В.С. Усатюк (аспирант)

ЗАДАЧИ ТЕОРИИ РЕШЕТОК И ИХ ВЗАИМНЫЕ РЕДУКЦИИ

Братск, Братский государственный университет

Задачи теории решеток лежат в основе целого класса криптографических примитивов и протоколов «постквантовой криптографии»:

- ассиметричных системах шифрования: Айтая-Дворка(Ajtai-Dwork), Реджева(Regev), Джентри (Gentry), NTRU [1];
- криптографических хеш-функциях: Айтая ([2],[3]), LASH [4], SWIFFT [5], SWIFFTX [6];
- протоколах цифровой подписи: Гольдвассера-Гольдштейна-Халеви (GGH)[7], NTRUS_{IGN} [8], Джентри-Пейкерта-Вейкантанатана[9], Миссиансио-Вадхена[10], Миссиансио-Любашевского[11];
- протоколах защищенного обмена данными и идентификационных схемах: Джентри-Пейкерта-Вейкантанатана (IBE) [9], Пейкерта-Вейкантанатана [12], Пейкерта-Вейкантанатана-Вотерса(ОТ) [13], Любашевского [14].

Поэтому изучение и уточнение свойств задач теории решеток это одна из основных целей, как при построении, так и при криптоанализе примитивов и протоколов на основе задач теории решеток. Важность этого направления исследований обусловлена так же наличием у задач теории решеток (при некоторых параметрах) свойств криптостойкости к алгоритмам, выполняемым на квантовых компьютерах. Роль последнего обстоятельства, в свете недавнего открытия коллективом ученных под руководством Джереми О'Брайена механизма создания фотонных квантовых компьютеров посредством традиционной литографии СБИС, резко возрастает ([15], [16]).

Решетка — дискретная аддитивная подгруппа, заданная на множестве R^n , то есть решетку L можно представить как множество целочисленных линейных комбинаций $L(b_1,...,b_2)=\{\sum_{i=1}^n x_ib_i:x_1,...,x_n\in Z\}$, n-линейно независи-

мых базисных векторов $\{\overline{b}_1,...,\overline{b}_n\}\subset R^m$ в m-мерном Евклидовом, где m и n, размерность и ранг решетки соответственно (рис. 1). У решетки может быть множество базисов, $L = \sum_{i=1}^{n} \overline{a}_{i} \cdot Z$, (рис. 2). На рисунках 3, 4 показаны фундаментальные параллелепипеды образованные базисами. Площади (объемы в многомерном случае) фундаментальных параллелепипедов образованных всевозможными базисами одной решетки L, det(L) будут равны, det L- инвариант решетки. Под кратчайшим вектором решетки будем понимать вектор, длина которого $\lambda(L) = \min_{x,y \in L, x \neq y} \|x - y\| = \min_{x \in L, x \neq y} \|x\|$ (рис. 5). Тогда многомерным обобщением этого понятия для решетки размерностью n, L^n будет i-й последовательный минимум $\lambda_i(L)$, под которым понимают наименьший радиус окружности(шара) содержащий i-линейно независимых векторов $\lambda_{_i}^{\ p}(L)=r\,,\;\;r\in R$: $\exists v_i\in L,\max_i \left\|v_i\right\|\leq r\,,\;\;$ где v_i -это линейно независимые вектора (рис. 6). Первый последовательный минимум в решетке $\lambda_1^{\ p}(L)$ соответствует длине кратчайшего вектора в решетке. Нормы определяют в контексте конкретной каждой задачи, однако обычно используются $\ell_1 = \max_j \sum_i \left| a_{ij} \right|, \ell_2 \text{ - Евклида или } \ell_\infty = \left\| (x_1, x_2, ..., x_n) \right\|_\infty = \max_{i=1,2,...,n} \left| x_i \right| \text{ - Чебышева.}$

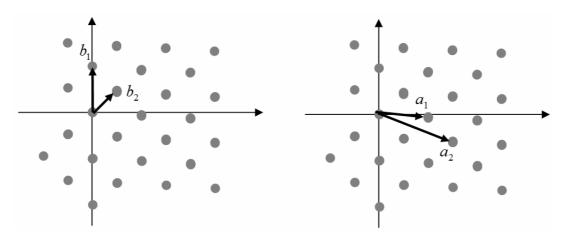


Рис. 1. Решетка с базисом $\{\overline{b}_1,\overline{b}_2\}\in B$ Рис. 2. Решетка с базисом $\{\overline{a}_1,\overline{a}_2\}\in B$

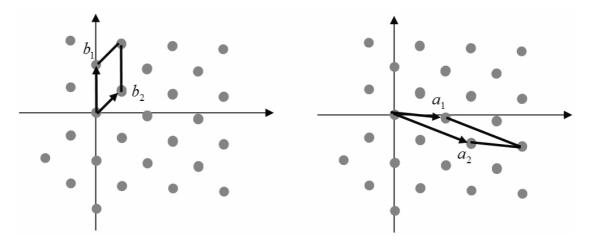


Рис. 3, 4. Фундаментальные параллелепипеды, образованные базисами

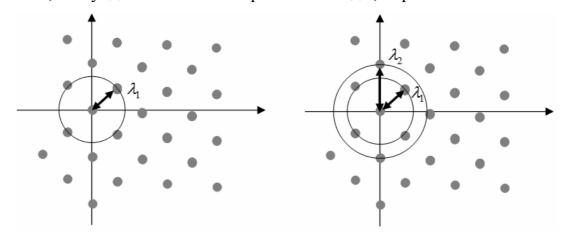


Рис. 5. Кратчайший вектор Рис. 6. Кратчайший базис решетки L в R^2

Идеальная решетка — это решетка со свойствами идеала на некотором кольце чисел, то есть результат сложения и умножения векторов в такой решетке так же принадлежит ей самой. Пусть задано кольцо многочленов с целочисленным коэффициентами R = Z[x]/f(x) взятых по модулю f(x), где f(x) - унитарный приведенный многочлен степени n. Так как заданное отношение изоморфно над Z^n и аддитивные группы и идеалы кольца являются подгруппами в R, полученная конструкция представляет собой решетку. Такой класс решеток принято называть идеальными решетками.

Таким образом, познакомившись с основными определениями теории решеток, перечислим задачи, применяемые при построении и оценке сложности в рассматриваемых нами системах шифрования[17]:

- 1. По базису решетки найти кратчайший ненулевой вектор (shortest vector problem, SVP; поиск кратчайшего вектора), (рис. 7);
- 2. По базису решетки $B \in Z^{mxn}$ и вещественному $\gamma > 0$, найти ненулевой вектор $\overline{b} \in BZ^n \setminus \{0\} : \|\overline{b}\|_p \le \gamma \cdot \lambda^{p_1}(L)$ с р-нормой (γ -approximation shortest vector problem, SVP_{γ}^p ; приближенный поиск кратчайшего вектора), (рис. 8);

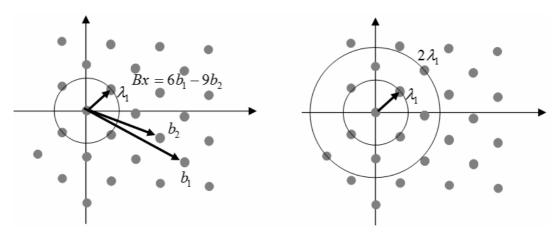


Рис. 7. Пример SVP-задачи в R^2 Рис. 8. Пример SVP_{γ} -задачи в R^2

- 3. По базису решетки B и заданному вектору $\bar{j} \notin L(B)$, найти ближайший вектор $\bar{b} \in L(B)$ (Closes vector problem, CVP; поиск ближайшего вектора), является неоднородным(гетерогенным) вариантом SVP-задачи), (рис. 9);
- 4. По базису решетки $B \in Z^{mxn}$, вещественному $\gamma > 0$ и заданному вектору $\bar{j} \in LR^n$, найти ненулевой вектор $\bar{b} \in BZ^n : \|\bar{j} \bar{b}\|_p \le \gamma \lambda_1^p(L)$ с р-нормой $(\gamma approximate closes vector problem, <math>CVP^p_{\gamma}$);

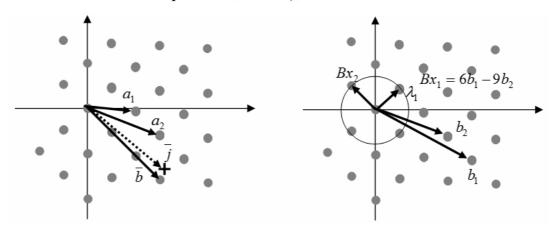


Рис. 9. Пример CVP -задачи в R^2 Рис. 10. Пример SIVP -задачи в R^2

- 5. Пусть дана n-мерная решетка L. Найти линейно независимые вектора $\bar{b}_1,...,\bar{b}_n \in L$, для которых $\max_{i=1}^n \left\| \bar{b}_i \right\|_p \le \gamma \lambda^p_n(L)$, где $\lambda^p_n(L)$ i й последовательный минимум в решетке с p -нормой (γ -approximate shortest independent vector problem, $SIVP_{\gamma}^{\ p}(n,\gamma)$; приближенный поиск кратчайших линейно независимых векторов), (рис. 10);
- 6. Пусть дана n-мерная решетка L. Найти вектор $\overline{u} \in L \setminus \{0\} : \|u\|_p \leq \gamma \lambda_1^p(L)$, где $\lambda^p_1(L)$, это длина кратчайшего вектора в решетке c p-нормой и \overline{u} кратчайший γ уникальный вектор, т.е. $\forall w \in L : \lambda_1^p(L) \leq \|\overline{w}\|_p \leq \gamma \lambda_1^p(L)$ $\overline{w} = z\overline{u}$ для некоторых $z \in Z$ (γ -approximate unique shortest vector problem, uSVP $_{\gamma}^p(n,\gamma)$; поиск уникального кратчайшего вектора), (рис. 11);
- 7. Пусть дан базис B, q-нарной(модулярной) m-мерной решетки L_q^{mxn} , т.е. решетка L, для которой принадлежность вектора к решетки L определяется: $L(B) = \{B^T s \bmod q \subseteq Z^m, s \in Z^n\}$, q-простое число. На решетке равномерно распределен шум e (обычно с моментом ожидания равным 0 и дисперсией \sqrt{q}), q задан некоторым многочленом, $\overline{s} \in Z_q^n$ некоторый исходный вектор без шума, известно значение $(B\overline{s}+\overline{e})$. Найти исходную точку в решетке (исключить шум) по некоторому множеству известных $(B\overline{s}_i+\overline{e}_i)$. Задача обучения с ошибками (Learning with errors, LWE) является обобщением задачи обучения контроля целостности (четности) данных с шумами, (Рис. 12);

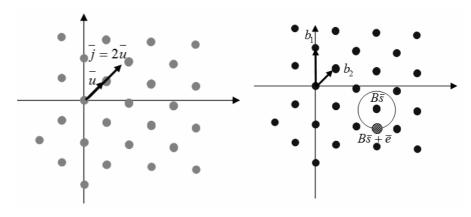


Рис. 11. Пример uSVP-задачи

Рис. 12. Пример LWE-задачи

- 8. Пусть дана m-мерная модулярная решетка $L_q^\perp(B) = \{ \overline{x} \in Z^m : B\overline{x} \equiv \overline{0}Z^n \bmod q \}$ образованная базисом $B \in Z_q^{n \times m}$, взятым случайно из равномерного распределения над $Z_q^{n \times m}$. Найти вектор кратчайший вектор $\overline{v} \in L_q^\perp(A) : \|\overline{v}\|_p \le \beta$ с p-нормой (Short integer solution problem, $\mathrm{SIS}_{\beta}^p(n,m)$; задача поиска вектора по норме в модулярной решетке);
- 9. Пусть дана m-мерная модулярная решетка $L_q^\perp(B)=\{\overline{x}\in Z^m: B\overline{x}\equiv \overline{0}Z^n \bmod q\}$ образованная базисом $B\in Z_q^{n\times m}$ и вектор $\overline{y}\in Z^n$, взятые случайно из равномерного распределения над $Z_q^{n\times m}$, Z^n соответственно. Найти вектор $\overline{v}\in \{\overline{x}\in Z^m: A\overline{x}\equiv \overline{y} \bmod q\}: \|\overline{v}\|_p \leq \beta$. (Short integer solution problem, ISIS $_\beta^p(n,m)$; гетерогенная задача поиска вектора по норме в модулярной решетке);
- 10. По базису решетки $B \in Z^{mxn}$ и вещественному $\gamma \ge 1$, найти ненулевой вектор $\overline{b} \in BZ^n \setminus \{0\} : \|\overline{b}\|_p \le \gamma \cdot \det(L(B))^{1/n}$ с p-нормой (γ -арргохітаte Hermite shortest vector problem, hermitSVP $_{\gamma}^p$; задача приближенного поиска кратчайшего вектора по Эрмиту);
- 11. Пусть дана n -мерная решетка $L^n \subseteq R^k$. Найти базис $B: \forall B' \in \{B \in Q^{n \times k}: L = L(B)\}, \max_{i=1}^n \{\left\|\overline{b_i}\right\|_p\} \le \gamma \max_{i=1}^n \{\left\|\overline{b_i}\right\|_p\} (\gamma \text{-approximate shortest basis problem, SBP}_{\gamma}^{\ p}(n);$ приближенный поиск кратчайшего базиса);
- 12. Пусть n-мерная решетка L^n , заданна некоторая p-норма. Найти длину $l^{(p)} \in R: l^{(p)} \le \lambda_1^{(p)}(L) \le \gamma l^{(p)}$, где $\lambda_1^{(p)}(L)$ длина кратчайшего вектора или первый последовательный минимум в решетке $L(\gamma$ -арргохітаte shortest length problem, $SLP_{\gamma}^{\ p}(n)$; задача приближенного поиска длины кратчайшего вектора в решетке);
- 13. По базису решетки $B \in Z^{m \times n}, m \ge n$ и радиусу $r \in R$ ответить на вопрос: «да» - если все точки решетки можно покрыть радиусом r, $r \ge p(L(B))$;

- «нет» если $\gamma \cdot r < \rho(L(B))$ (γ -approximate covering radius problem, $CRP_{\gamma}^{p}(n,r)$; приближенная задача покрытия решетки радиусами);
- 14. По базису решетки $B \in Z^{mxn}$, вещественному $\alpha \ge 1$ и вектору $\overline{u}: \exists \overline{t} \in L(B), \|\overline{u} \overline{t}\|_p < \alpha \cdot \lambda_1^p(L)$, найти вектор $\overline{v} \in L(B): \|\overline{u} \overline{v}\|_p = \min(\alpha \alpha)$ арргохітаte bounded distance decoding, $BDD_{\alpha}^{p}(u)$; приближенная задача о декодирование с ограниченным расстоянием);
- 15. По базису $B \in Z^{m \times n}$, вектору решетки $v \in BZ^n$ и положительным действительным числам $d, \gamma > 0$ ответить на вопрос: «да» если $\min\{\|v\|_p : v \in BZ^n \setminus 0\} \le d$; «нет» если $\min\{\|v\|_p : v \in BZ^n \setminus 0\} > \gamma d$ (Decisional shortest vector problem, $\operatorname{GapSVP}_{\gamma}^p$; Булева задача о поиске кратчайшего вектора);
- 16. По базису $B \in Z^{m \times n}$, вектору решетки $t \in BZ^n$ и положительным действительным числам $d, \gamma > 0$ ответить на вопрос: «да» если $\min\{\|t-v\|_p : v \in BZ^n\} \le d$; «нет» если $\min\{\|t-v\|_p : v \in BZ^n\} > \gamma d$ (Decisional closest vector problem, $\operatorname{GapSVP}_{\gamma}^p$; Булева задача поиска вектора близкого к вектору в решетке);
- 17. Пусть дан идеал $I \in Z(x)/f(x)$. Найти многочлен $g(x) \in I \setminus \{0\} : \|g \mod f(x)\|_p \le \gamma \lambda_1^p(I)$. (Approximate ideal shortest vector problem/Shortest polynomial problem, Ideal-SVP $_{\gamma}^p(f)$; приближенная задача поиска кратчайшего вектора в идеальной решетке/задача поиска кратчайшего полинома);
- 18. Пусть даны m-многочленов $g_1(x),...,g_m(x)$ выбранных случайно из равномерного распределения заданного на $Z_q(x)/f(x)$ и n-степень многочлена f(x). Найти целые $e_1,...,e_m \in Z(x)$: $\sum_{i\leq m} e_i g_i = 0 \pmod q, \|e\|_p \leq \beta$, где вектор e-получается путем конкатенацией(объединением) коэффициентов при всех e_i (Ideal small integer solution problem, Ideal-SIS $_{\beta}^p(g,n,m)$; задача поиска вектора по норме в идеальной решетке).

Рассмотрев задачи теории решеток, приведем ключевую теорему, лежащую в основе шифрования на основе задач теории решеток, **теорема Айтая** [2]: Определим для любого натурального $n \in N$, класс случайных решеток L^n порождаемых с полиномиальной временной сложностью. Предположим, что существует полиномиальный по временной сложности алгоритм А такой, что для любой случайно выбранной решетки $L \subset L^n$, найдет нетривиальный вектор \overline{v} , длина которого не превосходит n. Значит, существует вероятностный полиномиальный по временной сложности алгоритм В, который для любой решетки $L \subset R^n$ и некоторых констант c_0, c_1, c_2 с высокой вероятностью способен решить любую из следующих задач:

- SVP_{γ} -задачу с точностью $\gamma = n^{c_2}$;
- $SIVP_{\gamma}$ -задачу с точностью $\gamma = n^{c_0}$;
- SBP_{γ} задачу с точностью $\gamma = n^{c_1}$.

Этой теоремой Айтай установил связь между сложностью в худшем и среднем случаях вышеперечисленных задач, а так же продемонстрировал механизм создания односторонних функций. Цай и Неруркар в 1997, снизили значение констант: $c_0 > 3$, $c_1 > 3.5$, $c_2 > 4$ ([18]). Даниель Миссиансио и Одед Реджев в 2004 г. показали, что $c_2 = 1$ ([19]). Гольдштейн, Гольдвасер и Халеви исследуя односторонние функции Айтая, доказали наличие у некоторых классов решеток более сильных свойств - свойств криптографических хеш-функций [3]. Именно наличие связи между сложностью в худшем и среднем случаях позволяет построить некоторую систему шифрования, на основе одной из задач теории решеток взятой из известного случайного распределения, тем самым получив строгую оценку сложности расшифровки этой системы (криптостойкости) в худшем случае. Следует так же отметить, что большинство криптографических примитивов и протоколов (RSA, ЕСС и прочие) не обладают данным свойством, а основаны на сложности в среднем, что значительно затрудняет, как выбор параметров шифрования, так и строгое доказательство сложности их расшифровки.

Каждая из задач теории решеток, в зависимости от параметров (например, точности решения), принадлежит к некоторому классу временной/емкостной сложности для детерминированной и недетерминированной машин Тьюринга[20]. При анализе задач, внимание концентрируется именно на временной сложности, как ключевом параметре защищенности (собственно емкостная сложность заведомо не превышает временную). Задачи допускают взаимные редукции, что упрощает их исследование, например: $SBP_{\gamma}^{p}(n) \leq_{p} SIVP_{\gamma}^{p}(n), \quad ([2]); \quad uSVP_{\gamma} \leq BDD_{1/\gamma} \leq uSVP_{2/\gamma} \quad ([21]); GapCVP_{\gamma}^{p} \equiv_{p} CVP_{\gamma}^{p}, SVP_{\gamma}^{2} \leq_{p} CVP_{\gamma}^{2}[10].$

Покажем на примере редукцию SVP^p - и CVP^p -задач([22], [23]).

От СVР $^{\rm p}$ к SVР $^{\rm p}$: Пусть дан почти ортогональный базис образующий п-мерную решетку $L(B): B = \{\overline{b}_1,...,\overline{b}_n\}$. Определим решетку $L'(B'): B' = \{2\overline{b}_1,...,\overline{b}_n\}$ и решим СVР $^{\rm p}$ -задачу для вектора \overline{b}_1 и решетки L'(B'), получив вектор $\overline{v} \in L'$. Вычислим новый вектор $\overline{s}_1 = \overline{v} - \overline{b}_1$. Выполним предыдущие действия для векторов $\overline{b}_2,...,\overline{b}_n$, получив вектора $\overline{s}_2,...,\overline{s}_n$. Найдем кратчайший из векторов $\overline{s}_1,...,\overline{s}_n$.

От SVP^p к CVP^p: Пусть дан базис образующий п-мерную решетку $L_0^n(B'): B' = \{\overline{b_1},...,\overline{b_n}\}, B \in Z^n$ и некоторая точка $y \notin L^n(B')$. Решим первую часть SVP^p -задачи, выполнив ортогонализацию базиса, как необходимое условие поиска кратчайшего вектора. Вычислять длинны векторов, а так же выбирать среди них кратчайший вектор, в данном случае нет необходимости. Получим решетку $L^n(B) \equiv L_0^n(B')$. Найдем вектор $\overline{a} \in R^n$, решив линейную систему уравнений $B\overline{a} = y$. Округлив координаты полученного вектора до целых значений, получим искомый вектор $\overline{z} \in Z^n$.

Сложность CVP^p-задачи превосходит сложность SVP^p-задачи, так как необходимым элементом решения *CVP*-задачи является наиболее ресурсоемкая часть задачи поиска кратчайшего вектора, а именно приведение базиса решетки к ортогональному виду. Сложность вычисления длин векторов

будет зависеть от нормы $(O(n\log n)$ для норм Евклида ℓ_2 , [24]), а сложность нахождения минимального элемента будет O(n) в худшем случае. Причем от качества базиса будет зависеть погрешность CVP^p -алгоритма, для предложенного алгоритма $\varepsilon = \|B\overline{a} - B\overline{z}\| \leq \frac{1}{2} \left\|\sum_i b_i\right\|$. Например для решеток $L_1(B_1) \equiv L_2(B_2)$, $|\det(B_1)| = |\det(B_2)|$ образованных базисами $B_1 = \{(1,0),(0,1)\}$, $B_2 = \{(100,1),(99,1)\}$, погрешность будет $\varepsilon_1 = 1.4, \varepsilon_2 \approx 199$ соответственно.

Задачи теории решеток предоставляют широкие возможности реализации криптографических протоколов и примитивов, а так же затрагивают множество фундаментальных вопросов, начиная от задач линейного программирования и многомерной упаковки тел до обобщенных теоретико-числовых проблем. Построение криптографических систем на основе задач теории решеток невозможно без дальнейшего исследования вышеперечисленных задач и алгоритмов их решения.

Список литературы.

- 1. Усатюк В.С. Обзор систем ассиметричного шифрования на основе задач теории решеток криптостойких к квантовым вычислительным машинам. Материалы I международной научно-практической конференции «Молодежь. Наука. Инновация», http://rgu-penza.ru/mni/content/files/10_1_ Usat-juk.pdf, стр. 12.
- 2. Ajtai M. Generating Hard Instances of Lattice Problem. Proc. of 28th ACM Symp. on Theory of Comp. Philadelphia: ACM Press. 1996. p. 99-108.
- 3. Goldreich O., Goldwasser S., Halevi S. Collision-free hashing from lattice problems. Technical Report TR96-056. Electronic Colloquium on Computation Complexity (ECCC). 1996.
- 4. Kamel Bentahar, Dan Page, Markku-Juhani O. Saarinen, Joseph H. Silverman, Smart N. LASH. NIST. Second Cryptographic Hash Workshop. August 24-25 2006.

- 5. V. Lyubashevsky, D. Micciancio, C. Peinkert, A. Rosen SWIFFT: a modest proposal for FFT hashing. In FSE 2008.
- 6. Arbitman Y., Dogon G., Lyubashevsky V., Micciancio D., Peikert C., Rosen F. SWIFFTX: A Proposal for the SHA-3 Standard. In NIST. 2008.
- 7. Goldreich O, Goldwasser, Halevi S. Public-key cryptosystems from lattice reduction problems. In Advances in cryptology. Lecture Notes in Computer Science. №1294. 1997. p. 112-131.
- 8. Hoffstein J., Graham N. A. H., Pipher J., Silverman J. H., Whyte W. NTRUSIGN: Digital signatures using the NTRU lattice. In Proc. of CT-RSA, LNCS. №2612. 2003. p. 122–140.
- 9. Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In Proc. 40th ACM Symp. on Theory of Computing (STOC). 2008. p. 197-206.
- 10. Micciancio D., Vadhan S. Statistical zero-knowledge proofs with efficient provers: lattice problems and more. In Advances in cryptology. Lecture Notes in Computer Science. 2003. p. 282-298.
- 11. Lyubashevsky V., Micciancio. Asymptotically efficient lattice-based digital signatures. Lecture in Computer Science. 2008. №4948. p. 379–396
- 12. Peikert C., Vaikuntanathan V. Noninteractive statistical zero-knowledge proofs for lattice problems. In Advances in cryptology (CRYPTO), LNCS. Springer. №5157. 2008. p. 536-553.
- 13. Peikert C., Vaikuntanathan V., Waters B. A framework for efficient and composable oblivious transfer. LNCS. №5157. 2008. p. 554-571.
- 14. Lyubashevsky V. Lattice-based identification schemes secure under active attacks. In PKC. №4939. 2008. p. 162-179.
- 15. Politi A., Jonathan C. F. V., O'Brien J.L. Shor's Quantum Factoring Algorithm on a Photonic Chip. Science. №325(5945). 2009. p. 1221.
- 16. Ladd T. D., Jelezko F., Laflamme R., Nakamura Y., Monroe C., O'Brien J. L. Quantum computers. Nature. №464. 2010. p. 45-53

- 17. Lattices and survey of it's problems. Электронный ресурс: режим доступа, открытый, http://www.ecrypt.eu.org/wiki/index.php/Lattices
- 18. Cai J.Y., Nerurkar A. P. An improved Worst-case to Average case reduction for lattice problems. FOCS. 1997. pp. 468-477.
- 19. Micciansio D., Regev O. Worst-case to average-case reduction based on Gaussian measures. FOCS. 2004. p. 372-381.
- 20. Кузьмин О.В., Усатюк В.С. Роль задач теории решеток в постквантовой криптографии и их иерархия сложности // Комбинаторные и вероятностные проблемы дискретной математики: сб. науч. тр. Иркутск: Изд-во Иркут. гос. ун-та, 2010. (Дискретный анализ и информатика; Вып. 4). С.71–79.
- 21. Lyubashevsky V., Micciancio. On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem. Lecture Notes in Computer Science. №5677. 2009. p. 577-594.
- 22. Micciancio D. The shortest vector problem is NP-hard to approximate to within some constant. SIAM J. CS. No 30. 2001. p. 2008-2035.
- 23. Weiss A. Shortest Vector In A Lattice is NP-Hard to approximate. The Hebrew University of Jerusalem. Inapproximability Seminar, Spring 2005, http://www.cs.huji.ac.il/~inapprox/papers/SVP-micc.pdf, crp. 38
- 24. Celebi M. E., Celiker F., Kingravi H. A. On Euclidean Norm Approximations. http://arxiv.org/abs/1008.4870 crp 9. 28.08.2010