УДК 004.424.47, 004.056.55

В.Б. Уфимцева, М.Ю. Карпенко

Харківський національний університет міського господарства імені О.М. Бекетова, Харків

АНАЛІЗ ПОКАЗНИКІВ СТАТИСТИЧНОЇ БЕЗПЕКИ КРИПТОГРАФІЧНОГО АЛГОРИТМУ НА БАЗІ АРИФМЕТИКИ ФІБОНАЧЧІ

У статті розглянуто доцільність використання апарату арифметики Фібоначчі при побудові хеш-функцій. Показано перспективність цього напрямку досліджень в плані удосконалення статистичних показників симетричних криптографічних перетворень інформації за рахунок прискорення дифузійних процесів при використанні в схемах обміну підблоків мережі Фейстеля матричного перетворення Фібоначчі.

Ключові слова: *арифметика Фібоначчі, хеш-функції, метричні перетворення Фібоначчі, симетричні криптографічні системи, числа Фібоначчі, мережі Фейстеля.*

Вступ

Постановка проблеми. У зв'язку з особливим нематеріальним характером електронної інформації однією з найбільш важливих складових практично будь-якої комп'ютерної інформаційної системи є система захисту інформації. Розробка ефективних методів забезпечення цілісності та аутентифікації інформації сучасних систем вимагає використання комбінованих методів перетворення інформації. Так, електронний цифровий підпис документа формується за допомогою асиметричного перетворення. Однак, у зв'язку з низькою швидкістю обробки такого документа, зазвичай проводиться підпис не самого документа, а його агрегованого еквіваленту.

Аналіз останніх досліджень. Одним з найбільш розповсюджених функцій стиснення є хешування інформації на основі симетричного блочного перетворення. Існує багато ефективних методів хешування, розроблених такими відомими фахівцями, як Р.Л. Ривест, Р. Меркло та інші [1]. Однак, обсяги інформації, що обробляються сучасними комп'ютерними системами істотно зростають, що призводить до необхідності збільшення швидкості обробки даних.

Найбільш істотний внесок у вирішення проблеми обчислювальної складності функції хешування вносить метод симетричного перетворення інформації. Сучасні шифри будуються як ітераційні, при цьому увага дослідників зосереджена, як правило, на вивченні властивостей булевих функцій і нестійких процедур перестановок з метою поліпшення показників перемішування (за Шенноном). У даній роботі основну увагу зосереджено на можливості покращення показників перемішування на основі використання математичного апарату арифметики Фібоначчі, що дозволяє збільшити швидкість методу хешування внаслідок скорочення кількості ітерацій симетричного перетворення.

Метою роботи є вивчення перспектив і можливостей використання властивостей арифметики Фібоначчі для побудови процедур хешування інформації. Для досягнення цієї мети в роботі вирішуються такі завдання:

1) вивчення можливості застосування математичного апарату теорії чисел Фібоначчі для виконання криптографічних перетворень;

2) розробка практичних принципів і властивостей криптографічних перетворень інформації при використанні для процедур шифрування математичного апарату арифметики Фібоначчі;

3) аналіз і дослідження показників статистичної безпеки при використанні для побудови симетричних алгоритмів криптографічних перетворень арифметики узагальнених чисел Фібоначчі.

1. Базові поняття арифметики Фібоначчі

У ході вирішення першого завдання виконано аналіз ефективності застосування арифметики Фібоначчі при побудові криптографічних перетворень і показана перспективність цього напрямку для криптографії. Основним об'єктом досліджень цього напрямку стали узагальнені числа Фібоначчі [2], або так звані р-числа, які є лінійною рекурентною послідовністю порядку $k = p + 1$ з законом рекурсії:

$$F_p(i + p + 1) = F_p(i + p) + F_p(i), \qquad (1)$$

де $p \in Z \cap p \geq 0$ та $k \in Z$,

при початкових умовах:

$$F_p(1) = F_p(2) = \ldots = F_p(p + 1) = 1. \qquad (2)$$

Традиційні підходи до опису ЛРП базуються здебільшого на використанні характеристичних многочленів. Як показали дослідження, для узагальнених - чисел Фібоначчі характеристичні многочлени мають вигляд:

$$f(x) = x^{p+1} - x^p - 1. \qquad (3)$$

При аналізі лінійних рекурентних послідовностей р-чисел Фібоначчі були виділені послідовності р-чи-

сел Фібоначчі максимального періоду для $p = \overline{1,152}$ [3]. Аналіз основних властивостей послідовностей чисел Фібоначчі з максимальним періодом показав: період М-послідовностей р-чисел Фібоначчі дорівнює $T = 2^{p+1} - 1$. Для заданого f(x) існує $2^{p+1} - 1$ різних послідовностей, які є $2^{p+1} - 1$ різними зсувами М-послідовності $F_p(.)$ і мають вигляд

$$F_p(\cdot), Q_p F_p(\cdot), Q_p^2 F_p(\cdot), \ldots, Q_p^p F_p(\cdot).$$

Кількість одиничних символів на періоді М-послідовності р-чисел Фібоначчі дорівнює $N(F^p(i) = 1) = 2^p$, а нульових – $N(F^p(i) = 0) = 2^p - 1$, тобто вага Хеммінга $\mathrm{wt}\left(F_p(0,1,\ldots,T-1)\right) = 2^p$. Ймовірності появи 1 і 0 визначаються виразами:

$$p\left(F_p(i) = 1\right) = \frac{2^p}{2^{p+1} - 1} = \frac{1}{2} + \frac{1}{2^{p+2} - 2}; \quad (4)$$

$$p\left(F_p(i) = 0\right) = \frac{2^p - 1}{2^{p+1} - 1} = \frac{1}{2} - \frac{1}{2^{p+2} - 2} \quad (5)$$

і при збільшенні р досягають значень як завгодно близьких до 1/2.

У послідовності р чисел Фібоначчі максимальної довжини серії з одного символу (одиниці або нуля) зустрічаються 2^{p+1} раз, з двох одиниць або нулів – 2^{p+2} раз і т.д. Серії з р нулів і одиниць зустрічаються тільки по одному разу. Порівнюючи вирази для оцінки ймовірності появи серій з однакових символів для випадкової послідовності з відповідною ймовірністю для М-послідовності, можна переконатися в їх практичній еквівалентності.

Властивість зсуву та додавання. Для кожного цілого $s\left(1 \le s \le 2^{p+1} - 1\right)$ існує таке ціле, $r \ne s\left(1 \le r < 2^{p+1} - 1\right)$, що

$$\left\{F_p(i)\right\} + \left\{F_p(i - s)\right\} = \left\{F_p(i - r)\right\}.$$

Дворівнева автокореляційна функція:

$$R_F(\tau) = \begin{cases} 1, \tau = 0\left(\mathrm{mod}\left[2^{p+1} - 1\right]\right); \\ -1/\left(2^{p+1} - 1\right), \tau \ne 0\left(\mathrm{mod}\left[2^{p+1} - 1\right]\right). \end{cases} \quad (6)$$

Серед Т ненульових М-послідовностей р-чисел Фібоначчі, що сформовані на основі породжуючого полінома f(x), є одна, що має властивість $F_p(i) = F_p(2i), i \in Z$ [3]. Виходячи з виду початкових векторів характеристичних послідовностей р-чисел Фибоначчи для заданого f(x) можна дійти висновку, що:

$$F_p(0,1,2,\ldots,p) = \begin{cases} 10^p, & p = 2k; \\ 01^p, & p = 2k + 1, \end{cases} \quad k \in N. \quad (7)$$

Децимацією послідовності р-чисел Фібоначчи за індексом $q\left(q \in N\right)$ називається формування нової послідовності $G_p(i) = F_p(iq), i \in Z$. Будь-яка М-послідовність періоду $T = 2^{p+1} - 1$ може бути одержана внаслідок децімації за нечітким індексом q. При децімації послідовності $F_p(.)$ за індексом $q = T - 1 = 2^{p+1}$ одержано зворотну послідовність $G_p(i) = F_p\left(i(T-1)\right) = F_p(-i)$ із зворотним поліномом $g(x) = x^{p+1} f\left(x^{-1}\right) = x^{p+1} + x + 1$.

У роботі обґрунтовується підхід, що будується на використанні поняття узагальненої Q_p-матриці Фібоначчі $(p + 1) \times (p + 1)$ [2].

$$Q_p = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}. \quad (8)$$

При аналізі основних властивостей матриць Фібоначчі показано, що при використанні в криптографічних перетвореннях множення матриці даних на Q_p^n-матрицю Фібоначчі обчислювальна складність C(p), оцінена числом операцій множення, знижується на $(p + 1)^3$, тому операція множення довільній матриці М розміром $(p+1) \times (p+1)$ на Q_p^n-матрицю Фібоначчі (і, відповідно, операція піднесення матриці Фібоначчі в ступінь) зводяться до простих операцій додавання і зсуву. Відзначено важливу властивість матриць, яка полягає в тому, що матриці Фібоначчі є невиродженими, оскільки детермінант матриці Q_p^n дорівнює $(-1)^{pn}$ [2]. Ця властивість визначає можливість використання матриць Фібоначчі для багатьох додатків у тому числі, – для криптографічних перетворень даних. Властивість збереження за модулем значення детермінанта довільної матриці після множення на Q_p^n-матрицю Фібоначчі:

$$\mathrm{DetC} = \mathrm{Det}\left(M \times Q_p^n\right) = (-1)^{pn} \cdot \mathrm{DetM} \quad (9)$$

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

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

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

$$k = (p+1) \times k_i, \qquad (10)$$

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

$$R_k = \frac{k_i}{(p+1) \cdot w + k_i}$$

де p – порядок Q_p-матриці Фибоначчи; w – довжина слова в бітах (стандартними значеннями є 8, 16 або 32 біт).

Дослідження показали, що надмірність, яка виникає при використанні в перетвореннях інформації арифметики Фібоначчі, від'ємно (обернено) пропорційна порядку p матриці Фібоначчі, але швидко зростає при збільшенні значення ступеню n матриці.

Встановлено, що проведення обчислень у кільці цілих чисел $Z/(q)$ усуває проблему виникнення надмірності інформації при використанні узагальнених матриць Фібоначчі. Достовірність цього факту була доведена математично на підставі висунутої гіпотези щодо гомоморфізму p-чісел і Q_p матриць Фібоначчі в кільці цілих чисел [4].

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

2. Аналіз процедур криптографічного перетворення інформації на основі арифметики Фібоначчі

У ході дослідження був запропонований варіант реалізації симетричного шифру на основі модифікованої мережі Фейстеля з використанням арифметики Фібоначчі.

Необхідною умовою стійкості шифру є досягнення повної дифузії. Важливу роль у процесі дифузії в блокових шифрах грають схеми обміну підблоками (СО) і F-функцій. У традиційних схемах Фейстеля (СФ) F-функція є найбільш (в обчислювальному сенсі) дорогою операцією в раунді і також відіграє ключову роль в дифузійному процесі внаслідок її повноти. Тому оцінка повної дифузії проводилась у термінах обсягу необхідних обчислень F-функцій.

В результаті проведеного аналізу найбільш придатною структури СФ (з точки зору дифузійного процесу) була обрана схема змішування функцій із замкнутою ланцюжком F-функцій, що залежать від двох підблоків (попереднього поточному підблоку і наступного). Перший цикл робить три останніх підблоки повними, наступний раунд робить всі інші підблоки повними. Отже, достатньо тільки двох раундів для повної дифузії, або більш конкретно обчислення 2n-3 F-функцій.

У відповідності з метою роботи була досліджена доцільність використання в СО множення на матрицю Фібоначчі [5]. Були проведені дослідження схем перетворення інформації з використанням матриць Фібоначчі 1-го порядку (4 підблоків, аналогічно RC6), 2-го порядку (9 підблоків) і зроблено узагальнення для схеми з N підблоками.

Проведений аналіз показав, що при $p = 1$ і $n = 1$ для досягнення повної дифузії потрібне виконання шести F-функцій (аналогічно RC6, яка досягає повної дифузії після обчислення шести функцій). Однак, при ступені матриці Фібоначчі $n = 2, n = -1$ і $n = -2$ все підблоки досягають повної дифузії за один раунд, тобто для досягнення повної дифузії потрібно виконання чотирьох F-функцій, що менше, ніж у RC6 і в СФ з аналогічною схемою змішування F-функцій.

При порядку матриці Фібоначчі $p > 1$ повна дифузія досягається за два раунди, проте навіть за один раунд у кожному кластері значно збільшується відносна дифузія, оскільки охоплюється не тільки поточний кластер, але й усі попередні. А оскільки кількість підблоків у кожному кла-стері порівняно і навіть більше), ніж кількість підблоків у сучасних блокових шифрах (3 підблоки в кожному кластері при $p = 2$, при $p = 3–4$ підблоки, при $p = 4–5$ підблоків і т.д. проти $2 \div 4$ підблока в блоці), то таке розповсюдження дифузії спільно з недетермінованістю сприяє посиленню криптостійкості методу.

Посилення процесу дифузії дозволяє створювати на основі цього методу алгоритми, швидкодію яких може бути збільшено за рахунок зменшення кількості ітерацій.

За розробленою схемою при порядку матриці Фібоначчі $p = 1$ з використанням нелінійної функції циклічного зсуву шифру RC6 був побудований алгоритм криптографічного перетворення інформації MDEM, статистичні дослідження суворого лавинного критерію якого підтвердили підвищення швидкості дифузії в порівнянні з аналогом – шифром RC6 завдяки використанню в мережі Фейстеля схеми обміну на основі множення на матрицю Фібоначчі. MDEM при порядку матриці Фібоначчі $p = 1$ і всіх ступенях матриці задовольняє СЛК після 2 раундів (табл. 1), що аналогічно чотирьом раундів RC6, а останній – тільки після п'яти раундів.

Результати статистичного аналізу критеріїв збалансованості, кореляції між входом і виходом алгоритму і кореляційного імунітету підтвердили збереженні статистичної стійкості методу. Вихідна послідовність MDEM має властивості випадкової після 1 раунду (2 раунди RC6), що на 2 раунди швидше, ніж у метода RC6. Таким чином, більш швидке протікання дифузійних процесів в MDEM, у порівнянні з RC6, дає можливість зменшення числа ітерацій і, як наслідок, збільшення швидкості обробки даних.

Таблиця 1

Результати частотного тесту для перевірки суворого лавинного критерію
(мінімальне значення пропорції дорівнює 0.987015)

n	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION
1	1010	999	963	1010	939	1054	957	1043	949	1076	0.016250	0.9889
2	966	1060	973	1024	933	1030	1006	1036	919	1053	0.008410	0.9912
-1	1000	1023	1032	996	971	1045	995	1062	901	975	0.027589	0.9880

Висновки

В результаті дослідження математичного апарату теорії чисел Фібоначчі був виділений ряд властивостей, аналіз яких показав доцільність використання арифметики узагальнених чисел Фібоначчі для виконання операцій хешування інформації. Такою властивістю насамперед є правило множення довільній матриці на матрицю Фібоначчі, які зводяться до простих операцій додавання і зсуву, що призводить до значного зниження обчислювальної складності. Аналіз доцільності використання в СО множення на матрицю Фібоначчі показав прискорення дифузійних процесів при використанні в СО множення на матрицю Фібоначчі порівняно з СФ, що використовує аналогічну схему змішування F-функцій, і шифром RC6. За розробленою схемою з використанням нелінійної функції циклічного зсуву шифру RC6 був побудований алгоритм криптографічного перетворення інформації. Експериментально перевірена та підтверджена ефективність використання арифметики Фібоначчі з точки зору поліпшення показників перемішування при розробці систем симетричного криптографічного перетворення інформації. Статистичні дослідження підтвердили підвищення швидкості дифузії порівняно з аналогом – шифром RC6 завдяки використанню в мережі Фейстеля схеми обміну на основі множення на матрицю Фібоначчі.

Таким чином, більш швидке протікання дифузійних процесів при використанні арифметики Фібоначчі в схемах обміну, порівняно з іншими методами, дає можливість скоротити час обробки інформації при використанні таких алгоритмів у функціях хешування.

Список літератури

1. Schneier B. Applied Cryptography / B.. Schneier. – New York: John Wiley & Sons, 1996.

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

3. Уфимцева В.Б. О свойствах семейства последовательностей обобщенных чисел Фибоначчи и их применении для генерации псевдослучайных чисел / В.Б. Уфимцева // Вісник ХНТУСГ. – Вып.68. – Х.:ХНТУСГ, 2008. – С. 300-305.

4. Самойленко Н.И. Свойства р-чисел и Q_p^n-матриц Стахова в кольце целых чисел Z/(q) / Н.И. Самойленко, В.Б. Уфимцева // Радиоэлектроника и информатика. – Х.: ХНУРЭ, 2003. – № 1. – С. 111-115.

5. Самойленко Н.І. Дифузійний аналіз мережі Фейстеля зі схемами обміну на основі матриць Фібоначчі / Н.І. Самойленко, В.Б. Уфимцева // Наукові вісті НТУ «КПІ». – 2002. - № 6 (26). – С. 146-152.

Надійшла до редколегії 22.05.2015

Рецензент: д-р техн. наук, проф. М.І. Самойленко, Харківський національний університет міського господарства імені О.М. Бекетова, Харків.

ИСПОЛЬЗОВАНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ОБОБЩЕННЫХ ЧИСЕЛ ФИБОНАЧЧИ В КРИПТОГРАФИЧЕСКИХ АЛГОРИТМАХ

В.Б. Уфимцева, М.Ю. Карпенко

Рассматривается целесообразность использования аппарата арифметики Фибоначчи при разработке функций хеширования информации. Точнее, построение хеш-функций на основе симметричного блочного превращения информации с использованием обобщенных чисел и матриц Фибоначчи. Рассмотрены практические принципы, проанализированы свойству и показана перспективность этого направления исследований в рамках усовершенствования статистических показателей криптографических преобразований за счет увеличения диффузии при использовании в схемах обмена подблоками сети Фейстеля матричного превращения Фибоначчи.

***Ключевые слова**: хеш-функция, симметричные криптографические системы, числа, Фибоначчи, схема Фейстеля.*

USING A SEQUENCE OF GENERALIZED FIBONACCI NUMBERS IN CRYPTOGRAPHIC ALGORITHMS

V.B. Ufimtseva, N.Y. Karpenko

The article is devoted to the development of the hash-function of the symmetrical transformation of information which is characterized by the improved indices of mixing. The possibilities of applying the mathematical apparatus of the theory of Fibonacci's numbers for fulfilling the operations of cryptographic conversions are analyzed. Practical principles are developed and the properties of the cryptographic transformations of information with the use for the procedures of the coding of the mathematical of the generalized numbers and matrices of Fibonacci are analyzed. The analysis of the indices of statistical safety is done and the effectiveness of the use of matrix conversion of Fibonacci, from the point of view of an improvement in the indices of mixing, with the development of the systems of symmetrical cryptographic coding is experimentally checked and confirmed.

***Keywords:** hash-function, symmetric cryptosystems, Fibonacci numbers, Feistel Network.*