Криптосистема Айтаи-Дворка

Шокуров

12 марта 2025 г.

Сводимость

Теорема

Для любой функции $\gamma : \mathbb{N} \to \{\mathbb{R} | r \geq 1\}$ задача SVP_γ (соотв. $G_{AP}SVP_\gamma$) сводится по Куку к задаче CVP_γ (соотв. $G_{AP}CVP_\gamma$).

Описанная в предыдущей лекции процедура **Сводимость** выполняет это сведение по Куку.

Докажем теорему в случае задачи распознавания:
$(\mathbf{B}, r) \in G_{AP}SVP_\gamma \Leftrightarrow \exists j : (\mathbf{B}^{(j)}, \mathbf{b}_j, r) \in G_{AP}CVP_\gamma$. Другие случаи разбираются аналогично.
Пусть $(\mathbf{B}, r)$ — вход задачи $G_{AP}SVP_\gamma$. Ему соответствуют m задач $G_{AP}CVP_\gamma$ для входов $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$. Докажем, что если на входе $(\mathbf{B}, r)$ задачи $G_{AP}SVP_\gamma$ получен ответ YES, то хотя бы один ответ YES получен в последовательности результатов решения задачи $G_{AP}CVP_\gamma$ для входов $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$, а если на входе $(\mathbf{B}, r)$ задачи $G_{AP}SVP_\gamma$ получен ответ NO, то ответ NO получен для всех входов $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ для задачи $G_{AP}CVP_\gamma$.

Пусть на входе $(\mathbf{B}, r)$ задачи $G_{AP}SVP_\gamma$ получаем YES и $\mathbf{v} = \sum_{i=1}^{n} c_i \mathbf{b}_i$ — кратчайший вектор в решетке $L(\mathbf{B})$. Тогда $|\mathbf{v}| \leq r$ и, следовательно, при некотором j коэффициент c_j нечетный. Поэтому вектор $\mathbf{u} = \frac{c_j + 1}{2}(2\mathbf{b}_j) + \sum_{i \neq j}^{n} c_i \mathbf{b}_i$ принадлежит решетке $L(\mathbf{B}^{(j)})$ и выполняется $\|\mathbf{u} - \mathbf{b}_j\| = \|\mathbf{v}\| \leq r$, что означает исход YES для запроса оракула на входе $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$.

Предположим теперь, что на входе $(\mathbf{B}^{(j)}, \mathbf{b}_j, r)$ задачи $G_{AP}CVP_\gamma$ получаем YES, т.е. при некотором $\mathbf{u} \in L(\mathbf{B}^{(j)})$ выполняется соотншение $\|\mathbf{u} - \mathbf{b}_j\| \leq r$. Поэтому для ненулевого вектора $\mathbf{v} = (2c'_j - 1)\mathbf{b}_j + \sum_{i \neq j}^{n} c_i \mathbf{b}_i$ решетки $L(\mathbf{B})$ выполняются соотношения $\|\mathbf{v}\| = \|\mathbf{u} - \mathbf{b}_j\| \leq r$, что означает исход YES для запроса на входе $(\mathbf{B}, r)$ задачи $G_{AP}SVP_\gamma$.

Сведение задачи о рюкзаке к задаче нахождения кратчайшего вектора

Пусть имеется задача о рюкзаке, заданная вектором $(a_1, \ldots, a_n, s) = (\mathbf{a}, s)$. Рассмотрим решетку **L**, порожденную матрицей

$$\mathbf{L} = \begin{pmatrix} c \cdot \mathbf{a} & c \cdot s \\ 2\mathbf{I} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{B}, \mathbf{t} \end{pmatrix},$$

где c достаточно большая константа, например, большая $\sqrt{n}$, **I** — единичная матрица, а **1** — вектор-столбец из единиц. Заметим, что если $\mathbf{x} = (x_1, \ldots, x_n)$ — решение задачи о рюкзаке, тогда решетка с базисом **L** содержит вектор длины $\sqrt{n}$, который получается как сумма первых n столбцов, умноженных на компонеты вектора x, и последнего столбца, умноженного на -1. Если кратчайший (или некоторый короткий) вектор выражается через представленный базис как **Lx**, где $x_i = 0$ или $x_i = 1$ при $i = 1, \ldots, n$ и $x_{n+1} = -1$ и имеет длину не более $\sqrt{n}$, то **x** определяет решение задачи о рюкзаке.

Сведение задачи о рюкзаке к задаче нахождения кратчайшего вектора

Алгоритм решения задачи о кратчайшем векторе, предложенный Lagarias-Odlyzko:

1. Домножим коэффициенты задачи на достаточно большую константу $(c \cdot a_1, \ \ldots, c \cdot a_n, s)$.
2. Сводим задачу о рюкзаке к задаче CVP с входом $(\mathbf{B}, \mathbf{t})$.
3. Будем решать CVP задачу $(\mathbf{B}, \mathbf{t}, \sqrt{n})$, используя следующий эвристический алгоритм (в задачах криптоанализа этот алгорим назывется методом встраивания): чтобы найти ближайший к $\mathbf{t}$ вектор решетки, будем искать короткий вектор в решетке $\mathbf{L}$. Если это будет вектор вида $\mathbf{Bx} - \mathbf{t}$, то $\mathbf{Bx}$ будет коротким вектором, близким к $\mathbf{t}$.

Сведение задачи о рюкзаке к задаче нахождения кратчайшего вектора

Причина, по которой первая строка домножается на достаточно большой сомножитель c связана с тем, что не известно как точно решить задачу о кратчайшем векторе решетки. В этом случае предлагается использовать, например LLL-алгоритм. При домножении первой строки на достаточно большой коэффициент c, достаточно короткий вектор должен иметь нулевую первую координату. А также для координат короткого вектора должно выполняться соотношение $\sum a_i x_i = (-x_{n+1})s$. Нет никакой гарантии, что $x_{n+1} = -1$ и $x_i = 0$ или $x_i = -1$ при $i = 1, \ldots, n$. Однако, при случайном выборе коэффициентов a_i этот алгоритм решает задачу о рюкзаке с высокой вероятностью.

Сведение задачи о рюкзаке к задаче нахождения кратчайшего вектора

Теорема

Задача $G_{AP}SVP_1$ (задача распознавания, ассоциированная с точной задачей SVP) в l_∞ норме является NP-полной.

Доказательство.

Задача лежит в классе *NP*, поскольку на входе $(\mathbf{B}, r)$ легко выполнить прверку, что некоторый вектор *y* принадлежит решетке и имеет длину меньше *r*. Трудность следует из того, что задача о рюкзаке сводится к задаче *CVP*, а описанный выше алгоритм в случае метрики l_∞ дает кратчайший вектор с координатами 0 или 1. □

Рандомизированные сводимости

Рандомизированная сводимость — это полиномиально вычислимая вероятностная функция (машина Тьюринга)

$$f : G_{AP}SVP_{\gamma} \to G_{AP}CVP_{\gamma}.$$

- Ненадежная рандомизированная сводимость (UR-редукция). При этой редукции все входы *YES* преобразует во входы *YES*, а входы *NO* во входы *NO* с вероятностью p. Ненадежной называется по той причине, что при ответе *NO* вероятность исхода *YES* составляет $1 - p$ (ошибка в надежности). При этом требуется, чтобы на входе длины n выполнялось соотношение $1 - p \geq 1/n^c$, где константа c не зависит от n.
- Обратная ненадежная рандомизированная сводимость (RUR-редукция). В этом случае все входы *YES* преобразует во входы *YES* с вероятностью p, а входы *NO* во входы *NO*. Величина $1 - p$ называется ошибкой полноты (сводимости). При этом требуется, чтобы на входе длины n выполнялось соотношение $1 - p \geq 1/n^c$, где константа c не зависит от n.

Рандомизированные сводимости

Теорема

Для любой функции $\gamma : \mathbb{N} \to \{r \in \mathbb{R} | r \geq 1\}$ существует RUR-редукция SVP_γ (соответственно, $G_{AP}SVP_\gamma$) к CVP_γ (соответственно, $G_{AP}CVP_\gamma$) с с ошибкой полноты $1/2$. Более того, при такой сводимости сохраняются размерности и ранги исходных SVP задач.

Доказательство.

Сопоставим входу $(\mathbf{B}, r)$, где $\mathbf{B} = (\mathbf{b}_1, \ \ldots, \mathbf{b}_n)$ задачи SVP выход $(\mathbf{B}', \mathbf{b}_1, r)$, где $\mathbf{B}'$ определим так. Положим $c_1 = 1$ и выберем $c_i \in \{0, 1\}$ ($i = 2, \ \ldots, n$) как равномерно распрелеленную независимую последовательность. Для всех $i = 1, \ \ldots, n$ положим $\mathbf{b}'_i = \mathbf{b}_i + c_i\mathbf{b}_1$. Докажем, что при ответе YES на входе $(\mathbf{B}, r)$ получим ответ YES с вероятностью 1/2, а при ответе NO на втом же входе, на выходе получим NO всегда. □

Продолжение доказательства.

Начнем с ответа NO. Пусть получили, что $(\mathbf{B}', \mathbf{b}_1, r)$ не является входом со значением NO. Тогда при некотором $\mathbf{u} \in L(\mathbf{B}')$ выполняется $\|\mathbf{u} - \mathbf{b}_1\| \leq \gamma(n)r$. Поскольку $\mathbf{B}'$ подрешетка решетки $\mathbf{B}$ и $\mathbf{b}_1 \notin L(\mathbf{B}')$, вектор $\mathbf{u} - \mathbf{b}_1 \neq \mathbf{0}$ лежит в $L(\mathbf{B})$ и его длина не более $\gamma(n)r$, т.е. $(\mathbf{B}, r)$ не дает на выходе *NO*. □

Продолжение доказательства.

Пусть теперь на входе $(\mathbf{B}, r)$ получаем ответ YES и пусть $\mathbf{v} = \sum x_i \mathbf{b}_i$ — кратчайший вектор. Тогда при некотором j коэфициент x_i нечетный. Положим $\alpha = x_1 + 1 - \sum_{i>1} c_i x_i$. Если x_i четно при $i > 1$, то то x_1 нечетно и, следовательно, α четно. Если же x_i нечетно при некотором $i > 1$, то α четно с вероятностью 1/2. В обоих случаях с вероятностью не менее 1/2 α четно и вектор $\mathbf{u} = \frac{1}{2}\mathbf{b}'_1 + \sum_{i>1} x_i \mathbf{b}'_i$ принадлежит решетке $L(\mathbf{B}')$, причем

$$\begin{aligned} \mathbf{u} - \mathbf{b}_1 &= \left(\alpha \mathbf{b}_1 + \sum_{i>1} x_i (\mathbf{b}_i + c_1 \mathbf{b}_1) - \mathbf{b}_1 \right) \\ &= \left(x_1 - \sum_{i>1} c_i x_i \right) \mathbf{b}_1 + \sum_{i>1} x_i \mathbf{b}_i + \sum_{i>1} x_i c_i \mathbf{b}_1 = \mathbf{v}. \end{aligned}$$

Поэтому $\|\mathbf{u} - \mathbf{b}_1\| \leq r$, и, следовательно, на входе $(\mathbf{B}', \mathbf{b}_1, r)$ будет получен ответ YES. □

Двойственная решетка.

Определение

Двойственной к решетке L называется решетка вида

$$L^* = \{x \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z}\ \forall y \in L\}.$$

Определение

Пусть P_1 и P_2 — два вероятностных распределения на σ-алгебре Ω. Расстояние между ними определяется формулой

$$\sup_{\substack{A,B\in\Omega \\ A\cap B=\emptyset}} \{|P_1(A) - P_2(A)| + |P_1(B) - P_2(B)|\}.$$

(d, M)-решетки.

Определение

Пусть заданы натуральное n и вещественные $M > 0$ и $d > 0$. Полная решетка $L \subset \mathbb{Z}^n$, содержащая $(n-1)$-мерную подрешетку L', для которой выполняются свойства

1. *L' имеет базис из векторов длины которых не более M;*
2. *если $(n-1)$-мерное подпространство $Span(L') = H \subset \mathbb{R}^n$ и $H' \neq H$ сдвиг H, имеет непустое пересечение с L, то расстояние между H и H' не менее d,*

называется (d, M)-решеткой.

Генерация ключей.

1. Порождаем $(n-1)$-мерную решетку L' с базисом $(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ с условием $\|\mathbf{b}_i\| \leq M$. Пусть H — линейная оболочка L'.
2. Выбираем $d \geq n^c M$.
3. Выбираем из большого куба случайный вектор $\mathbf{b}_n$ с расстоянием $d \leq d_L \leq 2d$ от H.
4. Секретный ключ — вектор $\mathbf{b}_n^*$.
5. Открытый ключ — случайный базис B' в $L = L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

Алгоритм шифрования 1

Вход: Сообщение $\bar{x}$, i-й бит которого x_i.
Выход: Набор Y векторов, i-й вектор которого $\bar{y}_i = (\bar{y}_1^1, \ \ldots, \bar{y}_1^n)$ такой, что $\bar{y}_j^i = \frac{\bar{z}_j^i}{n}$, где $\bar{z}_j^i$ — целое.
Выполнение: 1. Для каждого бита $x_i = 1$ сообщения $\bar{x}$ выбираем случайный вектор $y_i = (y_1^i, \ \ldots, y_n^i)$ в соответствии с равномерным распределением в параллелепипеде $\mathcal{P}(\mathbf{b}_1^*, \ \ldots, \mathbf{b}_n^*)$. Для каждой координаты y_j^i вектора y_i вычисляем ее рациональное приближение $\bar{y}_j^i = \frac{\bar{z}_j^i}{n}$, такое что $|y_j^i - \bar{y}_j^i| < \frac{1}{n}$.
2. Биту $x_i = 0$ сообщения $\bar{x}$ ставим в соответствие сумму случайного вектора $z_i \in \mathbb{R}^n$, выбранного в соответствии с нормальным распределением с функцией плотности $\rho(w) = e^{-\pi\|w\|^2}$, $w \in \mathbb{R}^n$, и случайного вектора решетки $L(\mathbf{B})$. Вектор z_i определяет единственный элемент $y_i \in \mathcal{P}(\mathbf{b}_1^*, \ \ldots, \mathbf{b}_n^*)$, такой что $y_i - z_i \in L$. Для каждой координаты y_j^i вектора y_i вычисляется его рациональное приближение $\bar{y}_j^i = \frac{\bar{z}_j^i}{n}$, такое что $|y_j^i - \bar{y}_j^i| < \frac{1}{n}$.

Алгоритм дешифрования 1

Через $[[x]]$ обозначим расстояние до ближайшего целого к x.
Вход Набор Y, векторов $\bar{y}_i$.
Выход: Последовательность $\bar{x}'$ битов x'_i.
Выполнение: Для всех i находим скалярное произведение $\alpha_i = (\bar{y}_i, \mathbf{b}^*_n)$. Если $[[\alpha_i]] \geq \tilde{c}(\log n)^{\frac{1}{2}}$, то получаем бит $x'_i = 1$, иначе — бит $x'_i = 0$.

Теорема

Пусть $2n^{-\frac{\varepsilon}{3}} < \delta_1 < \tilde{c}(\log n)^{\frac{1}{2}} < \frac{1}{3}\delta_2$, *где* $\delta_1 > 0, \delta_2 > 0$. *Тогда алгоритм дешифрования 1 расшифровывает каждый бит сообщения, зашифрованного алгоритмом шифрования 1 с вероятностью ошибки* $p = p_1 + p_2$, *где* $p_1 < \delta_2 n^{-\frac{\varepsilon}{3}}, p_2 < c_1 e^{-c_2 n^{\frac{2\varepsilon}{3}}}$, *где* $c_1 = \frac{2}{\pi\delta_1}, c_2 = \frac{\pi\delta_1^2}{4}$.

Алгоритм шифрования 2

Вход: Сообщение $\bar{x}$, i-й бит которого x_i.
Выход: Набор Y векторов, i-й вектор которого $\bar{y}_i = (\bar{y}_1^1, \ \ldots, \bar{y}_1^n)$ такой, что $\bar{y}_j^i = \frac{\bar{z}_j^i}{n}$, где $\bar{z}_j^i$ — целое.
Выполнение: Если $x_i = 0$, то положим $s_i = 0 \in \mathbb{R}^n$, если же $x_i = 1$, то положим $s_i = fj_A \in \mathbb{R}^n$. Пусть $z_i \in \mathbb{R}^n$ — случайный вектор с нормальным распределением, функция плотности которого $\rho(w) = e^{-\pi \|w\|^2}$, $w \in \mathbb{R}^n$. Возьмем вектор $y_i = (y_1,^i, \ \ldots, y_n^i)$ из параллелепипида $\mathcal{P}(2f_1, \ \ldots, 2f_n)$, такой что $y_i - (z_i + s_i) \in 2L^*$. Такой вектор y_i будет один и только один: $y_i = s_i + z_i + \sum_{j=1}^{n} 2a_j f_j$ для некоторого набора $a_j \in \mathbb{Z}, j \in \bar{1,n}$, поэтому его координатами в базисе $D' = (2f_1, \ \ldots, 2f_n)$ будут дробные части соответствующих координат вектора $s_i + z_i$ в этом базисе. Для каждой координаты y_j^i вектора y_i вычисляется его рациональное приближение $\bar{y}_j^i = \frac{\bar{z}_j^i}{n}$, такое что $|y_j^i - \bar{y}_j^i| < \frac{1}{n}$.

Алгоритм дешифрования 2

Обозначим через k_w ближайшее целое к w.

Вход: Набор Y, векторов $\bar{y}_i$.

Выход: Последовательность $\bar{x}'$ битов x'_i.

Выполнение: Для всех i находится скалярное произведение $\alpha_i = (\bar{y}_i, u)$. Если $k_{\alpha_i} \equiv 0 \mod 2$, то получаем бит $x'_i = 0$, иначе — бит $x'_i = 1$.

Теорема

Алгоритм дешифрования 2 расшифровывает каждый бит сообщения, зашифрованного алгоритмом шифрования 2 с вероятностью ошибки $p < c_1 n^{-\frac{\varepsilon}{3}} e^{-c_2 n^{\frac{2\varepsilon}{3}}}$, *где* $c_1 = \frac{2}{\pi c'}, c_2 = \pi c'^2, c' = \frac{1}{2} - n^{-\frac{\varepsilon}{3}}$.

Диофантова аппроксимация

Определение

Пусть $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ *и пусть* $\varepsilon > 0$. *Пусть* $Q \in \mathbb{N}$ *удовлетворяет условию* $Q \geq \varepsilon^{-n}$. *Задача одновременной диофантовой аппроксимации заключается в нахождении таких* $q, p_1, \ldots, p_n \in \mathbb{Z}$, *что* $0 < q \leq Q$ *и*

$$|\alpha_i - p_i/q| \leq \varepsilon/q$$

для всех $1 \leq i \leq n$.

Теорема

Пусть $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ *— рациональные числа, числители и знаменатели которых ограничены по абсолютной величине значением X. Пусть* $0 < \varepsilon < 1$. *Тогда можно найти за полиномиальное время такие целые числа* $(q, p_1, \ldots, p_n)$, *что* $0 < q < 2^{n(n+1)/4}\varepsilon^{-(n+1)}$ *и* $|\alpha_i - p_i/q| \leq \varepsilon/q$ *для для всех* $1 \leq i \leq n$.

Доказательство теоремы об аппроксимации

Положим $Q = 2^{n(n+1)/4}\varepsilon^{-(n+1)}$ и рассмотрим решетку $L \subset \mathbb{Q}^{n+1}$, базис которой задан матрицей

$$\begin{pmatrix} 1/Q & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix}.$$

Размерность решетки $n+1$ и ее детерминант равен $1/Q$.
Произвольный вектор решетки представляется в виде

$$(q/Q, q\alpha_1 - p_1, q\alpha_2 - p_2, \ \dots, q\alpha_n - p_n).$$

Элементы базиса решетки ограничены рациональными числами, числители и знаменатели которых не превосходят по модулю величины $\max\{X, 2^{n(n+1)/4}/\varepsilon^{n+1}\}$.

Доказательство теоремы об аппроксимации

Отметим, что решетка L имеет не целочисленный, а рациональный базис. Применим *LLL*-алгоритм к решетке L получим ненулевой вектор

$$v = (q/Q, q\alpha_1 - p_1, \ \ldots, q\alpha_n - p_n)$$

такой, что

$$\|v\| \leq 2^{n/4} \det(L)^{1/(n+1)} = 2^{n/4} \cdot 2^{-n/4}\varepsilon = \varepsilon < 1.$$

Если $q = 0$, то $v = (0, -p_1, \ \ldots, -p_n)$, причем $p_i \neq 0$ при некотором i и, следовательно, $\|v\| \geq 1$. Поэтому $q \neq 0$. Без ограничения общности, можно предполагать, что $q > 0$. Поскольку $\|v\|_\infty \leq \|v\|$, выполняются неравенства $q/Q \leq \varepsilon < 1$. Поэтому $0 < q < Q\varepsilon \leq 2^{n(n+1)/4}\varepsilon^{-(n+1)}$. Аналогично, получаем неравенства $|q\alpha_i - p_i| < \varepsilon$ для всех $1 \leq i \leq n$.

Случайный класс решеток.

Пусть набор векторов $\nu = [u_1, \ldots, u_m]$, где $u_i \in \mathbb{Z}^n$.

Тогда $\Lambda(\nu, q)$ — определяется как решетка всех последовательностей целых $h_1, \ldots, h_m$ таких, что

$$\sum_{i=1}^{m} h_i u_i \equiv 0 \pmod{q}$$

Упражнение. Векторы $(h_1, \ldots, h_m)$ образуют решетку.

При заданном n положим $m = \lfloor c_1 n \log n \rfloor$, $q = \lfloor n^{c_2} \rfloor$.

Выберем случайные независимые векторы $v_1, \ldots, v_{m-1}$ равномерно на множестве всех векторов $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, с $0 \leq x_i < q$.

Выберем $\delta_1, \ldots, \delta_{m-1}$ случайно и равномерно из множества $\{0, 1\}$.

Определим

$$v_m \equiv -\sum_{i=1}^{m-1} \delta_i v_i \pmod{q}$$

где каждая компонента v_m принадлежит $[0, q-1]$.

Для $\lambda = (v_1, \ldots, v_m)$ будем писать λ_{n,c_1,c_2}.

По теореме Дирихле для достаточно больших c_1 $\exists$ вектор короче, чем n.

Теорема

$\exists$ c_1, c_2, c_3: если есть вероятностный полиномиальный алгоритм A, который получая на вход случайную переменную λ_{n,c_1,c_2} с вероятностью не менее $1/2$ выдает ненулевой вектор решетки $\Lambda(\lambda_{n,c_1,c_2}, \lfloor n^{c_2} \rfloor)$ длины не более n, то есть вероятностный алгоритм B, который принимая на вход линейно независимые векторы $a_1, \ldots, a_n \in \mathbb{Z}^n$, за время полиномиальное от $\sigma = \sum_{i=1}^{n} size(a_i)$, выдает $z, (d_1, \ldots, d_n)$ такие, что с вероятностью более $1 - 2^{-\sigma}$ выполнено:
1) если v — кратчайший ненулевой вектор в решетке $L(a_1, \ldots, a_n)$, то

$$z \leq ||v|| \leq n^{c_3} z;$$

2) $d_1, \ldots, d_n$ является базисом, причем $\max_{i=1}^{n} ||d_i|| \leq n^{c_3} bl(L)$.

Односторонние функции. Пусть $m = \lfloor c_1 n \log n \rfloor$, $q = \lfloor n^{c_2} \rfloor$, c_1, c_2 — даны в теореме.

Областью определения f будет множество $v_1, \ldots, v_{m-1}, \delta_1, \ldots, \delta_{m-1}$, где каждое v_i, является n-мерным вектором $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, причем $0 \leq x_i < q$, и каждое δ_i есть 0 или 1.

Пусть $x = (v_1, \ \ldots, v_{m-1}, \delta_1, \ \ldots, \delta_{m-1}) \in \mathrm{domain}(f)$ и

$$v_m \equiv -\sum_{i=1}^{m-1} \delta_i v_i \pmod{q}$$

где все компоненты v_m — целые числа из интервала $[0, q-1]$.

Положим

$$f(x) = (v_1, \ \ldots, v_{m-1}, v_m).$$

f — односторонняя функция. Пусть $y = (v_1, \ldots, v_m) = f(x)$, где x — случайный элемент $\mathrm{domain}(f)$.

Поскольку y является случайной переменной λ_{n,c_1,c_2}, то если есть алгоритм инвертирования f на y, который находит x': $f(x') = y$, то этот алгоритм находит также короткий ненулевой вектор в $\Lambda(\lambda_{n,c_1,c_2}, \lfloor n^{c_2} \rfloor)$.

Из теоремы вытекает, что если хотя бы одна из двух проблем трудна в худшем случае (не имеет полиномиального вероятностного алгоритма), то f — односторонняя функция.