УДК 004.22

Л.М. Тимошенко,
кандидат економічних наук, доцент,
С.В. Івасєв,
К.В. Вербик

УДОСКОНАЛЕННЯ АЛГОРИТМУ ФАКТОРИЗАЦІЇ ДЛЯ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У статті обґрунтовані теоретичні основи розробки вдосконаленого методу Ферма, в результаті чого отримано підвищення швидкодії за рахунок використання теоретико-числового базису Крестенсона та символів Якобі.

Ключові слова: *факторизація, метод Ферма, теоретико-числовий базис Крестенсона, символ Якобі, символ Лежандра.*

В статье обоснованы теоретические основы разработки усовершенствованного метода Ферма, в результате чего получено повышение быстродействия за счет использования теоретико-числового базиса Крестенсона и символов Якоби.

Ключевые слова: *факторизация, метод Ферма, теоретико-числовой базис Крестенсона, символ Якоби, символ Лежандра.*

Theoretical bases of the development of an improved method of Fermat, for the promotion of the performance due to the use of theoretical and numerical basis of Krestenson and Jacobi symbols.

Keywords*: factorization, method of Fermat, theoretical and numerical basis of Krestenson, Jacobi symbol, symbol Legendre.*

Вступ

Для потреб практичної криптографії актуальна проблема побудови швидких алгоритмів знаходження "випадкових" простих чисел заданої довжини. Швидкість роботи алгоритмів знаходження простих чисел важлива для систем, які використовують схему RSA, оскільки ключами в них власне і є великі прості числа [1].

Безпека системи RSA базується на завданні факторизації великих чисел [6].

Метод факторизації Ферма − алгоритм факторизації (розкладання на множники) непарного цілого числа, запропонований П'єром Ферма (1601−1665) в 1643 році. Він ефективний у випадках, коли n − добуток двох цілих чисел, близьких одне до одного [5].

В основу методу покладено пошук цілих чисел x та y, які задовольняють співвідношення $x^2-y^2=n$, що веде до розкладання $n=(x-y)\cdot(x+y)$.

Метод Ферма ґрунтується на теоремі про представлення числа у вигляді різниці двох квадратів [3]:

Якщо $n>1$ непарна, то існує взаємно однозначна відповідність між розкладаннями на множники n=a·b і уявленнями у вигляді різниці квадратів $n=x^2-y^2$ з $x>y>0$, задане формулами $x=\frac{a+b}{2}$, $y=\frac{a-b}{2}$, $a=x+y$, $b=x-y$.

Способи кодування інформаційних потоків визначаються теоретико-числовими базисами, які застосовуються для їх представлення. Найбільш поширені: унітарний, Хаара, Грея, Радемахера, Крестенсона, Галуа.

Базис Крестенсона, який породжує систему числення залишкових класів, успішно застосовується для побудови спецпроцесорів стиснення інформації та реалізації високопродуктивних процесорів опрацювання інформаційних потоків, в системах криптозахисту інформації [4].

Основна частина

Запропоновано скористатися теоретико-числовим базисом Крестенсона, який дозволяє зменшити обчислювальну складність за рахунок зменшення розрядностей чисел, над якими проводяться операції.

У методі Ферма потрібно знайти два числа x та y такі, що $x^2 - y^2 = n$, тоді $(x + y) * (x - y) = n$.

Далі в рівнянні $x^2 = y^2 - n$, виконаємо таке перетворення:

$$x^2 \bmod p = y^2 - n \bmod p \qquad (1)$$

одержимо $x^2 \equiv (y^2 - n) \bmod p$.

Для розв'язання цього рівняння доцільно скористатися символами Якобі, які дозволяють однозначно вказувати, чи обчислюється корінь за модулем.

Нехай p – просте, a – ціле число. Символ Лежандра $\left(\frac{a}{p}\right)$ визначається:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \textit{ якщо } p \textit{ ділиться на } a \\ 1, \textit{ якщо } a \in Q_p \\ -1, \textit{ якщо } a \in \overline{Q}_p \end{cases}$$

Число a, яке не ділиться на непарне просте p, є квадратичним лишком за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv 1 (\bmod p)$, і квадратичним нелишком тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

За теоремою Ферма $a^{p-1} \equiv 1 \pmod p$ при НСД$(a, p) = 1$ та НСД$(2, p) = 1$ або:

$$\left(a^{\frac{p-1}{2}} + 1\right) * \left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \bmod p \qquad (2)$$

Звідси вираз в одній із дужок ділиться на p. Обидві дужки не можуть ділитися на p, оскільки тоді на p ділилася б і їх різниця, яка дорівнює 2, а за умовою теореми p – непарне просте число. Якщо a є квадратичним лишком, то $a = x^2 \pmod p$ для деякого такого x, що НСД(x, p) = 1. Отже, $a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p$, тобто $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ або $a^{\frac{p-1}{2}} - 1$ ділиться на p. Якщо a є квадратичним нелишком, то $a^{\frac{p-1}{2}} - 1$ не ділиться на p, звідки $a^{\frac{p-1}{2}} + 1$ повинно ділитися на p або $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p \tag{3}$$

Якщо число a є квадратичним лишком за модулем p, то за означенням символа Лежандра $\left(\frac{a}{p}\right)=1$, а за критерієм Ейлера $a^{\frac{p-1}{2}} \pmod p$ 1. Відповідно, якщо число a є квадратичним нелишком за модулем p, то $= \left(\frac{a}{p}\right) \equiv -1$ і $a^{\frac{p-1}{2}} \pmod p \equiv -1$, звідки і випливає твердження.

Символ Якобі є узагальненням символу Лежандра на випадок, коли n є непарним, але необов'язково простим.

Нехай n – непарне ціле число, n≥3. Відомо [2], що $n = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$, де p_i – прості числа. Символ Якобі $\left(\frac{a}{n}\right)$ визначається так:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \left(\frac{a}{p_2}\right)^{k_2} \ldots \left(\frac{a}{p_t}\right)^{k_t} \tag{4}$$

Зазначимо, що якщо n просте, то символ Якобі стає символом Лежандра.

З властивостей символу Якобі випливає, що якщо n непарне, а число a подати у вигляді $a = 2^k a_1$, де a_1 – непарне число, то

$$\left(\frac{a}{n}\right) = \left(\frac{2^k}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2^k}{n}\right)\left(\frac{n \bmod a_1}{a_1}\right)(-1)^{\frac{(a_1-1)(n-1)}{4}} \tag{5}$$

Ця формула дає можливість обчислити значення символа Якобі, не маючи розкладу числа n на прості множники.

На відміну від символу Лежандра, символ Якобі $\left(\frac{a}{n}\right)$ не визначає, чи є число a квадратичним лишком за модулем n. Справді, якщо $a \in Q_n$, то $\left(\frac{a}{n}\right) = 1$, але з того, що $\left(\frac{a}{n}\right) = 1$, не випливає те, що $a \in Q_n$.

$$V = x - x^2 = t - t^2 = 0{,}24$$

Знаходимо x таким чином:

$$x \equiv \sqrt{(y^2 - n)} \bmod p. \qquad (6)$$

Тоді удосконалення методу Ферма полягає в тому, що ми завідомо відкидаємо ті значення (y^2-n), для яких не існує корінь за модулем, і зменшуємо розрядність обчислень за рахунок модульної операції.

Удосконалений алгоритм факторизації прийме такий вигляд:

1. Ввід P_0
2. Ввід Prime[0..n]
3. i=0
4. sqstart =Sqrt(P_0)
5. sqstartm =Sqrt(P_0)
6. Diference = sqstart * sqstart
7. Diference = Diference-P_0
8. i++
9. sqstart= sqstart+2
10. sqstartm[i]= (sqstartm +2) mod Prime[i]
11. Якщо символ Якобі (sqstartm[i], Prime[i])≠1,
тоді крок 8
12. Якщо i=n – крок 14
13. Якщо символ Якобі (sqstartm[i], Prime[i])=1, тоді i++,
крок 10
14. Якщо Sqrt(Diference) дробове, тоді крок 6
15. Вивід sqrt(Diference+sqstart*sqstart)+sqrt(Diference)
16. Вихід

Висновки

Розроблено вдосконалений метод Ферма, в результаті якого отримали підвищення швидкодії за рахунок використання теоретико-числового базису Крестенсона та символів Якобі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Алферов А.П.* Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М. : Издательский дом “Гелиос АРВ”, 2005. – 480 с.

2. *Акушинский И.Я.* Машинная арифметика в остаточных классах : монография / И.Я. Акушинский, Д.И. Юдицкий. – М. : Советское радио, 1968. – 439 с.

3. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

4. *Николайчук Я.М.* Теоретичні основи побудови спецпроцесорів у базисі Крестенсона / Я.М. Николайчук, О.І. Волинський, С.В. Кулина // Вісник Хмельницького національного університету. – 2007. – № 3. Т. І. (93). – С. 85–90.

5. *Николаенко О.В.* Анализ методов факторизации в криптографических системах защиты информации / О.В. Николаенко, Л.Н. Тимошенко, К.В. Вербик. – Матеріали ІІІ міжнародної науково-практичної конференції ІУСТ-Одеса-2014. – С. 173–175.

6. *Смарт Н.* Криптография / Н. Смарт. – М. : Издательский дом “ТЕХНОСФЕРА”, 2005. – 526 с.

Отримано 28.08.2014.