СИММЕТРИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ. СИНТЕЗ И АНАЛИЗ

УДК 621.391:519.2

СУБ'ЕКСПОНЕНЦІЙНІ АЛГОРИТМИ РОЗВ'ЯЗАННЯ СИСТЕМ ЛІНІЙНИХ БУЛЕВИХ РІВНЯНЬ ЗІ СПОТВОРЕНИМИ ПРАВИМИ ЧАСТИНАМИ

А.М. ОЛЕКСІЙЧУК

Описано загальну схему побудови відомих суб'експоненційних алгоритмів розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. Виділено і проаналізовано найважливіші допоміжні задачі та процедури, що використовуються у зазначених алгоритмах, отримано неасимптотичні оцінки їх надійності. Викладені результати можуть бути використані при розв'язанні ряду задач криптоаналізу і теорії вивідування.

Ключові слова: система лінійних рівнянь зі спотвореними правими частинами, задача про адитивне представлення, суб'експоненційний алгоритм, кореляційний криптоаналіз.

ВСТУП

Системи лінійних булевих рівнянь зі спотвореними правими частинами є традиційним об'єктом досліджень в теорії кодування та криптології [1, 2]. Розв'язання таких систем загального вигляду рівносильно декодуванню довільних двійкових лінійних кодів. Остання задача є NP-повною [3] і для неї не відомо (та, ймовірно, не існує) поліноміальних алгоритмів.

Дана стаття присвячена аналізу алгоритмів, які дозволяють розв'язувати системи лінійних булевих рівнянь зі спотвореними правими частинами від n невідомих за суб'експоненційний час, тобто за $2^{o(n)}$ операцій над n-вимірними двійковими векторами. Перший такий алгоритм запропоновано в 1988 р. І. М. Коваленком [4], який показав, що у випадку, коли матриця коефіцієнтів системи, яка складається з $2^{O\left(\frac{n}{\log n}\right)}$ лінійних рівнянь зі спотвореними правими частинами, є випадковою та задовольняє певній загальній умові, зазначену систему можна розв'язати з як завгодно високою при $n \to \infty$ надійністю, використовуючи в середньому $2^{O\left(\frac{n}{\log n}\right)}$ операцій.

Алгоритм Коваленка [4] було фактично перевідкрито тринадцять років потому А. Блюмом, А. Калаі та Х. Вассерманом [5], які вивчали задачу розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами та випадковими рівноймовірними матрицями коефіцієнтів у зв'язку з однією проблемою теорії вивідування (learning theory). Алгоритм Блюма-Калаі-Вассермана (BKW) [5] є більш простим у порівнянні з алгоритмом Коваленка. Він швидко набув широкої відомості та знайшов чимало застосувань як у теорії вивідування, так і за її межами. Зауважимо, що обидва алгоритми є застосовними лише до таких систем, які складаються з великої кількості (а саме, з $2^{O\left(\frac{n}{\log n}\right)}$) лінійних рівнянь.

У 2005 р. В. Любашевський [6] показав, що задача розв'язання системи з $n^{1+\alpha}$ лінійних рівнянь від n невідомих зі спотвореними правими частинами та рівноймовірною матрицею коефіцієнтів зводиться до аналогічної задачі для системи з $2^{O\left(\frac{n}{\log n}\right)}$ лінійних рівнянь і запропонував алгоритм розв'язання зазначених систем (які складаються з $n^{1+\alpha}$ лінійних рівнянь, $\alpha > 0$) зі складністю $2^{O\left(\frac{n}{\log\log n}\right)}$. Відзначені результати робіт [5, 6] узагальнені С. Коппарті та С. Сарафом [7] на випадок систем лінійних булевих рівнянь з "агностичними" спотвореннями, тобто таких систем рівнянь, праві частини яких можуть формуватися довільним чином.

Ідеї та результати, викладені у відзначених (та деяких інших) публікаціях, дозволяють встановити загальну схему, за якою будуються відомі суб'експоненційні алгоритми розв'язання систем лінійних рівнянь зі спотвореними правими частинами, виділити важливі задачі та проаналізувати окремі процедури, що використовуються у зазначених алгоритмах, отримати неасимптотичні оцінки їх надійності. Викладення відзначених результатів є метою даної статті.

Основні результати статті сформульовані у вигляді двох "теорем зведення". Перша теорема базується на ідеях роботи [5] та дає відповідь на запитання, як саме (з якими надійністю і трудомісткістю) можна розв'язувати системи лінійних рівнянь зі спотвореними правими частинами на основі заданого алгоритму розв'язання так званої задачі про адитивне представлення. Друга теорема базується на ідеях робіт [6, 7] і показує, як розв'язувати системи з невеликої кількості лінійних рівнянь зі спотвореними правими частинами на основі заданого алгоритму розв'язання таких систем, що складаються з великої кількості рівнянь. Проаналізовано також найважливіші властивості процедури самокорекції [7], яка може

бути корисною не тільки для розв'язання систем лінійних рівнянь зі спотвореннями. Сформульовано ряд задач подальших досліджень.

1. ЗВЕДЕННЯ ЗАДАЧІ РОЗВ'ЯЗАННЯ СИСТЕМИ ЛІНІЙНИХ РІВНЯНЬ ЗІ СПОТВОРЕНИМИ ПРАВИМИ ЧАСТИНАМИ ДО ЗАДАЧІ ПРО АДИТИВНЕ ПРЕДСТАВЛЕННЯ

Задача про *адитивне r-представлення* (або *r-суму*, *r-sum problem*) полягає в наступному [8]. Задано список, тобто впорядкований набір L, що складається з l векторів $z_1,\dots,z_l \in V_n = \{0,1\}^n$. Потрібно для будь-якого вектора $z \in V_n$ знайти r (не обов'язково різних) номерів $\nu_1,\dots,\nu_r \in \overline{1,l}$ таких, що $z_{\nu_1} \oplus \dots \oplus z_{\nu_r} = z$. Припускається, що будь-який алгоритм **A** розв'язання цієї задачі або завершується успішно, тобто знаходить шуканий набір $\nu_1,\dots,\nu_r$, або видає негативну відповідь, тобто не знаходить зазначеного набору (хоча такий може існувати).

Нехай вектори $z_1,\dots,z_l$ у списку L генеруються незалежно один від одного у відповідності з певним розподілом ймовірностей P на множині V_n. Мінімальна за всіма векторами $z \in V_n$ ймовірність успішного завершення алгоритму **A** при вхідних даних (L,z) називається *P-надійністю алгоритму* **A** та позначається $\pi_{\mathbf{A},P} = \pi_{\mathbf{A},P}(n,r,l)$. Якщо P є рівномірним розподілом на множині V_n, то P-надійність алгоритму **A** називається його *надійністю* та позначається $\pi_{\mathbf{A}}$. *Трудомісткість алгоритму* **A** визначається як найбільше число операцій над n-вимірними двійковими векторами, що виконуються при його застосуванні до будь-яких вхідних даних (L,z), та позначається $T_{\mathbf{A}} = T_{\mathbf{A}}(n,r,l)$.

Відзначимо окремий випадок задачі про адитивне r-представлення, в якому задається r вхідних списків $L_1,\dots,L_r$ довжини $l_1,\dots,l_r$ відповідно, що складаються з незалежних в сукупності випадкових та рівноймовірних двійкових векторів довжини n. Потрібно знайти набір $z_1 \in L_1,\dots,z_r \in L_r$ такий, що $z_1 \oplus \dots \oplus z_r = 0$ [9, 10]. Зрозуміло, що при $l_1 + \dots + l_r = l$ будь-який алгоритм **A** розв'язання останньої задачі дозволяє розв'язувати першу: достатньо розбити вхідний список L на r частин $L_1, L_2, \dots, L_r$ та застосувати алгоритм **A** до списків $L_1 \oplus z, L_2, \dots, L_r$.

Задача про адитивне представлення добре відома в теорії кодування, теорії обчислювальних алгоритмів та криптоаналізі [8–10]. Зокрема, на ній, тією чи іншою мірою, базуються відомі суб'експоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами. Нижче доводиться загальна теорема, яка дозволяє будувати алгоритми розв'язання зазначених систем рівнянь на основі будь-яких алгоритмів розв'язання задачі про адитивне представлення.

Розглянемо систему рівнянь

$$Ax = b, \tag{1}$$

де A – булева матриця розміру $m \times n$, b – вектор довжини m з координатами

$$b_i = A_i a \oplus \xi_i,\ i \in \overline{1,m}, \tag{2}$$

де $A_1,\dots,A_m$ – рядки матриці A, $a = (a_1,\dots,a_n)^T$ – невідомий двійковий вектор (істинний розв'язок системи рівнянь (1)), $\xi_1,\dots,\xi_m$ – незалежні випадкові величини, розподілені за законами

$$\mathrm{P}\{\xi_i = 0\} = 1 - \mathrm{P}\{\xi_i = 1\} = \frac{1}{2}(1 + \theta_i),\ i \in \overline{1,m}, \tag{3}$$

де $\theta_i \ge \theta > 0$ для кожного $i \in \overline{1,m}$.

Позначимо e_i вектор довжини n, i-а координата якого дорівнює 1, а решта – 0, $i \in \overline{1,n}$. Сформулюємо допоміжне твердження, яке неодноразово використовується далі.

Лема 1 (*нерівність Гефдінга*) [11]. Нехай $\zeta_1,\dots,\zeta_t$ – незалежні випадкові величини такі, що $\alpha_j \le \zeta_j \le \beta_j$, $\alpha_j, \beta_j \in \mathbf{R}$, $j \in \overline{1,t}$. Тоді для будь-якого $x > 0$

$$\mathbf{P}\{\sum_{l=1}^{t}\zeta_l - \sum_{l=1}^{t}\mathbf{E}\zeta_l \ge tx\} \le \exp\left\{-\frac{2t^2x^2}{\sum_{l=1}^{t}(\beta_l - \alpha_l)^2}\right\}.$$

Наступна теорема базується на узагальненні міркувань, що використовуються при доведенні теореми 3 у статті [5].

Теорема 1. Припустимо, що матриця A системи рівнянь (1) складається з $m = nlt$ рядків, які є незалежними випадковими векторами, що мають однаковий розподіл ймовірностей P на множині V_n і не залежать від випадкових величин $\xi_1,\dots,\xi_m$. Тоді для будь-якого алгоритму **A** розв'язання задачі про адитивне представлення з параметрами n, r, l (див. вище) існує алгоритм **B**, який знаходить істинний розв'язок системи рівнянь (1) з імовірністю

$$\pi_{\mathbf{B}}(P,\theta) \ge (\pi_{\mathbf{A},P})^{tn}(1 - \exp\{-1/2 \cdot \theta^{2r}t\})^n, \tag{4}$$

використовуючи

$$T_{\mathbf{B}} = O(nt(T_{\mathbf{A}} + r)) \tag{5}$$

операцій над n-вимірними двійковими векторами.

Доведення. Алгоритм **B**, що пропонується, має такий вигляд.

1. Розіб'ємо систему рядків матриці A на tn списків $L_{i,j}$ довжини l кожний та застосуємо алгоритм **A** до вхідних даних $(L_{i,j}, e_i)$ для всіх $i \in \overline{1,n}$, $j \in \overline{1,t}$. Якщо хоча б в одному випадку алгоритм **A** завершується неуспішно, то алгоритм **B** припиняє роботу. Інакше для кожного $i \in \overline{1,n}$ отримаємо рівності вигляду

$$e_i = A_{\nu_1(i,j)} \oplus \dots \oplus A_{\nu_r(i,j)},\ j \in \overline{1,t}, \tag{6}$$

де $A_{\nu_1(i,j)},\dots,A_{\nu_r(i,j)} \in L_{i,j}$.

2. Для будь-яких $i \in \overline{1,n}$, $j \in \overline{1,t}$ обчислимо значення $b(i,j) = b_{\nu_1(i,j)} \oplus \ldots \oplus b_{\nu_r(i,j)}$ та відновимо i-у координату вектора a за мажоритарним правилом:

$$a_i = 1 \Leftrightarrow \sum_{j=1}^{t} b(i,j) \geq \frac{t}{2}.$$

Безпосередньо з наведеного опису випливає, що трудомісткість алгоритму **B** визначається за формулою (5).

Доведемо формулу (4). Нехай A – випадкова $m \times n$-матриця з незалежними рядками, що розподілені на множині V_n за законом P. Тоді усі списки $L_{i,j}$, які формуються на кроці 1 алгоритму, складаються з незалежних в сукупності випадкових векторів, що мають такий самий закон розподілу.

Позначимо $\Im$ множину значень випадкової матриці A, для кожного з яких алгоритм **A** завершується успішно при всіх його застосуваннях на кроці 1. Далі, для кожного $A^{(0)} \in \Im$ позначимо $\Re(A^{(0)})$ подію, яка полягає в тому, що алгоритм **B** вірно відновлює вектор a на кроці 2 за умови, що $A = A_0$. В силу незалежності матриці A та випадкових величин $\xi_1, \ldots, \xi_m$ ймовірність вірного відновлення вектора a дорівнює

$$\pi_{\mathbf{B}}(P,\theta) = \sum_{A^{(0)} \in \Im} \mathbf{P}\{A = A^{(0)}\}\, \mathbf{P}\{\Re(A^{(0)})\}. \qquad (7)$$

Зафіксуємо матрицю $A^{(0)} \in \Im$ та оцінимо ймовірність події $\Re(A^{(0)})$. Позначимо $L_{i,j}^{(0)}$, $i \in \overline{1,n}$, $j \in \overline{1,t}$, списки, які формується на кроці 1 алгоритму **B** за вхідною матрицею $A^{(0)}$. Помітимо, що на підставі формул (2) та (6) справедливі наступні рівності:

$$a_i = e_i a = b(i,j) \oplus (\xi_{\nu_1(i,j)} \oplus \cdots \oplus \xi_{\nu_r(i,j)}),$$
$$i \in \overline{1,n},\ j \in \overline{1,t}.$$

При цьому числа $\nu_1(i,j), \ldots, \nu_r(i,j)$ є (не обов'язково різними) номерами рядків, що належать списку $L_{i,j}^{(0)}$. Отже, для будь-яких $(i,j) \neq (i',j')$ справедливе співвідношення

$$\{\nu_1(i,j), \ldots, \nu_r(i,j)\} \cap \{\nu_1(i',j'), \ldots, \nu_r(i',j')\} = \varnothing,$$

з якого випливає, що випадкові величини $\xi_{\nu_1(i,j)} \oplus \cdots \oplus \xi_{\nu_r(i,j)}$, $i \in \overline{1,n}$, $j \in \overline{1,t}$, є незалежними в сукупності. Нарешті, на підставі формули (3) та умови $\theta_s \geq \theta > 0$, $s \in \overline{1,m}$, виконується нерівність

$$\mathbf{P}\{\xi_{\nu_1(i,j)} \oplus \cdots \oplus \xi_{\nu_r(i,j)} = 0\} \geq \frac{1}{2}\left(1 + \theta^r\right),$$
$$i \in \overline{1,n},\ j \in \overline{1,t}.$$

Таким чином, для оцінки ймовірності події $\Re(A^{(0)})$ можна скористатися нерівністю Гефдінга (див. лему 1). Згідно з цією нерівністю, ймовірність помилки при відновленні кожного окремого значення a_i, $i \in \overline{1,n}$, на другому кроці алгоритму **B** не перевищує $\exp\{-1/2 \cdot \theta^{2r} t\}$. Отже,

$$\mathbf{P}\{\Re(A^{(0)})\} \geq (1 - \exp\{-1/2 \cdot \theta^{2r} t\})^n.$$

Підставляючи зазначену оцінку в формулу (7), з урахуванням нерівності $\mathbf{P}\{A \in \Im\} \geq (\pi_{\mathbf{A},P})^n$ отримаємо формулу (4). Теорему доведено.

Як видно з доведення, теорема залишається справедливою і в тому випадку, коли алгоритм **A** дозволяє знаходити з ймовірністю не менше за $\pi_{\mathbf{A},P}$ адитивне r-представлення кожного з векторів $e_1, \ldots, e_n$ (але не обов'язково довільного вектора $z \in V_n$). Наведемо конкретний приклад такого алгоритму, що запропоновано в [5].

Лема 2 (*алгоритм BKW*). Нехай u, v, λ – натуральні числа і

$$n \leq uv,\ r = 2^{u-1},\ l = (u + \lambda - 1)2^v. \qquad (8)$$

Тоді існує алгоритм $\mathbf{A}_0$, який знаходить адитивне r-представлення кожного з векторів $e_1, \ldots, e_n$ у випадковому рівноймовірному списку L довжини l з надійністю $\pi_{\mathbf{A}_0} \geq 1 - e^{-\lambda}$, використовуючи $T_{\mathbf{A}_0} = O(u(u+\lambda)2^v)$ операцій над n-вимірними двійковими векторами.

Доведення. Опишемо алгоритм знаходження r-представлення вектора e_1. Адитивні представлення векторів $e_2, \ldots, e_n$ можна побудувати, застосовуючи зазначений алгоритм до списків, які отримуються шляхом циклічного зсуву всіх векторів зі списку L на $1, \ldots, n-1$ позицій відповідно.

Не обмежуючи загальності, вважатимемо, що $n = uv$ (у протилежному випадку допишемо до кожного вектора довжини n необхідну кількість нулів). Отже, будь-який вектор $z \in V_n$ можна розглядати як послідовність u двійкових слів довжини v біт кожне та записувати у вигляді $z = (z^{(1)}, \ldots, z^{(u)})$, де $z^{(i)} \in V_v$, $i \in \overline{1,u}$.

Алгоритм $\mathbf{A}_0$ знаходження адитивного r-представлення вектора e_1 у випадковому рівноймовірному списку $L^{(i)}$ має такий вигляд.

Розіб'ємо вхідний список на блоки, відносячи до одного і того ж блоку L_c ($c \in V_v$) усі вектори $z \in L$ такі, що $z^{(u)} = c$. Зауважимо, що зазначене розбиття можна отримати, використовуючи $O(l)$ операцій, де l – довжина списку L.

Далі для кожного непорожнього блоку L_c виконаємо наступну процедуру: виберемо з блоку L_c випадково та рівноймовірно один вектор, додамо його до кожного іншого вектора з цього блоку та вилучимо зі списку L. В результаті отримаємо новий список $L^{(1)}$, що складається не менше ніж з $l_1 = l - 2^v$ векторів, які задовольняють наступним умовам:

(а) для будь-якого $z \in L^{(1)}$ виконується рівність $z^{(u)} = 0$;

(б) кожен вектор $z \in L^{(1)}$ є сумою точно двох векторів зі списку L;

(в) підвектори, що складаються з перших $u-1$ слів усіх векторів зі списку $L^{(1)}$, є незалежними в сукупності випадковими рівноймовірними векторами довжини $(u-1)v$.

Справедливість тверджень (а) – (в) випливає безпосередньо з наведеного опису процедури формування списку $L^{(1)}$ за списком L і умови випадковості та рівноймовірності останнього.

Далі застосуємо аналогічну процедуру до списку $L^{(1)}$ та отримаємо список $L^{(2)}$, що складається не менше ніж з $l_2 = l - 2^v - 2^v$ векторів, які задовольняють умовам, аналогічним (а) – (в). Продовжуючи зазначений процес, отримаємо послідовність списків $L^{(1)}$, ..., $L^{(u-1)}$ таких, що для кожного $i \in \overline{1,u-1}$ список $L^{(i)}$ складається не менше ніж з $l - i2^v$ векторів z, кожен з яких задовольняє умові $z^{(u-i+1)} = ... = z^{(u)} = 0$ та є сумою точно 2^i векторів зі списку L. При цьому підвектори, що складаються з перших $u-i$ слів усіх векторів зі списку $L^{(i)}$, є незалежними в сукупності випадковими рівноймовірними двійковими векторами довжини $(u-i)v$.

На останньому кроці, при $i = u-1$, отримаємо список $\tilde{L}$, який складається не менше ніж з $\lambda 2^v = l - (u-1)2^v$ незалежних випадкових та рівноймовірних векторів $z^{(1)} \in V_v$ таких, що вектори $(z^{(1)}, 0, ..., 0)$ утворюють список $L^{(u-1)}$. Оскільки ймовірність появи будь-якого фіксованого вектора довжини v у списку $\tilde{L}$ є не менше за $1 - \left(\frac{2^v - 1}{2^v}\right)^{\lambda 2^v} \geq 1 - e^{-\lambda}$, то вектор e_1 зустрінеться у списку $L^{(u-1)}$ з такою самою ймовірністю. При цьому, оскільки кожен вектор з останнього списку є сумою точно $r = 2^{u-1}$ векторів, що належать списку L, то шукане адитивне r-представлення вектора e_1 можна отримати з імовірністю $\pi_{\mathbf{A}_0} \geq 1 - e^{-\lambda}$.

Нарешті, як випливає з наведеного опису алгоритму $\mathbf{A}_0$, його трудомісткість складає $T_{\mathbf{A}_0} = O(ul) = O(u(u+\lambda)2^v)$ операцій. Лему доведено.

В [5] рекомендується вибирати значення параметрів u, v наступним чином:

$$u = \left\lceil \frac{\log n}{2} \right\rceil, \; v = \left\lceil \frac{2n}{\log n} \right\rceil.$$

Нехай для простоти $n = 2^{2^s}$, де $s \in \mathbf{N}$. Тоді

$$u = \frac{\log n}{2}, \; v = \frac{2n}{\log n} \qquad (9)$$

і, згідно зі співвідношеннями (8),

$$2r = \sqrt{n}, \; l = \left(\frac{\log n}{2} + \lambda - 1\right) 2^{\frac{2n}{\log n}}. \qquad (10)$$

Розглянемо систему рівнянь (1), що задовольняє умовам (2) та (3). Як і вище, припустимо, що $\theta_i \geq \theta > 0$ для кожного $i \in \overline{1,m}$ та покладемо

$$t = \left\lceil 2C\theta^{-\sqrt{n}} \ln n \right\rceil, \; \lambda = \left\lceil \ln(tn\delta^{-1}) \right\rceil, \qquad (11)$$

вважаючи, що величини $C > 1$, $\delta \in (0,1)$ і θ є константами (тобто не залежать від n). Позначимо $\mathbf{B}_0$ алгоритм розв'язання системи рівнянь (1) з випадковою рівноймовірною матрицею коефіцієнтів, який будується за алгоритмом $\mathbf{A}_0$ у відповідності з доведенням теореми 1. На підставі цієї теореми та рівностей (9) – (11) справедливі такі співвідношення:

$$m = nlt = O\left(n^{3/2} \log n \log(\theta^{-1}) \, \theta^{-\sqrt{n}} 2^{\frac{2n}{\log n}} \right) = 2^{O\left(\frac{n}{\log n}\right)}, \qquad (12)$$

$$\pi_{\mathbf{B}_0} \geq 1 - tne^{-\lambda} - n\exp\{-1/2 \cdot \theta^{2r} t\} \geq 1 - \delta - n^{1-C}, \qquad (13)$$

$$T_{\mathbf{B}_0} = O\left(n^{3/2} \log^2 n \log(\theta^{-1}) \, \theta^{-\sqrt{n}} 2^{\frac{2n}{\log n}} \right) = 2^{O\left(\frac{n}{\log n}\right)}. \qquad (14)$$

Отже, доведено наступне твердження.

Наслідок 1. За виконанням співвідношень (9) – (12) існує алгоритм, який знаходить істинний розв'язок системи рівнянь (1) зі спотвореною правою та випадковою рівноймовірною лівою частинами з надійністю (13) і трудомісткістю (14).

Відзначимо, що наслідок 1 випливає з основного результату статті [4] і доводиться в [5] (за винятком оцінки надійності алгоритму).

Спираючись на теорему 1, можна побудувати алгоритми розв'язання систем лінійних рівнянь зі спотвореними правими частинами, що базуються на узагальненому алгоритмі Вагнера [9, 10]. Цей алгоритм призначено для знаходження адитивного r-представлення нульового вектора за r незалежними випадковими рівноймовірними списками та є за сутністю близьким до алгоритму BKW. Для зменшення трудомісткості знаходження r-представлення в [10] пропонується розбивати n-вимірні вектори на слова різної довжини (зауважимо, що аналогічна ідея використовується в [12] для побудови оптимальних у певному класі модифікацій алгоритму Коновальцева).

Розв'язання задачі про адитивне представлення є найбільш трудомістким етапом знаходження істинного розв'язку системи рівнянь (1). Отже, будь-який прогрес у вирішенні цієї задачі призведе до зменшення складності алгоритмів розв'язання систем лінійних рівнянь зі спотвореними правими частинами. Найкращі з відомих сьогодні алгоритмів мають ті ж самі асимптотичні характеристики, що й алгоритм, зазначений у наслідку 1: трудомісткість розв'язання системи з $2^{O\left(\frac{n}{\log n}\right)}$ лінійних рівнянь від n невідомих зі спотвореними правими частинами та випадковою рівноймовірною матрицею коефіцієнтів складає $2^{O\left(\frac{n}{\log n}\right)}$ операцій.

2. ПРОЦЕДУРА САМОКОРЕКЦІЇ

У випадку, коли система (1) містить невелику кількість рівнянь або розподіл її матриці коефіцієнтів помітно відрізняється від рівномірного, можна застосовувати так звану процедуру самокорекції, яка має за мету звести знаходження істинного розв'язку цієї системи рівнянь до

розв'язання задачі, що розглянута в попередньому пункті.

Термін "самокорекція" запропоновано в [7] і позначає певну процедуру, що дозволяє отримувати з невеликої кількості незалежних випадкових двійкових векторів, які мають "не надто поганий" розподіл, довільну кількість незалежних векторів, що розподілені "майже" рівномірно.

Сформулюємо точне означення. Нехай G – матриця розміру $T\times n$ з рядками $G_1,\dots,G_T\in V_n$, χ – вектор довжини T з координатами $\chi_1,\dots,\chi_T\in\{0,1\}$. *Процедура самокорекції з параметрами* (m,k), де $m,k\in\mathbf{N}$, полягає у застосуванні до вхідних даних (G,χ) наступного алгоритму.

Для кожного $i\in\overline{1,m}$:

1) згенерувати незалежні в сукупності випадкові величини $\mu_{1,i},\dots,\mu_{k,i}$ з рівномірним розподілом на множині $\overline{1,T}$;

2) обчислити

$$X_i=G_{\mu_{1,i}}\oplus\dots\oplus G_{\mu_{k,i}},\ \xi_i=\chi_{\mu_{1,i}}\oplus\dots\oplus\chi_{\mu_{k,i}}.$$

Результатом виконання алгоритму є список, що складається з m випадкових векторів (X_i,ξ_i), $i\in\overline{1,m}$. Зрозуміло, що зазначені вектори є незалежними в сукупності та однаково розподіленими на множині V_{n+1}, і основне питання полягає в тому, за яких умов вектор X_i має "майже" рівномірний розподіл на V_n, а випадкова величина ξ_i "майже" не залежить від вектора X_i. Більш точно, позначимо $P_{X,\xi}$ сумісний розподіл ймовірностей випадкових елементів $X=G_{\mu_1}\oplus\dots\oplus G_{\mu_k}$ та $\xi=\chi_{\mu_1}\oplus\dots\oplus\chi_{\mu_k}$ (опускаючи для простоти позначень індекс i). Розглянемо також розподіл ймовірностей $U_\xi(x,u)=2^{-n}\mathbf{P}\{\xi=u\}$, $(x,u)\in V_{n+1}$. Потрібно оцінити відстань по варіації між зазначеними розподілами на множині V_{n+1}.

Нагадаємо, що відстань по варіації між розподілами ймовірностей P та Q на довільній скінченній множині Ω визначається за формулою

$$d(P,Q)=\frac{1}{2}\sum_{\omega\in\Omega}|P(\omega)-Q(\omega)|.$$

Наступне добре відоме твердження, доведення якого неважко отримати безпосередньо з означення відстані по варіації, містить основні властивості цього параметра, що використовуються далі.

Лема 3 (*властивості відстані по варіації*).

1. Для будь-яких розподілів ймовірностей P, Q на скінченній множині Ω справедлива рівність $d(P,Q)=\max\limits_{B\subseteq\Omega}\{|P(B)-Q(B)|\}$.

2. Нехай $\Omega=\Omega_1\times\dots\times\Omega_m$, P_i,Q_i – розподіли ймовірностей на множині Ω_i, $i\in\overline{1,m}$. Позначимо $P=P_1\times\dots\times P_m$, $Q=Q_1\times\dots\times Q_m$. Тоді

$$d(P,Q)\le\sum_{i=1}^m d(P_i,Q_i).$$

Доведемо зараз лему, яка встановлює верхню оцінку відстані по варіації між розподілами ймовірностей $P_{X,\xi}$ та U_ξ.

Лема 4. Нехай G – $T\times n$-матриця з рядками $G_1,\dots,G_T\in V_n$, χ – T-вимірний вектор з координатами $\chi_1,\dots,\chi_T\in\{0,1\}$, $X=G_{\mu_1}\oplus\dots\oplus G_{\mu_k}$, $\xi=\chi_{\mu_1}\oplus\dots\oplus\chi_{\mu_k}$, де $\mu_1,\dots,\mu_k$ – незалежні випадкові величини з рівномірним розподілом на множині $\overline{1,T}$. Тоді справедлива нерівність

$$d(P_{X,\xi},U_\xi)=\frac{1}{2}\sum_{\substack{x\in V_n,\\ u\in\{0,1\}}}|\mathbf{P}\{X=x,\xi=u\}-2^{-n}\mathbf{P}\{\xi=u\}|\le$$

$$\le 2^n(\Delta_{G,\chi})^k, \qquad (15)$$

де

$$\Delta_{G,\chi}=T^{-1}\max_{\substack{y\in V_n\setminus\{0\},\\ u\in\{0,1\}}}\left|\sum_{j=1}^T(-1)^{G_jy\oplus u\chi_j}\right|. \qquad (16)$$

Доведення. Позначимо

$$\varphi_k(y,w)=\left(T^{-1}\sum_{j=1}^T(-1)^{G_jy\oplus w\chi_j}\right)^k,\ (y,w)\in V_{n+1}. \qquad (17)$$

За допомогою безпосередньої перевірки неважко переконатися в тому, що для будь-якого $(x,u)\in V_{n+1}$ виконуються рівності

$$\mathbf{P}\{X=x,\xi=u\}=2^{-(n+1)}\sum_{(y,w)\in V_{n+1}}(-1)^{xy\oplus uw}\varphi_k(y,w),$$

$$\mathbf{P}\{\xi=u\}=\frac{1}{2}\left(1+(-1)^u\left(T^{-1}\sum_{j=1}^T(-1)^{\chi_j}\right)^k\right)=$$

$$=\frac{1}{2}\left(1+(-1)^u\varphi_k(0,1)\right). \qquad (18)$$

Звідси випливає, що

$$\mathbf{P}\{X=x,\xi=u\}-2^{-n}\mathbf{P}\{\xi=u\}=2^{-(n+1)}\times$$

$$\times\left(\sum_{y\in V_n\setminus\{0\}}(-1)^{xy}\varphi_k(y,0)+(-1)^u\sum_{y\in V_n\setminus\{0\}}(-1)^{xy}\varphi_k(y,1)\right)$$

і, отже, на підставі формул (16) та (17)

$$|\mathbf{P}\{X=x,\xi=u\}-2^{-n}\mathbf{P}\{\xi=u\}|\le 2^{-(n+1)}\times$$

$$\times\left(2^n\max_{y\in V_n\setminus\{0\}}|\varphi_k(y,0)|+2^n\max_{y\in V_n\setminus\{0\}}|\varphi_k(y,1)|\right)\le$$

$$\le(\Delta_{G,\chi})^k.$$

З отриманої нерівності випливає формула (15). Лему доведено.

Отже, близкість сумісного розподілу випадкових елементів X та ξ до розподілу ймовірностей U_ξ на множині V_{n+1} визначається параметром (16). Відзначимо теоретико-кодовий сенс цього параметра.

Позначимо $C(G,\chi)$ лінійний код з твірною матрицею $\begin{pmatrix}G^T\\ \chi\end{pmatrix}$, тобто код довжини T, що складається зі слів вигляду $Gy\oplus u\chi$, де $(y,u)\in V_{n+1}$. Неважко бачити, що величина $T^{-1}\sum\limits_{j=1}^T(-1)^{G_jy\oplus u\chi_j}$ дорівнює $1-2wt(Gy\oplus u\chi)$, де є $wt(Gy\oplus u\chi)$ є

відносною вагою слова $Gy \oplus u\chi$ коду $C(G,\chi)$. Отже, параметр $\Delta_{G,\chi}$ співпадає з найменшим числом $\Delta \in [0,1]$, для якого відносна вага кожного слова $Gy \oplus u\chi$ коду $C(G,\chi)$, де $y \neq 0$, знаходиться в межах від $\frac{1}{2}(1-\Delta)$ до $\frac{1}{2}(1+\Delta)$.

Назвемо код $C(G,\chi)$ γ *-збалансованим*, якщо виконується умова $\Delta_{G,\chi} \le T^{-\gamma}$, де $\gamma > 0$.

Безпосередньо з леми 4 випливає такий результат.

Наслідок 2. Нехай $C(G,\chi) \in$ γ -збалансованим кодом,

$$k = \left\lceil \frac{(1+c)n}{\gamma \log T} \right\rceil,\ c > 0. \qquad (19)$$

Тоді в умовах леми 4 справедлива нерівність

$$d(P_{X,\xi}, U_\xi) \le 2^{-cn}. \qquad (20)$$

Отже, для γ -збалансованих кодів відстань по варіації між розподілами ймовірностей $P_{X,\xi}$ та U_ξ на множині V_{n+1} експоненційно швидко прямує до нуля при $n \to \infty$, якщо k визначається за формулою (19), де $c = const$.

Як показує наступна лема, властивістю γ -збалансованості з високою ймовірністю володіють певні випадкові коди.

Лема 5. Нехай рядки $T \times n$ -матриці G є незалежними випадковими рівноймовірними векторами на множині V_n, а координати вектора χ – незалежними випадковими величинами, що не залежать від матриці G. Нехай, далі, $T = n^{1+\alpha}$, де $\alpha > 0$,

$$\gamma = \frac{\alpha(1-c)}{2(1+\alpha)},\ 0 < c < 1. \qquad (21)$$

Тоді випадковий код $C(G,\chi)$ є γ -збалансованим з імовірністю біля $1 - 2^{1-n}$.

Доведення. З умови леми випливає, що для будь-яких $y \in V_n \setminus \{0\}$, $u \in \{0,1\}$ випадкові величини $(-1)^{G_j y \oplus u\chi_j}$, $j \in \overline{1,T}$, є незалежними та рівноймовірними. Отже, на підставі леми 1

$$\mathbf{P}\{\Delta_{G,\chi} > T^{-\gamma}\} =$$

$$= \mathbf{P}\left\{ \max_{y \in V_n \setminus \{0\}} \left| T^{-1} \sum_{j=1}^{T} (-1)^{G_j y \oplus u\chi_j} \right| > T^{-\gamma} \right\} <$$

$$< 2^n \cdot 2\exp\{-2T(T^{-\gamma})^2\} < 2^{n+1-2T^{1-2\gamma}}.$$

Далі, згідно з рівністю $T = n^{1+\alpha}$ та формулою (21),

$$n + 1 - 2T^{1-2\gamma} = n + 1 - 2n^{(1+\alpha)(1-2\gamma)} < n + 1 - 2n = 1 - n,$$

звідки випливає, що $\mathrm{P}\{\Delta_{G,\chi} > T^{-\gamma}\} < 2^{1-n}$. Лему доведено.

3. ЗАСТОСУВАННЯ САМОКОРЕКЦІЇ ДО РОЗВ'ЯЗАННЯ СИСТЕМ ЛІНІЙНИХ РІВНЯНЬ ЗІ СПОТВОРЕНИМИ ПРАВИМИ ЧАСТИНАМИ

Даний пункт присвячено доведенню теореми Любашевського [6] про можливість розв'язання за суб'експоненційний час системи лінійних рівнянь зі спотвореними правими частинами та випадковою рівноймовірною матрицею коефіцієнтів розміру $T \times n$, де $T = n^{1+\alpha}$, $\alpha > 0$. Доведення, що наводиться нижче, використовує основну ідею роботи [6], але проводиться іншим, більш простим методом. Наводиться також вираз оцінки надійності алгоритму розв'язання заданої системи рівнянь, який відсутній у [6].

Розглянемо систему рівнянь

$$Gx = h, \qquad (22)$$

де G – випадкова рівноймовірна булева матриця розміру $T \times n$, h – вектор з координатами

$$h_i = G_i a \oplus \chi_i,\ i \in \overline{1,T}, \qquad (23)$$

$G_1, \ldots, G_T$ – рядки матриці G, $a = (a_1, \ldots, a_n)^T \in V_n$ – невідомий істинний розв'язок системи рівнянь (22), $\chi_1, \ldots, \chi_T$ – незалежні випадкові величини, розподілені за законами

$$\mathbf{P}\{\chi_i = 0\} = 1 - \mathbf{P}\{\chi_i = 1\} = \frac{1}{2}(1 + \theta_i),\ i \in \overline{1,T}, \qquad (24)$$

де $\theta_i \ge \theta > 0$ для кожного $i \in \overline{1,T}$.

Ідея побудування суб'експоненційного алгоритму розв'язання системи (22) полягає в наступному. Застосуємо до вхідних даних (G,h) процедуру самокорекції з параметрами (m,k) та подамо отриманий список векторів

$$(A_i = G_{\mu_{1,i}} \oplus \cdots \oplus G_{\mu_{k,i}},$$

$$b_i = A_i a \oplus (\chi_{\mu_{1,i}} \oplus \cdots \oplus \chi_{\mu_{k,i}}))\ ,\ i \in \overline{1,m}, \qquad (25)$$

на вхід довільного алгоритму **B**, який дозволяє розв'язувати системи рівнянь вигляду (1) з певній надійністю $\pi_{\mathbf{B}}(\theta)$ за суб'експоненційний від n час. Згідно з наслідком 2 та лемою 5, вибираючи належним чином параметр k, можна добитися того, щоб випадкові вектори A_i були "майже" рівноймовірними на множині V_n, а випадкові величини $\xi_i = \chi_{\mu_{1,i}} \oplus \cdots \oplus \chi_{\mu_{k,i}}$ "майже" не залежили від A_i, $i \in \overline{1,m}$. Звідси, спираючись на лему 3, неважко вивести, що ймовірність вірного відновлення вектора a з отриманої після самокорекції системи рівнянь "майже" не відрізняється від $\pi_{\mathbf{B}}(\theta^k)$. Нарешті, спираючись на теорему 1, можна вибрати параметр m таким чином, щоби сумарний час відновлення вектора a (за допомогою процедури самокорекції та алгоритму **B**) суб'експоненційно залежав від n.

В [6] пропонується використовувати в ролі **B** алгоритм із [5], а замість самокорекції застосовувати декілька іншу процедуру, яка полягає в додаванні k різних рядків розширеної матриці системи (22), що вибираються за урновою схемою без повернення. Зазначимо, що аналогічна процедура використовується на першому кроці алгоритму Коваленка [4], а також у деяких інших алгоритмах розв'язання систем лінійних рівнянь зі спотвореними правими частинами [13]. Проте обидві ймовірнісні схеми (рівноймовірного вибору рядків з поверненням чи без нього) приводять

до однакових асимптотичних оцінок трудомісткості алгоритмів, а незалежний рівноймовірний вибір рядків, що здійснюється при виконанні самокорекції, дозволяє помітно спростити ймовірнісний аналіз.

Перейдемо до більш точного викладення наведених міркувань. Перш за все, доведемо просту лему, яка встановлює зв'язок між значеннями надійності будь-якого алгоритму розв'язання системи рівнянь (1) при різних розподілах ймовірностей рядків її матриці коефіцієнтів та спотворень у правій частині.

Лема 6. Нехай $\pi_{\mathbf{B}}(P_1)$ і $\pi_{\mathbf{B}}(P_2)$ – ймовірності вірного відновлення істинного розв'язку системи рівнянь (1) з використанням довільного алгоритму $\mathbf{B}$ за умови, що випадкові вектори (A_i,ξ_i), $i\in\overline{1,m}$, є незалежними в сукупності та розподілені за законами P_1 і P_2 відповідно. Тоді

$$|\pi_{\mathbf{B}}(P_1)-\pi_{\mathbf{B}}(P_2)|\le m\,d(P_1,P_2)\,. \qquad (26)$$

Доведення. Нерівність (26) випливає безпосереньо з тверджень 1 і 2 леми 3.

Наступна лема містить основні властивості випадкових векторів (25), які формуються за вхідною системою рівнянь (22).

Лема 7. Нехай виконуються умови леми 5 та рівності (19), (24). Тоді для будь-яких $\varepsilon\in(0,\theta)$ та $i\in\overline{1,m}$ з імовірністю не менше за $1-2^{1-n}-\exp\{-2n^{1+\alpha}\varepsilon^2\}$ (відносно розподілу пари (G,χ)) виконуються наступні твердження:

1) відстань по варіації між розподілом випадкового вектора

$$(A_i=G_{\mu_{1,i}}\oplus\cdots\oplus G_{\mu_{k,i}},\ \xi_i=\chi_{\mu_{1,i}}\oplus\cdots\oplus\chi_{\mu_{k,i}})$$

та розподілом ймовірностей $U_{\xi_i}(x,u)=2^{-n}\mathbf{P}\{\xi_i=u\}$, $(x,u)\in V_{n+1}$, не перевищує 2^{-cn};

2) випадкова величина ξ_i приймає значення, що дорівнює нулю, з імовірністю не менше за $\frac{1}{2}\left(1+(\theta-\varepsilon)^k\right)$.

Доведення. Позначимо $\Im_1$ та $\Im_2$ події (у просторі значень випадкового елементу (G,χ)), що полягають у невиконанні умови 1) та умови 2) відповідно. На підставі наслідку 2 і леми 5 справедлива нерівність $\mathbf{P}_{G,\chi}(\Im_1)<2^{1-n}$.

Для оцінки ймовірності події $\Im_2$ скористаємося формулою (18), у відповідності з якою

$$\mathbf{P}\{\xi_i=0\}=\frac{1}{2}\left(1+\left(T^{-1}\sum_{j=1}^{T}(-1)^{\chi_j}\right)^k\right).$$

Використовуючи лему 1, отримаємо, що

$$\mathbf{P}_{G,\chi}(\Im_2)=\mathbf{P}_{G,\chi}\left\{\mathbf{P}\{\xi_i=0\}<\frac{1}{2}\left(1+(\theta-\varepsilon)^k\right)\right\}\le$$

$$\mathbf{P}_{\chi}\left\{T^{-1}\sum_{j=1}^{T}(-1)^{\chi_j}<\theta-\varepsilon\right\}\le$$

$$\le\mathrm{P}_{\chi}\left\{T^{-1}\sum_{j=1}^{T}(-1)^{\chi_j}-T^{-1}\sum_{j=1}^{T}\theta_j<-\varepsilon\right\}\le$$

$$\le\exp\{-2T\varepsilon^2\}=\exp\{-2n^{1+\alpha}\varepsilon^2\}\,.$$

Таким чином, на підставі отриманих нерівностей

$$1-\mathrm{P}_{G,\chi}(\Im_1\cup\Im_2)\ge 1-2^{1-n}-\exp\{-2n^{1+\alpha}\varepsilon^2\}\,,$$

що й треба було довести.

Сформулюємо, нарешті, основний результат даного пункту.

Теорема 2. Нехай $\mathbf{B}$ – довільний алгоритм, що дозволяє відновлювати істинний розв'язок системи рівнянь (1), яка задовольняє умовам (2), (3) і має випадкову рівноймовірну матрицю коефіцієнтів розміру $m\times n$, з надійністю $\pi_{\mathbf{B}}(\theta)$ і трудомісткістю $T_{\mathbf{B}}$.

Розглянемо систему рівнянь (22), що задовольняє умовам (23), (24) і має випадкову рівноймовірну матрицю коефіцієнтів розміру $T\times n$, де $T=n^{1+\alpha}$, $\alpha>0$. Позначимо $\mathbf{B}'$ алгоритм розв'язання цієї системи рівнянь, який складається з наступних кроків.

1. Покласти

$$k=\left\lceil\frac{2n}{\alpha\log n}\left(\frac{1+c}{1-c}\right)\right\rceil,\ 0<c<1 \qquad (27)$$

та застосувати процедуру самокорекції з параметрами (m,k) до вхідних даних (G,h).

2. Подати отриманий список вигляду (25) на вхід алгоритму $\mathbf{B}$ та знайти за допомогою останнього шуканий вектор a.

Тоді алгоритм $\mathbf{B}'$ дозволяє відновлювати істинний розв'язок системи рівнянь (22) з ймовірністю

$$\pi_{\mathbf{B}'}(\theta)\ge\left(1-2^{1-n}-\exp\{-2n^{1+\alpha}\varepsilon^2\}\right)\times$$
$$\times\left(\pi_{\mathbf{B}}\left((\theta-\varepsilon)^k\right)-2^{-cn}m\right), \qquad (28)$$

де ε – довільне число з інтервалу $(0,\theta)$ (за умови, що обидва співмножники у правій частині формули (28) є додатними числами), використовуючи

$$T_{\mathbf{B}'}=O(T_{\mathbf{B}}+mk) \qquad (29)$$

операцій над n-вимірними двійковими векторами.

Доведення. Справедливість формули (29) випливає безпосередньо з означення алгоритму $\mathbf{B}'$. Далі, значення (27) отримується шляхом підстановки виразу (21) у формулу (19) і для доведення нерівності (28) достатньо скористатися твердженнями лем 6 та 7.

Дійсно, згідно з лемою 7, сумарна ймовірність пар (G,χ), для яких виконуються обидва твердження 1) і 2), є не менше за $1-2^{1-n}-\exp\{-2n^{1+\alpha}\varepsilon^2\}$. При цьому на підставі зазначених тверджень та нерівності (26) для кожної з цих пар ймовірність вірного відновлення вектора a на другому кроці алгоритму $\mathbf{B}'$ є не менше за $\pi_{\mathbf{B}}\left((\theta-\varepsilon)^k\right)-2^{-cn}m$.

Теорему доведено.

З наведеної теореми неважко отримати один з основних результатів роботи [6] про існування алгоритму розв'язання системи рівнянь (22) зі складністю $2^{O\left(\frac{n}{\log\log n}\right)}$.

Розглянемо в ролі **В** алгоритм розв'язання системи рівнянь (1), який будується у відповідності з доведенням теореми 1 за алгоритмом BKW з параметрами $u=\left\lceil \frac{\log\log n}{2} \right\rceil$ та $v=\left\lceil \frac{2n}{\log\log n} \right\rceil$ (див. лему 2). Нехай для простоти

$$u=\frac{\log\log n}{2},\ v=\frac{2n}{\log\log n}.$$

Тоді на підставі формул (8) та (27)

$$2r=2^u=\sqrt{\log n},$$

$$2rk=\frac{2n}{\sqrt{\log n}}\left(\frac{1+c}{1-c}\right)=O\left(\frac{n}{\sqrt{\log n}}\right).$$

Позначимо $\theta_\varepsilon=\theta-\varepsilon$ і покладемо

$$t=\left\lceil 2C\,\theta_\varepsilon^{-2rk}\ln n \right\rceil,\ \lambda=\left\lceil \ln(tn\delta^{-1}) \right\rceil,$$

вважаючи, що величини $C>1$, $\delta\in(0,1)$ і θ є константами (тобто не залежать від n). На підставі леми 2 і теореми 1 справедливі наступні нерівності:

$$\pi_{\mathbf{B}}\left(\theta_\varepsilon^{\,k}\right)\ge(1-e^{-\lambda})^{tn}(1-\exp\{-1/2\cdot\theta_\varepsilon^{\,2kr}t\})^n\ge$$

$$\ge 1-tne^{-\lambda}-n\exp\{-1/2\cdot\theta_\varepsilon^{\,2kr}t\}\ge 1-\delta-n^{1-C}.$$

Крім того,

$$m=nlt=nt(\lambda+u-1)2^v=$$

$$=O\left(n^2\sqrt{\log n}\,\log(\theta_\varepsilon^{-1})\,\theta_\varepsilon^{-2kr}2^{\frac{2n}{\log\log n}}\right)=$$

$$2^{O\left(\frac{n}{\log\log n}\right)}$$

і, отже,

$$T_{\mathbf{B}}=O(unlt)=O(um)=2^{O\left(\frac{n}{\log\log n}\right)}.$$

Підставляючи зазначені оцінки в формули (28), (29), отримаємо, що

$$\pi_{\mathbf{B}'}(\theta)\ge\left(1-2^{1-n}-\exp\{-2n^{1+\alpha}\varepsilon^2\}\right)\times$$

$$\times\left(1-\delta-n^{1-C}-2^{-cn}m\right),\qquad(30)$$

за умови, що обидва співмножники у правій частині цієї нерівності є додатними числами;

$$T_{\mathbf{B}'}=O(T_{\mathbf{B}}+mk)=2^{O\left(\frac{n}{\log\log n}\right)}.\qquad(31)$$

Таким чином, доведено наступне твердження [6].

Наслідок 3. Нехай система рівнянь (22) задовольняє умовам (23), (24) і має випадкову рівноймовірну матрицю коефіцієнтів розміру $T\times n$, де $T=n^{1+\alpha}$, $\alpha>0$. Тоді існує алгоритм, який знаходить істинний розв'язок цієї системи рівнянь з надійністю (30) і трудомісткістю (31).

ВИСНОВКИ

Найбільш трудомістким етапом суб'експоненційних алгоритмів розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами [4–6] є знаходження адитивних представлень певних булевих векторів у списку, що складається з рядків матриці коефіцієнтів заданої системи рівнянь. Для розв'язання останньої задачі (за умови незалежного, випадкового та рівноймовірного вибору зазначених рядків) можна використовувати алгоритми BKW [5], Вагнера [9] або узагальнення останнього алгоритму, запропоноване Міндером і Синклером [10].

Алгоритм Вагнера є менш трудомістким у порівнянні з алгоритмом BKW, але має ту ж саму асимптотичну часову складність, що й останній. Обидва зазначених алгоритми дозволяють розв'язувати системи з $2^{O\left(\frac{n}{\log n}\right)}$ лінійних рівнянь від n невідомих зі спотвореними правими частинами та випадковими рівноймовірними матрицями коефіцієнтів, використовуючи $2^{O\left(\frac{n}{\log n}\right)}$ операцій. Алгоритми з [5, 9, 10] базуються на ідеї одночасного виключення декількох невідомих, яка лежить в основі алгоритму Коновальцева розв'язання систем лінійних алгебраїчних рівнянь над скінченним полем. При цьому в [10] для зменшення трудомісткості алгоритму пропонується розбивати вхідні вектори на слова різної довжини (зауважимо, що аналогічна ідея використовується в [12] для побудови оптимальних у певному класі модифікацій алгоритму Коновальцева).

У випадку, коли вхідна система містить невелику кількість рівнянь або розподіл її матриці коефіцієнтів помітно відрізняється від рівномірного, можна використовувати алгоритм, наведений у формулюванні теореми 2. Зазначений алгоритм базується на ідеях робіт [6, 7] і дозволяє розв'язувати системи з $n^{1+\alpha}$ ($\alpha>0$) лінійних рівнянь від n невідомих зі спотвореними правими частинами та випадковими рівноймовірними матрицями коефіцієнтів за $2^{O\left(\frac{n}{\log\log n}\right)}$ операцій.

З практичного погляду, важливою задачею подальших досліджень є отримання оцінок надійності й трудомісткості алгоритмів розв'язання задачі про адитивне представлення [5, 9, 10] у випадку нерівномірного розподілу векторів, що утворюють вхідні списки. Цікавим є також питання про оптимальність зазначених алгоритмів. Зауважимо, що, згідно з [14], алгоритм Коновальцева є асимптотично оптимальним у класі таких алгоритмів розв'язання невироджених систем лінійних рівнянь над скінченним полем, які базуються на елементарних перетвореннях рядків їх матриць коефіцієнтів.

Литература

[1] *Балакин Г.В.* Введение в теорию случайных систем уравнений // Труды по дискретной математике. – М.: ТВП. – 1997. – Т. 1. – С. 1–18.

[2] *Левитская А.А.* Системы случайных уравнений над конечными алгебраическими структурами //

Кибернетика и системный анализ. – 2005. – Т. 41, № 1. – С. 82–116.

[3] *Berlekamp E.R.*, *McElice R.J.*, *van Tilborg H.* On the inherent intractability of certain coding problems // IEEE Trans. Inform. Theory. – 1978. – Vol. 24. – № 3. – P. 384 – 386.

[4] *Коваленко І.М.* Про алгоритм суб'експоненційної складності декодування сильно спотворених лінійних кодів // Доп. АН УРСР. Сер. А. – 1988. – № 10. – С. 16 – 17.

[5] *Blum A.*, *Kalai A.*, *Wasserman H.* Noise-tolerant learning, the parity problem, and the statistical query model // J. ACM. – 2003. – Vol. 50. – № 3. – P. 506 – 519.

[6] *Lyubashevsky V.* The pariry problem in the presence of noise, decoding random linear codes, and the subset sum problem // APPROX and RANDOM'05, Proceedings. – Springer Verlag, 2005. – P. 378 – 389.

[7] *Kopparty S.*, *Saraf S.* Local list decoding and testing of random linear codes from high-error // http://web.mit.edu/swastik/www/papers.

[8] *Bhattacharyya A.*, *Indyk P.*, *Woodruff D.P.*, *Xie N.* The complexity of linear dependence problems in vector spaces // Innovations in Computer Science – ICS 2010, Bijing, China, Jan. 7 – 9, 2011, Proceedings. – P. 496 – 508.

[9] *Wagner D.* A generalized birthday problem // Advances in Cryptology – CRYPTO'02, Proceedings. – Springer Verlag, 2002. – P. 288 – 303.

[10] *Minder L., Sinclair A.* The extended k-tree algorithm // The 19th Annual ACM-SIAM Sympposium on Discrete Algorithms, Proceedings, 2009. – P. 586 – 595.

[11] *Hoeffding W.* Probability inequalities for sums of bounded random variables // J. Amer. Statist. Assoc. – 1963. – Vol. 58. – № 301. – P. 13 – 30.

[12] *Гаврилкевич М.В.*, *Солодовников В.И.* Эффективные алгоритмы решения задач линейной алгебры над полем из двух элементов // Обозрение прикл. промышл. матем. – 1995. – Т. 2. – Вып. 3. – С. 400–437.

[13] *Johansson T.*, *Jonsson F.* Fast correlation attacks through reconstruction linear polynomials // Advances in Cryptology – CRYPTO'00, Proceedings. – Springer Verlag, 2000. – P. 300 – 315.

[14] *Глухов М.М.* О сложности решения систем линейных уравнений над конечным коммутативным цепным кольцом // Труды по дискретной математике. – М.: ФИЗМАТЛИТ. – 2002. – Т. 6. – С. 14–30.

Надійшла до редколегії 14.02.2012

Олексійчук Антон Миколайович, доктор технічних наук, професор кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ". Область наукових інтересів: теоретична криптографія.

УДК 621.391:519.2

Субъэкспоненциальные алгоритмы решения систем линейных булевых уравнений с искаженными правыми частями / А.Н. Алексейчук // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 128–136.

Описана общая схема построения известных субъэкспоненциальных алгоритмов решения систем линейных булевых уравнений с искаженными правыми частями. Выделены и проанализированы важнейшие вспомогательные задачи и процедуры, используемые в указанных алгоритмах, получены неасимптотические оценки их надежности. Изложенные результаты могут быть использованы при решении ряда задач криптоанализа и теории выведывания.

Ключевые слова: система линейных уравнений с искаженными правыми частями, задача об аддитивном представлении, субъэкспоненциальный алгоритм, корреляционный криптоанализ.

Библиогр.: 14 назв.

UDC 621.391:519.2

Sub-exponential algorithms for solving systems of linear Boolean equations with noised right-hand side / A.N. Alekseichuk // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 128–136.

A general framework for constructing the known sub-exponential algorithms for solving systems of linear Boolean equations with noised right-hand side is described. Significant problems and procedures used in these algorithms are considered and analysed. The obtained results can be used in solving some problems from cryptanalysis and learning theory.

Keywords: system of linear equations with noised right-hand side, additive representation theory, sub-exponential algorithm, correlation cryptanalysis.

Ref.: 14 items.