решіток. Розроблено багато лінз Ротмана в різних діапазонах частот (до 37 ГГц). Максимальна кількість входів у існуючих зразках 41, максимальне число променів 46, мінімальний рівень бічних пелюстків менше -30дБ, максимальний сектор по куту місця 120°, а максимальний сектор по азимутом 120°.

1. Устройства СВЧ и антенны. Проектирование фазированных антенных решеток: Учеб. Пособие для вузов / Под ред. Д. И. Воскресенского. – М.: Радиотехника, 2003. – 632с.
2. Rotman W. And Turner R. Wide-angle microwave lens for line source applications // IEEE Transactions Antennas Propagation, Vol. 11, No. 6, November, 1963, pp. 623 – 632.
3. Peterson A. F. Scattering matrix integral equation analysis for the design of a waveguide Rotman lens // IEEE Transactions on antennas and propagation, Vol. 47, No. 5, May 1999. – pp. 870 – 878.
4. Hansen R. C. Design trades for Rotman lenses // IEEE Transactions on antennas and propagation, Vol. 39, No. 4, April 1991., pp. 464 – 472.

КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ОСНОВІ АРІФМЕТИКИ ФІБОНАЧІ

Викладачі Забегалов І. В., Булашенко А. В., студент Мезько О.,
ШХТК ШІСумДУ

Важливою складовою практично будь-якої комп'ютерної інформаційної системи є система захисту інформації. Радикальне вирішення проблем захисту електронної інформації може бути отримане на базі використання криптографічних методів, які дозволяють вирішувати важливі завдання захищеної автоматизованої обробки та передачі інформації. Основним із засобів захисту інформації в телекомунікаційних системах сьогодні є симетричні шифри.

У розвідці розглядається підхід, який будується на використанні поняття узагальненої Q_p-матриці Фібоначі. Вона являє собою квадратну $(p+1)\times(p+1)$-матрицю вигляду:

$$Q_p = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}. \quad (1)$$

Відзначена важлива властивість матриць, яка полягає в тому, що матриці Фібоначі є невиродженими, тому що детермінант матриці Q_p^n рівний $(-1)^{pn}$. Ця властивість визначає можливість використання матриць Фібоначі для багатьох додатків, і зокрема, для криптографічних перетворень інформації.

Властивість збереження по модулю значення детермінанта довільної матриці після множення на Q_p^n-матрицю Фібоначі

$$DetC = Det\left(M \times Q_p^n\right) = \left(-1\right)^{pn} \cdot DetM \quad (2)$$

дає можливість не тільки виявляти помилки без попередньої операції зворотного перетворення, але й виправити їх, що може бути використане в методах аутентифікації інформації.

Лінійність операції множення на матрицю Фібоначі визначила областю дослідження роботи в рамках застосування арифметики Фібоначі в схемах обміну підблоками симетричних методів перетворення, а в якості оцінки ефективності показники перемішування.

Аналіз властивостей матриць Фібоначі виявив основну перешкоду, що стоїть на шляху їх використання для операцій криптографічного перетворення операції множення на матрицю Фібоначі й обчислення детермінанта приводять до великої надмірності інформації. За допомогою проведених досліджень були отримані оцінки абсолютної надмірності

$$k = \left(p+1\right) \times k_i, \quad (3)$$

де k_i – абсолютна надмірність одного рядка інформаційної матриці після перетворення, і відносної надмірності

$$R_k = \frac{k_i}{\left(p+1\right) \cdot w + k_i}, \quad (4)$$

де p – порядок Q_p-матриці Фібоначі; w – довжина слова у бітах (стандартними є 8, 16 і 32 біта).

Дослідження показали, що надмірність, що виникає при використанні в перетвореннях інформації арифметики Фібоначі, обернено пропорційна порядку p матриці Фібоначі, але швидко зростає при збільшенні значення ступені n матриці.

Установлено, що проведення обчислень у кільці цілих чисел $Z/(q)$ усуває проблему виникнення надмірності інформації при використанні узагальнених матриць Фібоначі. Вірогідність цього факту була встановлена шляхом строгого математичного доказу висунутої гіпотези про гомоморфізм p-чисел і Q_p-матриць Фібоначі у кільці цілих чисел $Z/(q)$ [3].

Основним результатом можна вважати те, що збереження властивостей чисел і матриць Фібоначі у кільці цілих чисел по модулю q дозволило уникнути виникнення надмірності при використанні арифметики Фібоначі у різних додатках, у тому числі в алгоритмах криптографічного перетворення.

1. Stakhov A. P., Massingue V., Sluchenkova A. Introduction into Fibonacci coding and cryptography. – Kharkiv: Osnova, 1999. – 236 p.

2. Уфимцева В. Б. Свойства линейных рекуррентных последовательностей р–чисел Фібоначі над конечным полем $GF(q^m)$ // Материалы 7 Международного молодежного форума, ХТУРЕ. – Харьков. – 2003. – С. 417.

3. Булашенко А. В., Забегалов І. В., Мезько О. В. Математичні перетворення на основі арифметики Фібоначі // Збірник тез до студентського кафедрального науково-методичного семінару . – Суми: СумДУ – 2010. – С. 111 – 112.

4. Самойленко Н. І., Уфимцева В. Б. Дифузійний аналіз мережі Фейстеля зі схемами обміну на основі матриць Фібоначчі // Наукові вісті Національного технічного університету «Київський політехнічний інститут». – 2002. - № 6 (26). – С. 146-152.