ГІПЕРКОМПЛЕКСНИЙ RSA-АЛГОРИТМ

Ланде Д.В., Каліновський Я.О.,
Боярінова Ю.Є., Хіцко Я.В.,
ІПРІ НАН України, НТУУ «КПІ»

1. Вступ

Швидкий розвиток і доступність інформаційних технологій робить інформацію надзвичайно вразливою до несанкціонованого доступу. В зв'язку з цим виникає необхідність захисту інформації, який може бути отримано за допомогою як апаратних так і програмних засобів. Для боротьби з несанкціонованим доступом до інформації, збереження ії конфіденційності розроблено багато цифрових криптографічних алгоритмів.

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування [1,2]. Криптографічна система з відкритим ключем – системи шифрування, системи електронного цифрового підпису (ЕЦП), передбачають передачу відкритого ключа по відкритому, тобто незахищеному, каналу зв'язку, доступному для спостереження. Він використовується для перевірки ЕЦП і для шифрування повідомлення. Для генерації ЕЦП і для дешифрування повідомлення використовується секретний ключ. Традиційно для більшого захисту використовуються ключі у вигляді дійсних цілих чисел, довжиною, як правило, 1024 біт. Але в останній час йде мова про збільшення довжини ключа до 2048 біт для збільшення захисту інформації. Що ж до ускладнення злому збільшенням розміру ключа, то подвоєння його довжини в середньому збільшує час операцій відкритого ключа (шифрування і перевірка підпису) в чотири рази, а час операцій секретного ключа (розшифровка та підпис) у вісім разів. Тому виникає необхідність застосування інших засобів захисту інформації без збільшення довжини ключа.

2. Математичні засади для алгоритму RSA з гіперкомплексними числами

Звичайний алгоритм RSA діє наступним чином:

1) шифрування – деякий текст M шифрується за допомогою відкритого ключа (e,n) за алгоритмом

$$C = E(M) = M^e \bmod n. \qquad (1)$$

2) дешифрування – за допомогою закритого ключа (d,n) за алгоритмом

$$M = D(C) = C^d \bmod n. \qquad (2)$$

Звичайно, число *d* обчислюється за допомогою розширеного алгоритму Евкліда [3]. Алгоритм Евкліда також використовується при знаходженні числа *e*.

3. Гіперкомплексний варіант RSA-алгоритма

Для використання гіперкомплексного подання даних в алгоритмі RSA необхідно розглянути побудову функцій від гіперкомплексної змінної. Тобто для побудови виразів (1) та (2) будемо використовувати такі властивості показникової функції:

$$a^x = exp(x \cdot ln\, a) \qquad (3)$$

Тоді для обчислення алгоритму RSA необхідно розглянути побудову функцій от гіперкомплексного змінного [4], відповідно до (3) це будуть – експоненціальна та логарифмічна функції.

Задача побудови представлень трансцендентних функцій від гіперкомплексного змінного насамперед зводиться до їхнього визначення з точки зору структури обчислень над гіперкомплексним аргументом, а надалі – до подання їх у вигляді гіперкомплексної функції [4,5].

В загальному випадку побудова представлення експоненти від гіперкомплексної змінної викликає значні труднощі тому, що немає загальної формули піднесення до степеня гіперкомплексного числа. Беручи до уваги, що визначення суми степеневого ряду

викликає значні труднощі, для побудови представлення експоненти від гіперкомплексної змінної через степеневий ряд був розроблений метод асоційованих систем лінійних диференціальних рівнянь [8]. Він базується на тому, що степеневий ряд для експоненти задовольняє диференціальному рівнянню від гіперкомплексної змінної:

$$\dot{W} = MW \qquad (4)$$

де M, W – гіперкомплексні числа, тобто визначення експоненти за допомогою степеневого ряду і за допомогою розв'язку цього рівняння (4)– еквівалентні.

Знання експоненти гіперкомплексної змінної дозволяє будувати подання оберненої до неї функції. Логарифмічна функція гіперкомплексного аргументу визначається як функція, обернена до експоненти [6]. Для моделювання цифрового підпису з гіперкомплексними числами також необхідна модулярна аріфметика для різних гіперкомплексних числових систем [7]. Усі ці математичні засади дозволяють використовувати гіперкомплексні числові системи в алгоритмі цифрового підпису RSA.

4. Дослідження алгоритму RSA з використанням гіперкомплексних чисел

Безпека алгоритму RSA побудована на принципі складності факторизації. Наприклад, для випадку використання в алгоритмі RSA системи комплексних чисел може бути запропонований такий алгоритм факторизації.

Обчислити норму $N(A)$ комплексного числа A. Розкласти $N(A)$ на множники простих раціональних чисел $p_1,\ldots,p_s$. Всі p_i, $i = 1,2,\ldots,s$ виду $4k+3$ залишити без змін, решту p_j вигляду $4k+3$ розкласти на суму квадратів: $p_i = x^2 + y^2$, тоді отримаємо два додаткові множники: асоційовані з $x + yi$ та $y + xi$.

Обчислити всі можливі добутки отримані в кожному з випадків для простих комплексних чисел доти, доки не отримаємо число, асоційоване з вихідним числом A.

Цей алгоритм окрім розкладання дійсного числа $N(A)$ на прості множники вимагає розкладання всіх отриманих при попередньому розкладі чисел виду $4k+1$ на суму квадратів.

Складність знаходження добутку гіперкомплексного числа по модулю іншого гіперкомплексного числа визначається складністю множення одного числа на інше:

$$C = A * B = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n}\gamma_{ij}^{k}\, a_i\, b_j\, e_k \ .$$

Тобто ми можемо оцінити його складність як $O\left(n^3\right)$. Загальну складність кодування для комплексних чисел, як показують дослідження, можна оцінити як $O\left(n^3\left(n^2 * \log(n)\right)^{1.465}\right)$.

5. Висновки

Таким чином, дослідження доводять більшу стійкість алгоритму RSA з використанням гіперкомплексних числових систем порівняно з алгоритмом на основі дійсних чисел.

Література

1. *Шнайер Б.* Прикладная криптография / Б. Шнайер. — М.: Триумф, 1995. — 816 с.

2. *Stinson D. R.* Cryptography: Theory and Practice / D. R. Stinson. — Chapman and Hall, 2006.

3. *Ноден П.* Алгебраическая алгоритмика с упражнениями и решениями / П. Ноден, К. Китте. — М.: Мир, 1999. — 720 с.

4. *Калиновский Я.А.* Методы построения нелинейностей в расширениях комплексных чисел / Я.А. Калиновский, Н.В. Роенко, М.В. Синьков // Кибернетика и системный анализ. — 1996. — № 4. — С. 178–181.

5. *Синьков М.В.*, Калиновский Я.А. Представление экспонент в изоморфных гиперкомплексных числовых системах / М.В.Синьков, Я.А Калиновский // Реєстрація, зберігання і оброб. даних. — 2011. — Т.13, № 2. — С. 27–38.

6. *Синьков М.В.* Розробка та дослідження алгоритмів побудови зображення обернених функцій від гіперкомплексного змінного / М.В. Синьков, Я.О. Каліновський, Ю.Є. Боярінова // Реєстрація, зберігання і оброб. даних. — 2005. — Т. 7, № 1. — С. 32–42.

7. *Synkov M.V., Gubareni N.M.* Nonpositional Presentations in the Multidimensional Numerical Systems. — K.: Naukova dumka, 1979. —140 p. – Rus.

8. *Синьков М.В.* Конечномерные гиперкомплексные числовые системы. Основы теории. Применения. /М.В.Синьков, Я.А.Калиновский, Ю.Е.Бояринова.-К: Инфодрук, 2010. – 389 с.