О. В. Кузьмин, **В. С. Усатюк** (Иркутск, ИГУ, Братск, БрГУ).
Иерархия сложности задач теории решеток в семействе ассиметричных систем шифрования, криптостойких к квантовым вычислительным машинам.

Широко используемые на сегодняшний день ассиметричные системы шифрования основаны на двух типах задач теории чисел: задачах факторизации целых чисел, задачах дискретного логарифмирования.

Питер Шор в 1995 г. продемонстрировал полиномиальные алгоритмы обращения описанных выше задач на квантовых компьютерах [1]. Исаак Чжуан в 2001 г. экспериментально подтвердил выполнение алгоритма факторизации Шора на 7-кубитном квантовом компьютере [2]. Миклос Айтаи в 1996 г. в своей работе [3]: построил одностороннюю функцию на основе SVP-задачи (shortest vector problem, поиск кратчайшего ненулевого вектора в решетке) лежащую в основе ассиметричной системы шифрования Айтая; доказал, переформулировав в вероятностный вариант задачи о рюкзаке, что SVP-задача не имеет вероятностного полиномиального алгоритма решения, т. е. неразрешима за полиномиальное время на квантовых вычислителях.

Эта работа открыла новое направление в криптографии, целью которого является создание систем шифрования на основе задач теории решеток, криптостойких к квантовым вычислительным устройствам.

Решетка — дискретная аддитивная подгруппа, заданная на множестве $\mathbf{R}^n$, т. е. решетку L можно представить как множество векторов, заданных целочисленными линейно независимыми базисными векторами $B = \{\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_n\} \subset \mathbf{R}^n$, определенными по модулю некоторого целого числа $x \in Z^n$, $L = \sum_{i=1}^{n} \overline{b}_i Z = \{Bx\colon\ x \in Z^n\}$. Перечислим некоторые из задач теории решеток.

1. Приближенная SVP-задача — по базису решетки $L \in Z^{mxn}$ и вещественному $\gamma > 0$ найти ненулевой вектор, в γ-раз больший кратчайшего вектора $\overline{b} \in LZ^n \backslash \{0\}$: $\|\overline{b}\|_p \leqslant \gamma\lambda_1^p(L)$ (SVP_γ^p).

2. Поиск ближайшего вектора — по базису решетки $L \in Z^{mxn}$, вещественному $\gamma > 0$ и заданному вектору $\overline{y} \in LR^n$ найти ненулевой вектор $\overline{b} \in LZ^n$: $\|\overline{y} - \overline{b}\|_p \leqslant \gamma\lambda_1^p(L)$ (Closes Vector Problem, CVP_γ^p).

3. Приближенный поиск γ-уникального кратчайшего вектора $\overline{u}$ — поиск вектора $\overline{u} \in L\backslash\{0\}$: $\|u\|_p \leqslant \gamma\lambda_1^p(L)$, где $\lambda_1^p(L)$ — лина такого кратчайшего вектора в решетке с p-нормой, что $\lambda_1^p(L) \leqslant \|\overline{w}\|_p \leqslant \gamma\lambda_1^p(L)$, $\overline{w} = z\overline{u}$ для некоторых $z \in \mathrm{Z}$ для любого $w \in L$ (Unique Shortest Vector Problem, $\mathrm{USVP}^p(n,\gamma)$).

Задачи допускают взаимную редукцию, например, $\mathrm{USVP}^p(n,\gamma) \leqslant p\mathrm{SVP}^p(n,\gamma)$, $\mathrm{SVP}_\gamma^2 \leqslant p\mathrm{CVP}_\gamma^2$.

На рис. представлена иерархия сложности по времени выполнения для SVP_γ^p-задачи относительно γ, построенная на основе алгоритмов:

1) точного решения ($\gamma = 1$) со сложностью $2^{O(n)}$ и аналогичной сложностью по пространству, NPC (NP-полные) [4];

2) приближенного решения задач теории решеток: блочном алгоритме Коркина–Золотарева (block Korkin–Zolotarev, BKZ-LLL), методе приближения рядами Фурье и прочими методами: NPC для $\gamma > n^{(\log\log n)^{-1}}$, где n — размерность решетки [5]; P для субэкспоненциальной точности $\gamma = 2^{n(\log n \log n)^2/\log n}$ (см. [6, 7]); вероятно, не NPC ($NP \bigcap \mathrm{co}AM$) для $\gamma \geqslant \sqrt{n/\log n}$, $NP \bigcap \mathrm{co}NP$ для $\gamma \geqslant \sqrt{n}$, BPP для $\gamma \geqslant 2^{n\log\log n/\log n}$ (см. [8]).

Область $\gamma \in NP \bigcap (\mathrm{co}AM \bigcup \mathrm{co}NP)$ является криптографической, так как односторонние функции, построенные на основе задач теории решеток, обладают достаточной криптостойкостью и относительно эффективны по времени выполнения и пространству.

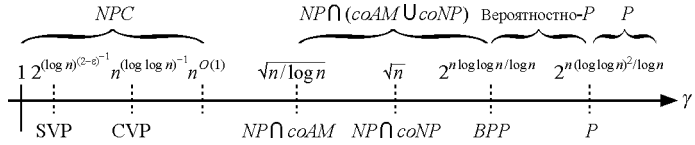

Рис. Сложность SVP^p_γ-задачи по времени выполнения

СПИСОК ЛИТЕРАТУРЫ

1. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. — SIAM J. Com., 1997, v. 26, № 5, p. 1484–1509.
2. *Chuang L. I.*, *Sherwood M. H.* Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. — Nature, 2001, v. 414, p. 883–887.
3. *Ajtai M.* Generating Hard Instances of Lattice Problem. — In: Proceedings of 28th ACM STOC, 1996, p. 99–108.
4. *Micciancio D.*, *Voulgaris P.* A Deterministic Single Exponential Time Algorithm for Most Lattice Problems based on Voronoi Cell Computations. — In: Proceedings of 42th ACM STOC, 2010, p. 351–358.
5. *Dinur I.*, *Kindler G.*, *Safra S.* Approximating CVP to Within Almost-Polynomial Factors is NP-hard. — Combinatorica, 2003, v. 23, № 2, p. 205–243.
6. *Schnorr C. P.* A hierarchy of polynomial time lattice basis reduction algorithms. — Theoretical Computer Science, 1987, v. 53, № 2–3, p. 201–224.
7. *Lenstra A. K.*, *Lenstra H. W.*, *Lovasz L.* Factoring polynomials with rational coefficients. — Math. Ann., 1982, v. 261, № 4, p. 515–534.
8. *Aharonov D.*, *Regev O.* Lattice problems in NP intersect coNP. — JACM, 2005, v. 52, № 5, p. 749–765.