В чому сутність методу квадратичного або загального решета числового поля при факторизації RSA модуля та їх можливості?

28. 4. Метод факторизації «квадратичне решето»

Розглянемо двійкове решето, яке, відповідно до сучасних поглядів, є найбільш швидким при довжині модуля не більше ніж 120 десяткових цифр.

Необхідно знайти два випадкові цілі числа *x* та *y* – такі, що: $x^2 = y^2 (\mathrm{mod}\, N)$.

Представимо у вигляді $x^2 - y^2 \equiv 0(\mathrm{mod}\, N)$.З урахуванням того, що в порівнянні операції виконуються за модулем *N*, його можна подати у вигляді рівняння: $x^2 - y^2 = kN$, k=1,2,... (9.8)

Якщо розкласти (9.8) як різницю квадратів, то отримаємо, що

$(x-y)(x+y) = kN$, k =1, 2, … . (9.9)

причому $N = P \times Q$.

Вираз (9.9) доцільно застосовувати в таких випадках:

$$1.\ (x-y)/N;$$
$$2.\ (x+y)/N;$$
$$3.\ (\mathrm{x}-\mathrm{y})/\mathrm{P} \vee (\mathrm{x}+\mathrm{y})/\mathrm{Q};$$
$$4.\ (\mathrm{x}-\mathrm{y})/\mathrm{Q} \wedge (\mathrm{x}+\mathrm{y})/\mathrm{P}.$$

(9.10)

У випадках 1 і 2 *P* або *Q* знайти не можна, оскільки модуль *N* не може бути розкладеним на співмножники. У випадках 3 та 4 маємо розв'язок.

Далі, якщо (x–y)/P, то ми можемо скористатися алгоритмом Евкліда та обчислити найбільший спільний дільник:

$$\begin{cases} НСД(x-y, N); \\ НСД(x+y, N). \end{cases}$$

(9.11)

Враховуючи (9.11), можна обчислити P або Q.

Практично факторизацію модуля *N* з використанням двійкового решета можна здійснити в такій послідовності.

1. Нехай N – число, яке необхідно факторизувати. Побудуємо деяку базу $Z = P_1 * P_2 * P_3 ... P_K$ з таким значенням Z, щоб $Z \approx N$, де $P_1, P_2, P_3, ... P_K$ – прості числа, краще невеликого розміру, Z – база двійкового решета.

2. Знайдемо $\lfloor \sqrt{N} \rfloor$, округливши знизу. Потім побудуємо числа вигляду

$(i + \sqrt{N})$ (9.12)

і знайдемо

$(i + \sqrt{N})^2 \bmod N = S^2$.

Як результат отримаємо порівняння:

$(i + \sqrt{N})^2 \equiv S^2 (\mathrm{mod}\, N)$.

Таким чином, маємо

$$X^2 = Y^2 (\mathrm{mod}\, N)\,. \quad (9.13)$$

Приклад 9.3 [13]. Зловмисник визначив, що направлене шифрування виконується на відкритому ключі отримувача $E_к$=31, модуль перетворення N=3599. Необхідно знайти особистий ключ отримувача D_k, з використанням якого можна здійснити розшифрування повідомлення M, якщо застосовується RSA перетворення.

Розв'язання задачі може здійснюватись у такому порядку:

1. Факторизуємо модуль N і визначаємо прості числа P та Q.
2. Знаходимо значення функції

$$\varphi(N) = \varphi(P \cdot Q) = \varphi(P) \cdot \varphi(Q).$$

3. Розв'язуємо порівняння

$$E_k \cdot D_k \equiv 1 (\mathrm{mod}\, \varphi(n)).$$

Факторизацію виконуємо, використовуючи метод двійкового решета.

Спочатку визначаємо базу розкладу – прості невеликі числа p_1, p_2,... $p_г$, добуток яких $P_б$ є близьким до N=3599:

$$P_б = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 = 3570.$$

Знаходимо

$$\left|\sqrt{N}\right| = \left|\sqrt{3570}\right| = 59.$$

Реалізація двійкового решета (розрахунки)

x	$Z = x + \left\|\sqrt{N}\right\|$	Z^2mod3599	2	3	5	7	17	лишок
1	60	1	–	–	–	–	–	1
2	61	122	1	–	–	–	–	61
3	62	245	–	–	1	2	–	–
4	63	370	1	–	1	–	–	37
14	73	1730	1	–	1	–	–	173
23	82	3125	–	–	5	–	–	–
26	85	27	–	3	–	–	–	–
49	108	867	–	1	–	–	2	–
61	120	4	2	–	–	–	–	–
62	121	245	–	–	1	2	–	–

Беремо рядки зі значеннями x=3 та x=62, у результаті маємо, що:

$$62^2 = 5 \cdot 7^2 = 245;$$

$$121^2 = 5 \cdot 7^2 = 245.$$

Перемноживши рядки, маємо

$$(62 \cdot 121)^2 = 5 \cdot 7^2 = 245$$

або

$$(7502)^2 = (245)^2 (\mathrm{mod}\, 3599).$$

Знайшовши залишок від значення 7502, маємо

$$(304)^2 = (245)^2 (\mathrm{mod}\, 3599).$$

Отже x=304, y=245.

Далі

НСД ($\left|304\text{-}245\right|$,3599)=59=P,

$$Q = \frac{N}{P} = \frac{3599}{59} = 61.$$

Отже, P=59, Q=61.

Далі знаходимо

$$\varphi(N) = \varphi(59 \cdot 61) = \varphi(59) \cdot \varphi(61) = 3480\,.$$

Тепер порівняння має такий вигляд:

$$E_k \cdot D_k = 1 (\mathrm{mod} 3480).$$

Після переходу до рівняння

$$31 \cdot D - 3480 \cdot K = 1,$$

подамо його у вигляді:

$$3480 \cdot (-K) + 31 \cdot D = 1.$$

Розв'язуємо це діафантове рівняння, використовуючи ланцюгові дроби:

$$\frac{3480}{31} = 112 + \frac{8}{31}; \; r_0=112;$$

$$\frac{31}{8} = 3 + \frac{7}{8}; \; r_1=3;$$

$$\frac{8}{7} = 1 + \frac{1}{7}; \; r_2=1;$$

$$\frac{7}{1} = 7 + \frac{0}{1}; \; r_3=7; \; \mu=3;$$

$$D = (-1)^{\mu} a_{\mu-1} + a_{\mu-2};$$

$$a_0 = r_0 = 112;$$

$$a_1 = r_1 \cdot a_0 + 1 = 3 \cdot 112 + 1 = 337;$$

$$a_2 = r_2 \cdot a_1 + a_0 = 1 \cdot 337 + 112 = 449;$$

$$D = (-1)^3 \cdot 449 (\mathrm{mod}\, 3480) = 3031.$$

Перевіримо правильність розв'язку:

$$E_k \cdot D_k = 31 \cdot 3031 (\mathrm{mod}\, 3480) = 1.$$

Таким чином, E_k=31; D_k=3031.

В узагальненому вигляді факторизації на основі використання загального решета числового поля можна подати таким чином:

- вибирання поліномів відповідних степенів;
- просіювання з відбиранням позитивних даних;
- обробка даних з розв'язанням задачі лінійної алгебри;
- знаходження нетривіальних рішень.

Метод загального решета числового поля дозволяє факторизувати модуль RSA перетворення зі складністю (асимптотичною):

$L_N(\gamma, \delta) = \exp(\delta (Ln(N))^{\gamma} Ln(Ln(N))^{1-\gamma})$, (9.14)

де $\gamma=1/3$, а $\delta = (64/9)^{(1/3)}$ T)(приблизно 1.923) параметри методу.

Для методу спеціального решета числового поля параметри методу дорівнюють γ=1/3, а $\delta = (32/9)^{1/3}$ (приблизно 1,526), (9.15)

тобто метод спеціального решета числового поля є менш складним (більш швидкодіючим).

Взагалі ідея методу загального решета числового поля належить Джону Полларду, який у 1988 році запропонував просіювання виконувати не у кільці цілих чисел, як це робиться в квадратичному решеті, а в алгебраїчному полі. Спочатку метод можна було використовувати для факторизації тільки чисел спеціального вигляду $2^n+(-)n$. Тому метод отримав назву «спеціального решета числового поля». Практична реалізація ідеї Полларда була здійснена в 1990 році, коли з його використанням було факторизовано число Ферма (2^{512}). Також були факторизовані деякі числа вигляду $b^c+(-)1$. У подальшому було запропоновано використовувати метод решета числового поля й для факторизації довільних цілих чисел. Була знайдена евристична оцінка його складності, яка визначалась у (9.14). Тобто множник δ був зменшений у порівнянні з квадратичним решетом з 1/2 до 1/3. Розглянемо етапи базового методу решета числового поля.

Нехай n – непарне ціле число, яке необхідно факторизувати. Основна ідея Полларда полягає в тому, щоб замінити поліном 2-го степеня $q(x) = (x+m)^2 - n$, який використовувався у квадратичному решеті, на довільний поліном $P_d(x)$ степеня $d \geq 3$, який задовольняє умові $P_d(m) = n$ для деякого цілого числа m. Далі, просіювання за множиною цілих чисел Z було замінене просіюванням в кільці $Z(\beta)$, яке отримується приєднанням до кільця Z цілого алгебраїчного числа β, що є коренем полінома $P_d(m)$. У порівнянні з квадратичним решетом, у решеті числового поля факторна база складається із простих елементів кільця алгебраїчних чисел.

Виграш при використанні решета числового поля полягає в тому, що умова $P_d(m) = n$ для деякого цілого m, що накладається на поліном $P_d(x)$, у порівнянні з коефіцієнтами, що використовуються у квадратичному решеті, може бути виконана при менших значеннях коефіцієнтів полінома $P_d(x)$.

Метод загального решета числового поля може бути реалізований через виконання таких кроків

1. Вибирається степінь незвідного полінома d ≥3. Можна взяти d = 2, але в цьому випадку у порівнянні з квадратичним решетом виграшу не буде.

2. Вибирається ціле число *m* – таке, що $\lfloor n^{1/(d+1)} \rfloor < m < \lfloor n^{1/d} \rfloor$, та розкладається число *n* за основою *m*, тобто подається у вигляді:

$$n = m^d + a_{d-1} m^{d-1} + \ldots + a_0 \qquad (9.16)$$

3. Із розкладом (9.16) пов'язується незвідний поліном у кільці $Z(x)$:

$$f_1(x) = x^d + a_{d-1} x^{d-1} + \ldots + a_0 \qquad (9.17)$$

4. Визначається поліном просіювання $F_1(a, b)$ як однорідний поліном від двох змінних *a* та *b*:

$$F_1(a, b) = b^d f_1(a/b) = a^d + a_{d-1}a^{d-1}b + a_{d-2}a^{d-2}b^2 + \ldots + a_0 b^d \qquad (9.18)$$

Необхідно відмітити, що значення $F_1(a,b)$ дорівнює нормі полінома $a - b \times x$ в алгебраїчному числовому полі Q [β], яке отримують доповненням поля раціональних чисел Q у загальному випадку комплексного кореня β багаточлена $f_1(x)$ [425]. При цьому властивості комутативності норми

$$Nr(h_1(x) \times h_2(x)) = (Nr(h_1(x)) \times (Nr(h_2(x))) \qquad (9.19)$$

дозволяють замість розкладання багаточлена з кільця Z(β) виконати розкладання їх норм.

5. Визначається другий багаточлен

$$f_2(x) = x - m \qquad (9.20)$$

та відповідний йому однорідний багаточлен

$$F_2(a, b) = a - b\,m. \qquad (9.21)$$

Головною вимогою при вибиранні пари багаточленів $(f_1(x), f_2(x))$ є виконання вимоги:

$$f_1(m) = f_2(m) \pmod n, \qquad (9.22)$$

яка в нашому випадку, очевидно, виконується, оскільки перший багаточлен у точці *m* дорівнює *n*, а другий – нулю.

6. Вибирається два позитивних числа L_1 та L_2, що визначають деяку прямокутну область

$$SR = \{1 \le b \le L_1, -L_2 \le a \le L_2\}, \qquad (9.23)$$

яку називають областю просіювання.

7. Нехай β – корінь багаточлена $f_1(x)$. Розглядається кільце багаточленів Z(β) (для формального описання алгоритму). Також визначимо алгебраїчну факторну базу FB_1, яка буде складатися з багаточленів першого порядку вигляду $a - b \times \beta$ з нормою, що є простим числом. Такі багаточлени є простими елементами, що не розкладаються, в кільці алгебраїчних цілих поля K = Q(β). Абсолютні величини норм багаточленів із факторної бази FB_1 обмежимо зверху деякою постійною B_1.

8. Також визначається раціональна факторна база FB_2, яка складається з усіх простих чисел, добуток яких обмежується другою постійною B_2.

9. Визначається також невелика множина багаточленів першого порядку $c - d \times \beta$, норма яких є простим числом. Позначимо цю множину як FB_3. Вона має задовільняти умові, що

$$FB_1 \wedge FB_3 = \emptyset$$

і називається факторною базою квадратичних характерів. Факторна база FB_3 необхідна на підсумковій стадії алгоритму для перевірки того факту, що знайдений у ході просіювання багаточлен є повним квадратом.

10. Далі для отримання гладких пар (a,b) множини M здійснюється просіювання багаточленів $\{a - b \times \beta \mid (a,b) \in SR\}$ згідно факторної бази FB_1, а також цілих чисел $\{a - b \times m \mid (a,b) \in SR\}$ згідно факторної бази FB_2. При цьому пара (a,b) називається гладкою, якщо НСД (a, b) = 1, а поліном $a - b \times \beta$ і число $a - b \times m$ розкладається по відповідним факторним базам FB_1 та FB_2. При цьому число гладких пар у множині M має бути більше загальної суми елементів усіх трьох баз щонайменше на 2 одиниці.

11. На цьому кроці шукається підмножина $S \supset M$ таке, що добуток усіх пар $\prod_{(a, b) \in S} Nr(a - b \times \beta) = H^2$ для $H \in Z$, а також $\prod_{(a, b) \in S} (a - b\,m) = B^2$, $B \in Z$.

Для знаходження множини S, як і в методі квадратичного решета, складається система лінійних алгебраїчних рівнянь з коефіцієнтами із множини $F_2 = \{0, 1\}$, результатом розв'язання якої й будуть номери S.

12. Формується багаточлен

$$g(\beta) = (f_1'(\beta))^2 \prod_{(a,b) \in S} (a - b\beta), \qquad (9.24)$$

де $f_1'(x)$ – похідна багаточлена $f_1(x)$.

13. Далі, якщо вся процедура виконана коректно, то багаточлен $g(\beta)$ є повним квадратом у кільці поліномів Z(β). Знаходимо квадратні корені із багаточлена $g(\beta)$ та цілого числа B^2, унаслідок чого знаходимо багаточлен $\alpha(\beta)$ та число B.

14. Замінюємо багаточлен $\alpha(\beta)$ на число $\alpha(m)$. Відображення $\varphi: \beta \to m$ є кільцевим гомоморфізмом кільця алгебраїчних цілих чисел $Z_к$ у кільце Z. Звідки отримаємо співвідношення:

$$A^2 = g(m)^2 = (\varphi(g(\alpha)^2) = \varphi\{(f_1'(\beta))^2 \prod_{(a, b) \in S} (a - b\,\beta)\} =$$

$$= (f_1'(m))^2 \prod_{(a, b) \in S} (a - b\,m) = (f_1'(m))^2 * C^2 (mod\ n) \qquad (9.25)$$

Таким чином, визначивши $B = f'(m)\ C$, знайдемо пару цілих чисел (A,B), які задовольняють умові

$$A^2 = B^2 \pmod n \qquad (9.26)$$

На останок можна знайти дільник числа *n*, обчислюючи НСД (n, A +(-) B).