество, которое объясняет их ценность для криптографии: для одного и того же большого основания p существует богатый выбор различных эллиптических кривых с разными значениями N. Эллиптические кривые составляют богатый источник «естественно возникающих» конечных абелевых групп, и это открывает большие возможности для применения в криптографии.

Операция сложения двух точек: пусть заданы две точки $Q=(x_2,y_2)\in E(GF(p))$ и $P=(x_1,y_1)\in E(GF(p))$. Сумма точек определяется как $R=P+Q=(x_3,y_3)$, где $y_3=(\lambda(x_1-y_3)-y_1)(\mathrm{mod}\,p)$, $x_3=(\lambda^2-x_1-x_2)(\mathrm{mod}\,p)$,

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}(\mathrm{mod}\,p), & \text{если } P\neq Q \ \ (x_1\neq x_2)\\ \dfrac{3x_1^{\,2}+a}{2y_1}(\mathrm{mod}\,p), & \text{если } P=Q \ \ (x_1=x_2)\end{cases}.$$

Скалярное умножение определяется для каждой точки $P\in E(GF(p))$ эллиптической кривой $E(GF(p))$ как $kP=\underbrace{P\oplus P\oplus\ldots\oplus P}_{k\ раз}$, где $k\in N$, операция $\oplus$ есть операция сложения на эллиптической кривой.

Алгоритм кодирования алфавитов открытых текстов точками эллиптической кривой

Н. Коблиц в 1985 году предложил вероятностный алгоритм представления кодирования открытых текстов. Алгоритм переводит буквы алфавита A в набор точек на эллиптической кривой. Отображение является инъективным, однако оно будет обладать тем свойством, что, зная координаты точки $P=(x_i,y_i)\in E(GF(p))$ можно однозначно восстановить какому числу i они соответствуют. Таким образом, возможен обратный процесс декодирования.

Схема криптокодирования с использованием эллиптических кривых [6].

1. Задаемся модулем эллиптической кривой p. В соответствии с условием $4a^3+27b^2\neq 0(\mathrm{mod}\,p)$ выбираем коэффициенты a и b данной эллиптической кривой.

2. Согласно формуле $p+1-2\sqrt{p}\leq m\leq p+1+2\sqrt{p}$ производим оценку порядка точек m эллиптической кривой.

3. Согласно соотношениям $m = nq,\ n \in Z,\ n \geq 1,\ 2^{254} < q < 2^{256}$ выбираем q – порядок циклической подгруппы группы точек эллиптической кривой.

4. Образующую поля, точку $P(x_p, y_p)$, выбираем исходя из соотношения $qP = 0$.

5. Выбираем случайное число k, являющееся секретным ключом данной криптосистемы.

6. Производим вычисление точки $kP = P_k(x_k, y_k)$.

7. По формуле $\alpha = \sum_{i=0}^{255} \alpha_i 2^i$ производим преобразование входного двоичного вектора в целое число α, и вычисляем точку $\alpha P = P_\alpha(x_\alpha, y_\alpha)$.

8. Вычисляем $P_k(x_k, y_k) + P_\alpha(x_\alpha, y_\alpha) = Q(x_Q, y_Q)$. Полученная точка $Q(x_Q, y_Q)$ является зашифрованным представлением исходного числа α, а величина k – секретным ключом данной криптосистемы.

9. Для расшифрования необходимо, зная секретный ключ k, получить точку $P_k(x_k, y_k)$, после чего вычислить $Q(x_Q, y_Q) - P_k(x_k, y_k) = P_\alpha(x_\alpha, y_\alpha)$.

Схема криптокодирования приведена на рис. 2.

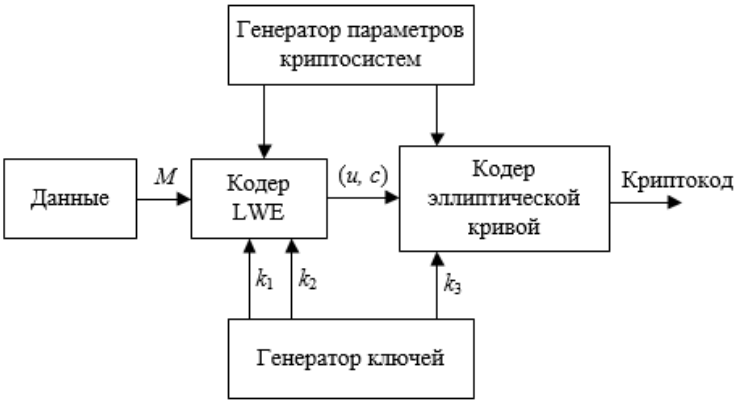

Рис. 2. Схема каскадного криптокодирования

Схема каскадного криптокодирования осуществляет последовательное преобразование информации сначала LWE системой, а затем кодером эллиптической кривой. Кодер LWE системы использует секретный ключ k_1 и открытый ключ k_2, используя для этого генератор нормального распределения. Кодер эллиптической кривой использует секретный ключ k_3, формируемый генератором случайных чисел.

Исходные данные для кодеров LWE системы и эллиптической кривой формирует генератор параметров криптосистем.

Моделирование алгоритма LWE-E

Результаты моделирования получены с помощью программного обеспечения Maple.

Открытый текст M сформируем случайным образом $M = [3\ \ 5\ \ 3\ \ 3\ \ 9\ \ 7\ \ 1]$.

1. Кодирование криптосистемой LWE.

Исходные данные $LWE = [3, 3, 6, 10, 9, 23]$. Секретный ключ формируется на основе нормального распределения randmatrix

$$S = \begin{bmatrix} 0 & 5 & 12 & 12 & 6 & 6 \\ 2 & 13 & 14 & 14 & 18 & 20 \\ 11 & 18 & 7 & 2 & 16 & 16 \end{bmatrix}.$$

Открытый ключ $(A;P)$: $A=\begin{bmatrix}2 & 4 & 4\\ 9 & 9 & 1\\ 7 & 19 & 14\end{bmatrix}$, $P=\begin{bmatrix}6 & 19 & 16 & 21 & 10 & 18\\ 6 & 19 & 11 & 15 & 2 & 20\\ 8 & 5 & 11 & 17 & 10 & 2\end{bmatrix}$

После криптокодирования LWE получим: первое слово криптокода $u=\begin{bmatrix}22 & 8 & 17\end{bmatrix}$ и второе слово криптокода $c=\begin{bmatrix}16 & 15 & 10 & 5 & 6 & 17 & 5\end{bmatrix}$.

2. Кодирование эллиптической кривой.

Найдем точки первого слова криптокода LWE $u=\begin{bmatrix}22 & 8 & 17\end{bmatrix}$. Точки имеют вид $Pu_1=\begin{bmatrix}8590 & 6540\end{bmatrix}$, $Pu_2=\begin{bmatrix}1864 & 1542\end{bmatrix}$, $Pu_3=\begin{bmatrix}9390 & 5333\end{bmatrix}$.

Для второго слова криптокода LWE $c=\begin{bmatrix}16 & 15 & 10 & 5 & 6 & 17 & 5\end{bmatrix}$ имеем множество точек: $Pc_1=\begin{bmatrix}4794 & 411\end{bmatrix}$, $Pc_2=\begin{bmatrix}5812 & 6876\end{bmatrix}$, $Pc_3=\begin{bmatrix}2395 & 7378\end{bmatrix}$, $Pc_4=\begin{bmatrix}5889 & 701\end{bmatrix}$, $Pc_5=\begin{bmatrix}6472 & 8143\end{bmatrix}$, $Pc_6=\begin{bmatrix}9390 & 5333\end{bmatrix}$, $Pc_7=\begin{bmatrix}5889 & 701\end{bmatrix}$.

В качестве примера проведем шифрование точки Pc_6: $EncrP_6=Pc_6+P_k=\begin{bmatrix}9728 & 490\end{bmatrix}$.

3. Декодирование точек криптокода осуществляется по правилу вычитания точки P_k. Проведем расшифрование точки $EncrP_6$: $DecrP_6=EncrP_6-P_k=\begin{bmatrix}9390 & 5333\end{bmatrix}$, что совпадает с точкой $Pc_6=\begin{bmatrix}9390 & 5333\end{bmatrix}$.

4. Расшифрование системой LWE для данного примера $l=\begin{bmatrix}3 & 5 & 3 & 3 & 9 & 7 & 1\end{bmatrix}$, что совпадает с исходным сообщением M.

Заключение

Исследование алгоритма LWE с кодированием алфавита точками эллиптической кривой позволяет построить трехключевые алгоритмы шифрования с мощность разнообразия, определяемой структурами многомерной решетки и эллиптических кривых, что повышает стойкость к пост-квантовым атакам. Криптосистема может быть рекомендована для защиты информации в системах связи и беспроводных сенсорных сетях.

CASCADE ALGORITHM LWE-E FOR ALGEBRAIC LATTICE CODES AND ELLIPTIC CURVES

M.A. ALISEYENKA, S.B. SALOMATIN

Abstract. Algebraic lattices, learning with errors cryptosystem and properties of elliptic curves are considered. An encoding algorithm based on learning with errors cryptosystem and elliptic curves are shown. The LWE-E algorithm is modeled.

Keywords: algebraic lattices, learning with errors cryptosystem, elliptic curves.

Список литературы

1. Ferdinand Nuwan Suresh. University of Oulu Graduate School, 2016. P. 178.
2. Olds C.D. Mathematical Association of USA, 2012. P. 192.
3. Johnson Norman W. Canadian Journal of Mathematics, 1999.
4. Stallings W. Cryptography and Network Security: Principles and Practic. Prentice-Hall, Upper Saddle River, New-Jersey, fifth edition, 2006.
5. Fadyn J.N. // Proceedings of the ICTCM 2014. P. 121–130.
6. Washington L.C. Elliptic Curves: Number Theory and Cryptography, Second Edition, CRC Press, 2008.