

Криптография на решетках

Шокуров А.В.

13 марта 2024 г.

Факторгруппы

Пусть $L = \mathcal{L}(\mathbf{B})$ — решетка ранга n и $M = \mathcal{L}(\mathbf{C})$ ее полная подрешетка. Иными словами $C = BA$ для некоторой невырожденной целочисленной матрицы A размера $n \times n$. Подрешетка M определяет отношение эквивалентности на решетке L : $x \sim_M y \Leftrightarrow x - y \in M$. Множество классов относительно этой эквивалентности обозначается через L/M . Очевидно, это отношение эквивалентности инвариантно относительно операции сложения, т.е. $x \sim_M y$ и $x' \sim_M y'$, тогда $x + x' \sim_M y + y'$ и выполняется соотношение $x + 0 \sim_M x$. Классы эквивалентности составляют абелеву группу относительно операции сложения классов. Как выбрать каноническое представление класса? Во-первых, это зависит от выбора базисов решеток L и M .

Задача. Доказать, что $L/M \simeq \mathbb{Z}^n / \mathcal{L}(A)$.

Факторгруппы

Пусть $\mathcal{P}(M)$ — основной параллелепипед решетки M

$$\mathcal{P}(M) = \{\mathbf{C}z \mid \forall i, 0 \leq z_i < 1\}.$$

Тогда для каждого класса $[x]_M$ существует $x' \in L \cap \mathcal{P}(M)$ эквивалентный x . Как получить такой элемент? Для этого представим $x = \mathbf{C}z$. Поскольку матрица \mathbf{C} невырождена, такое представление единственно. Положим $z'_i = \{z_i\}$ для всех $i = 1, \dots, n$. Тогда $x' = \mathbf{C}z'$. В частности, из правила Крамера получаем соотношение

$$|L/M| = \det M / \det L = \det \mathbf{A}.$$

Другой способ представления — использовать параллелепипед $\mathcal{P}(\mathbf{A}^*)$.

Задача. Доказать, что каждый класс из L/M имеет такое представление и это представление единственно. Построить алгоритм нахождения такого представления.

Эрмитова нормальная форма

Определение

Квадратная невырожденная матрица $A \in \mathbb{Z}^{n \times n}$ называется Эрмитовой, если

- **A** верхняя треугольная матрица, т.е. $a_{i,j} = 0$ для всех $i > j$.
- Все диагональные элементы матрицы **A** строго положительны, т.е. $a_{i,i} > 0$ для всех $i = 1, \dots, n$.
- Все недиагональные элементы приведены по модулю соответствующего диагонального элемента в той же строке, т.е. $0 \leq a_{i,j} < a_{i,i}$ для всех $i < j$.

Теорема

Для произвольной невырожденной целочисленной матрицы **A** существует унимодулярная матрица **U** такая, что **AU** эрмитова.

Отметим, что это означает возможность преобразования по столбцам произвольной невырожденной матрицы в эрмитову. 4/39

Эрмитова нормальная форма

Приведение к унимодулярной форме может быть выполнено за полиномиальное время. Для эффективного представления элементов группы $G = L/M$, приведем матрицу \mathbf{A} к эрмитовой форме. Далее будем теперь считать, что матрица \mathbf{A} эрмитова. Поскольку это так, то соответствующий ортогональный базис, полученный из этого процедурой ортогонализации Грамма-Шмидта, имеет вид $\mathbf{a}_i^* = a_{i,i} \mathbf{e}_i$. Тогда множество $\mathbb{Z}^n \times \mathcal{P}(\mathbf{A}^*)$ состоит из таких векторов $\mathbf{v} \in \mathbb{Z}^n$, что $0 \leq v_i < a_{i,i}$. В частности, каждая из координат может быть представлена $\log_2 a_{i,i}$ битами, а размер представления элементов группы составляет

$$\sum_{i=1}^n \log_2 a_{i,i} = \log_2 \prod_{i=1}^n a_{i,i} = \log_2 \det(\mathbf{A}) = \log_2 |G|.$$

Эрмитова нормальная форма

Специальный случай: $L = \mathbb{Z}^n$ и M произвольная целочисленная решетка. В этом случае используем обозначение $\mathbf{v} \bmod M$ для единственного представителя класса $[\mathbf{v}]_M$ относительно эрмитова базиса для M .

Нормальная форма Смита

Определение

Матрица $\mathbf{D} \in \mathbb{Z}^{n \times n}$ называется нормальной матрицей Смита, если она диагональна, ее диагональные элементы неотрицательны и $d_{i+1,i+1}$ делит $d_{i,i}$ для всех $i = 1, \dots, n$.

Теорема

Любая целочисленная квадратная матрица \mathbf{C} может быть приведена к нормальной форме по Смитту с помощью унимодулярных матриц \mathbf{U} и \mathbf{V} к матрице Смита, т.е. \mathbf{UAV} — матрица Смита. Это приведение можно выполнить за полиномиальное время.

Нормальная форма Смита

Заметим, что решетки, соответствующие матрицам \mathbf{A} и \mathbf{D} , не совпадают. Однако эти матрицы эквивалентны в том смысле, что группы $\mathbb{Z}^n / \mathcal{L}(\mathbf{A})$ и $\mathbb{Z}^n / \mathcal{L}(\mathbf{D})$ изоморфны.

Теорема

Пусть \mathbf{D} — нормальная форма матрицы \mathbf{A} . Тогда группа $G = L/M$ изоморфна аддитивной группе

$$S = \mathbb{Z}_{d_{1,1}} \oplus \dots \oplus \mathbb{Z}_{d_{n,n}}.$$

Также как в случае эрмитова представления, все элементы группы G представимы целозначными векторами $\mathbf{s} \in \mathbb{Z}^n$, для которых $0 \leq s_i < d_{i,i}$ при $i = 1, \dots, n$. Следовательно, такое представление имеет размер

$$\sum_{i=1}^n \log_2 d_{i,i} = \log_2 \det(\mathbf{A}) = \log_2 |G|.$$

Нормальная форма Смита

Поскольку операции по-компонентные, операции могут выполняться за время

$$\mathcal{O}\left(\sum_{i=1}^n \log_2 d_{i,i}\right) = \mathcal{O}(\log_2 |G|).$$

Теорема

Отображение

$$\psi : [\mathbf{x}]_M \mapsto \mathbf{D}\mathbf{C}^{-1}\mathbf{x} \bmod \mathbf{D}$$

задает изоморфизм групп S и G .

Решетки и хэш-функции

Айтаи-Гольдрейх-Гольдвассер-Хэлеви

Пусть $q \geq 2$ — целое число и \mathbf{A} случайная матрица размера $n \times m$ над кольцом \mathbb{Z}_q . Определено линейное отображение

$$f_{\mathbf{A}} : \mathbf{x} \mapsto \mathbf{Ax} \bmod q$$

из \mathbb{Z}_q^m в \mathbb{Z}_q^n . Очевидно, это отображение вычислимо, а также можно найти обратное, решив систему уравнений над \mathbb{Z}_q .

Рассмотрим теперь ограничение этой функции на множество B^m , где $B = \{0, 1\}$

$$h_{\mathbf{A}} : B^m \rightarrow \mathbb{Z}_q^n.$$

Задача нахождения коллизии $\mathbf{Ax} = \mathbf{Ay}$, где $\mathbf{x}, \mathbf{y} \in B^m$ заключается в нахождении векторов таких \mathbf{z} , что $\|\mathbf{z}\|_{\infty} = 1$ и $\mathbf{z} = \mathbf{x} - \mathbf{y}$. Отметим, что при $m > n \log_2 q$ функция $h_{\mathbf{A}}$ представляет собой хэш-функцию.

О коллизиях

Почему в этом случае найти коллизии? Оказывается, что нахождение коллизий в среднем является столь же сложной задачей, что и для задачи аппроксимации радиуса покрытия с точностью до полиномиального множителя $\gamma(n) < O(n^{2.5} \log n)$. Из этого факта и сводимости задачи нахождения радиуса покрытия к задаче нахождения кратчайшего вектора с точностью до множителя, получена сводимость задачи нахождения коллизии к задаче аппроксимации кратчайшего вектора с точностью $\gamma(n) < O(n^{3.5})$. Для "почти совершенных" решеток сводится к задаче нахождения ближайшего вектора с точностью до множителя \sqrt{n} . Задача нахождения коллизии соответствует задаче нахождения коротких векторов $\|z\|_2 \leq \sqrt{n} \|s\|_\infty = \sqrt{n}$ в решетке $L_A = \{z \mid Az \equiv 0 \pmod{q}\}$. Поэтому задачу стойкости хэш функции можно переформулировать как задачу нахождения короткого вектора в решетке в среднем и задачей аппроксимации длины кратчайшего вектора в любой решетке в худшем случае.

τ -совершенные решетки

Пусть L_n решетка полная решетка размерности n . Будем рассматривать такие решетки L , для которых существует такой алгоритм CVP_L , что на входе n и $\mathbf{t} \in \mathbb{Q}_n$ он находит ближайший к этому вектору вектор решетки L_n . Например, это решетки \mathbb{Z}^n .

Определение

Радиусом упаковки решетки называется такое наибольшее число $r = \rho(L)$, что открытые шары с центрами в точках решетки попарно не пересекаются.

Определение

Радиусом покрытия решетки называется такое наименьшее число R , что замкнутые шары с центрами в точках решетки покрывают все пространство.

τ -совершенные решетки

Определение

Положим $\tau_L = R/r = 2R/\lambda_1$, где R — радиус покрытия решетки, а r радиус упаковки. Для любого числа $\tau > 1$ будем называть решетку L τ -совершенной, если $\tau_L \leq \tau$.

Последовательность решеток L_n будем называть почти совершенной, если все решетки L_n являются τ -совершенными для некоторой постоянной величины τ , не зависящей от ранга n .

Пусть L — τ -совершенная решетка для некоторого τ от 1 до \sqrt{n} . Положим $\mathbf{c}_i = CVP_L(\alpha\rho(L)\mathbf{e}_i)$ — это точка решетки, находящаяся на расстоянии $\rho(L)$ от $\alpha\rho(L)\mathbf{e}_i$, т.е.

$$\mathbf{C} = \alpha\rho(L)\mathbf{I} + \mathbf{R},$$

где \mathbf{R} матрица, столбцы которой ограничены $\|\mathbf{r}_i\| \leq \rho(L)$. Решетки L и M определяют абелеву группу $G = L/M$.

τ -совершенные решетки

Отметим, что элементы группы G представимы $\log |G|$ битами, а операции в группе выполнимы за полиномиальное время.

Имеется также полиномиальный алгоритм вычисления гомоморфизма $\psi : L \rightarrow G$. При этом $\psi(\mathbf{x}) = 0$ тогда и только тогда, когда $\mathbf{x} \in M \subset L$.

Определим семейство хэш функций со значениями в G . Пусть m — целое. Зафиксируем последовательность из m элементов $a_1, \dots, a_m \in G$. Вектор $\mathbf{a} = (a_1, \dots, a_m)^t \in G^m$ определяет функцию $h_{\mathbf{a}} : \{0, 1\}^m \rightarrow G$ по формуле

$$h_{\mathbf{a}}(\mathbf{x}) = \sum_{i=1}^m x_i a_i = \sum_{i|x_i=1} a_i.$$

τ -совершенные решетки

При $m > \log_2 |G|$ определены хэш функции h_a и коллизии всегда существуют.

Теорема

При случайном равномерном выборе вектора $\mathbf{a} \in G^m$ задача нахождения коллизии является NP-трудной.

Теорема

Для каждого n существует τ -совершенная решетка с $\tau < 4$.

Схема шифрования GGH

(Гольдрайх-Гольдвассер-Хэлеви)

Секретный ключ. Имеется два способа.

- Строим $n \times n$ матрицу \mathbf{R} , выбирая ее элементы случайно и равномерно из множества $\{-l, \dots, l\}$.
- Строим $\mathbf{R} = k\mathbf{I} + \mathbf{R}'$, где \mathbf{R}' выбирается как в первом способе, а k — параметр, например, $k = \sqrt{nl}$.

Открытый ключ. Открытый ключ — другой базис решетки. Должен выбираться случайно из заданного распределения возможных базисов решетки. Имеется два способа.

- Первый способ — преобразование \mathbf{R} в базис \mathbf{B} с помощью некоторой последовательности операций над столбцами. В качестве коэффициентов выбираются случайно выбранные элементы из множества $\{-1, 0, 1\}$.
- Предлагается умножить исходную матрицу на последовательность унимодулярных множеств.

Схема шифрования GGH (Гольдрайх-Гольдвассер-Хэлеви)

Открытый ключ. Открытый ключ — другой базис решетки. Должен выбираться случайно из заданного распределения возможных базисов решетки. Имеется два способа.

- Первый способ — преобразование \mathbf{R} в базис \mathbf{B} с помощью некоторой последовательности операций над столбцами. В качестве коэффициентов выбираются случайно выбранные элементы из множества $\{-1, 0, 1\}$.
- Предлагается умножить исходную матрицу на последовательность унимодулярных множеств. В качестве унимодулярных матриц можно брать произведения нижней треугольной и верхней треугольной матриц. Эти матрицы имеют на диагоналях ± 1 , а вне диагонали состоят из элементов множества $\{-1, 0, 1\}$.

Схема шифрования GGN (Гольдрайх-Гольдвассер-Хэлеви)

Шифрование. На входе подается вектор \mathbf{x} и небольшой вектор возмущения (шум) \mathbf{r} . На выходе получаем $\mathbf{t} = \mathbf{B}\mathbf{x} + \mathbf{r}$.

Максимальная длина вектора \mathbf{r} указывается при задании открытого ключа. Вектор \mathbf{x} определен в достаточно большой области, поэтому $\mathbf{B}\mathbf{x}$ кажется случайным вектором решетки.

Дешифрование. Имеется два метода дешифрования.

- Первый метод — использовать алгоритм ближайшей плоскости с базисом \mathbf{R} . В соответствии с ним находится единственная точка $\mathbf{B}\mathbf{x}$ на расстоянии $\delta = (1/2) \min \|r_i^*\|$ от \mathbf{t} и восстанавливает вход $(\mathbf{x}, \mathbf{t} - \mathbf{B}\mathbf{x})$.
- Во втором случае, нужно вычислить $\mathbf{R}^{-1}\mathbf{t}$ и округлить координаты до ближайшего целого., а затем умножить результат на \mathbf{R} .

Факторкольцо

Рассмотрим кольцо $\mathbb{Z}[X]/(X^n - 1)$. Элементы этого кольца можно отождествить с многочленами с целыми коэффициентами степени не выше $n - 1$. Сложение определяется по-компонентно. Умножение задается формулой

$$\sum_{k=0}^{n-1} a_k X^k \sum_{k=0}^{n-1} b_k X^k = \sum_{k=0}^{n-1} \left(\sum_{i+j \equiv k \pmod{n}} a_i b_j \right) X^k.$$

Факторкольцо

Операции в кольце многочленов $\mathbb{Z}_q[X]/(X^n - 1)$ определяются так же, как и в кольце $\mathbb{Z}[X]/(X^n - 1)$ с той лишь разницей, что операции над коэффициентами выполняются в кольце \mathbb{Z}_q . В этом кольце имеется группа единиц.

Задача Если p — простое, то \mathbb{Z}_p — поле. Тогда многочлены $f(X) \in \mathbb{Z}_p[X]/(X^n - 1)$, для которых $\text{НОД}(f(X), X^n - 1) = 1$, лежат в группе единиц и обратный элемент можно найти с помощью алгоритма Евклида. Доказать, что этот алгоритм имеет сложность $\mathcal{O}(n^2 \log q)$.

Факторкольцо

Пусть теперь $q = p^t$, где p простое и многочлены $f(X) \in \mathbb{Z}_q[X]/(X^n - 1)$ такие, что $\text{НОД}(f(X), X^n - 1) = 1$ (Наибольший общий делитель вычисляется в кольце $\mathbb{Z}_q[X]$). Поскольку $\mathbb{Z}_q \supset \mathbb{Z}_p$ это же выполняется в кольце $\mathbb{Z}_p[X]$. В кольце $\mathbb{Z}[X]$ соотношение $\text{НОД}(f(X), X^n - 1) = 1$ также выполняется. С помощью алгоритма Евклида примененного для кольца $\mathbb{Z}_p[X]$ над полем \mathbb{Z}_p , для представителя многочлена $f(X)$ в $\mathbb{Z}[X]$ найдем многочлены $u, v, c \in \mathbb{Z}[X]$, для которых в кольце $\mathbb{Z}[X]$ выполняется равенство

$$uf + v(X^n - 1) = 1 - pc.$$

Факторкольцо

Поэтому $u * f = 1$ в $\mathbb{Z}_p[X]/(X^n - 1)$. Имеем также в кольце $\mathbb{Z}[X]$

$$\begin{aligned}(1 + pc) * u * f &= 1 - p^2 c^2 \\(1 + p^2 c^2) * (1 + pc) * u * f &= 1 - p^4 c^4 \\&\vdots\end{aligned}$$

$$(1 + p^{2^{s-1}} c^{2^{s-1}}) * \dots * (1 + p^2 c^2) * (1 + pc) * u * f = 1 - p^{2^s} c^{2^s}$$

в кольце $\mathbb{Z}[X]/(X^n - 1)$. При $2^s \geq t$ имеем

$$(1 + p^{2^{s-1}} c^{2^{s-1}}) * \dots * (1 + p^2 c^2) * (1 + pc) * u * f = 1 \pmod q$$

и, следовательно,

$$f^{-1} = (1 + p^{2^{s-1}} c^{2^{s-1}}) * \dots * (1 + p^2 c^2) * (1 + pc) * u.$$

Описание NTRU

Пусть p и q — два небольших взаимно простых числа (например, $p = 3$ и $q = 128$). (В общем случае p очень мало, а q — многочлен от параметра безопасности n .) Элементы кольца $R = \mathbb{Z}[X]/(X^n - 1)$ будем представлять многочленом или вектором в \mathbb{Z}^n вида

$$f = \sum_{i=0}^{n-1} f_i X^i = [f_0, f_1, \dots, f_{n-1}].$$

Произведение в этом кольце описывается формулой

$$f * g = [f_0, f_1, \dots, f_{n-1}] * [g_0, g_1, \dots, g_{n-1}] = [h_0, h_1, \dots, h_{n-1}],$$

где

$$h_k = \sum_{i=0}^k f_i g_{k-i} + \sum_{i=k+1}^{n-1} f_i g_{n+k-i}.$$

Описание NTRU

В кольцах $R_p = R/(p)$ и $R_q = R/(q)$ коэффициенты многочленов представляются остатками в диапазонах $[0, p - 1]$ и $[0, q - 1]$.

Рассмотрим также множество многочленов $\mathcal{P}_p(N)$, элементы которого представляются в виде

$$g = \sum_{i=0}^{N-1} g_i X^i = [g_0, g_1, \dots, g_{N-1}], \text{ где } g_p \in \left(-\frac{p}{2}, \frac{p}{2}\right].$$

Описание NTRU. Генерация ключа.

Генерация ключа. Выбираем два случайных многочлена $f \in R_1$ и $g \in R$ с маленькими коэффициентами (например, из множества $\{-1, 0, 1\}$) и взаимно простые числа p и q такие, что для многочлена f существуют обратные элементы f_p^{-1} и f_q^{-1} в кольцах $R_p = R/(p)$ и $R_q = R/(q)$. С вероятностью близкой к единице случайный многочлен f удовлетворяет этому условию. Обратные элементы f_p^{-1} и f_q^{-1} строятся с помощью алгоритма Евклида.

Затем вычисляется многочлен h в $R_q = R/(q)$

$$h \equiv pf_q^{-1} * g \pmod{q},$$

где умножение выполняется в кольце $R = \mathbb{Z}[X]/(X^N - 1)$. Открытым ключом шифрования объявляется многочлен h и числа q и p . Секретным ключом является пара f, g .

Описание NTRU. Шифрование.

Шифрование. Пусть имеется пара: текст m и случайный вектор r (предполагаем, что текст представляет собой многочлен с маленькими коэффициентами, например, -1, 0 и 1).
Зашифрованный текст t получается по формуле

$$t \equiv r * h + m \pmod{q}.$$

Описание NTRU. Дешифрация.

Дешифрация. Пусть t — шифртекст и f — секретный ключ. Сначала вычислим многочлен a по формуле

$$a \equiv f * t \pmod{q},$$

причем коэффициенты многочлена a выбираются из интервала от $-q/2$ до $q/2$. Рассматривая многочлен a как многочлен с целыми коэффициентами, вычислим многочлен $m' \in R_p$ по формуле

$$m' \equiv f_p^{-1} * a \pmod{p}.$$

Описание NTRU. Дешифрация.

В работе [Hoffstein J., Piper J., Silverman J., NTRU: A ring based public key cryptosystem, in Algebraic number theory (ANTS III), vol.1423 of Lecture Notes in Computer Science, pp. 267-288, Springer] показано, при соответствующем выборе параметров $t = a$ с большой вероятностью. Идея такова. Из определения t и h , имеем

$$a \equiv f * t \pmod{q} \equiv f * (m + r * h) \pmod{q} \equiv f * m + pgr \pmod{q}.$$

Поскольку коэффициенты многочленов f, m, g, r малы и p мало, то с вероятностью близкой к 1 коэффициенты многочлена целочисленного многочлена $fm + pgr$ лежат в интервале $[q/2, q/2]$. Тогда $a = fm + pgr$ над кольцом целых чисел и $m' \equiv f^{-1}(fm + pgr) \equiv m \pmod{p}$. Соответственно $r = (t - m)(ph)^{-1} \pmod{q}$.

Определение NTRU через решетки

Определение

Целочисленная решетка, содержащая решетку $q\mathbb{Z}^n$ называется q -модулярной.

Определение

Вектор $(x_n, x_1, \dots, x_{n-1})$ называется циркулянтном вектора $\mathbf{x} = (x_1, \dots, x_n)$ и обозначается $\mathbf{rot}(\mathbf{x})$.

Определение NTRU через решетки

Имеется следующее представление кольца $R = \mathbb{Z}[x]/(x^n - 1)$ циркулянтными матрицами. А именно, сопоставим вектору \mathbf{x} матрицу из столбцов $M_{\mathbf{x}} = (\mathbf{x}, \mathbf{rot}(\mathbf{x}), \dots, \mathbf{rot}^{n-1}(\mathbf{x}))$.

Задача. Доказать равенство $M_{\mathbf{x}}M_{\mathbf{y}} = M_{\mathbf{xy}}$.

Определение NTRU через решетки

Определение

Пусть $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ и $\mathbf{z} = (\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^{2n}$. Определим бициркулянт формулой $\mathbf{rot}_2(\mathbf{z}) = (\mathbf{rot}(\mathbf{x}), \mathbf{rot}(\mathbf{y}))$.

Определение

Целочисленная решетка \mathcal{L} размерности $2n$ называется бициклической, если из $\mathbf{x} \in \mathcal{L}$ следует, что $\mathbf{rot}_2(\mathbf{x}) \in \mathcal{L}$. Иными словами, решетка должна быть замкнута относительно бициркуляций.

Определение NTRU через решетки

Предложение

Пересечение сохраняет свойства q -модулярности и бицикличности. В частности, для любого множества векторов S определена минимальная q -модулярная бициклическая решетка, содержащая множество S .

Задача. Доказать предложение.

Определение NTRU-шифрования на решетках.

Секретный ключ.

Секретный ключ. Секретный ключ определяется коротким вектором $\mathbf{v} = (px_1, \dots, px_n, y_1, \dots, y_n)$, где $x_i, y_i \in \{-1, 0, 1\}$. Свяжем с этим вектором бициклическую q -модулярную решетку (см. предыдущее предложение). Порождающим множеством этой решетки являются бициркулянты вида $\mathbf{rot}_2^k(\mathbf{v})$ для всех $k = 0, \dots, n - 1$ и множество векторов вида qe_k , где $k = 1, \dots, 2n$.

Определение NTRU-шифрования на решетках.

Открытый ключ.

Открытый ключ. Открытый ключ определяется как эрмитов нормальный базис бициклической q -модулярной решетки, определяемой вектором v .

Определение NTRU-шифрования на решетках.

Задача. При $\mathbf{v} = (pg, f)$ (см. определение NTRU-шифрования через многочлены) выполняется равенство

$$H = \begin{pmatrix} qI & M_h \\ 0 & I \end{pmatrix}.$$

Иными словами, эта решетка определяется как минимальная бициклическая q -модулярная решетка, содержащая вектор (h, e_1) .

Определение NTRU-шифрования на решетках. Шифрование.

Шифрование. Рассмотрим вектор $(m, -r)$. При приведении этого вектора по модулю эрмитова нормального базиса H получим шифротекст $(t, 0)$, где t — многочлен из определения шифрования с помощью многочленов.

Задача. Докажите это.

Определение NTRU-шифрования на решетках.
Дешифрация.

Дешифрация. Алгоритм дешифрации не имеет геометрической интерпретации и выполняется по ранее описанным формулам.

Анализ

Анализ. Специфическая структура q -модулярных бициклических решеток позволяет представлять секретный и открытый ключ, используя только $O(n \log n)$ битов. С точки зрения эффективности NTRU-шифрование представляется хорошим методом: шифрование и дешифрация осуществляются очень быстро, также как и процедура порождения ключа шифрования быстро. Причем размер открытого ключа сопоставим с размерами широко используемых ключей в методах шифрования связанных с теорией чисел.

Анализ

Главный вопрос о стойкости этой криптосистемы остается в настоящее время открытым. Являются ли задачи на решетках такого специального вида трудными, как и в общем случае? Точное решение также NP-трудная задача? Аппроксимация также NP-трудна? Что можно сказать о трудности в среднем для этого класса решеток?

С теоретической точки зрения пока на эти вопросы ответы неизвестны. Однако эта криптосистема широко используется и хорошо себя зарекомендовала с практической точки зрения.