Н. И. Самойленко, В. Б. Уфимцева

О ВОЗМОЖНОСТЯХ ИСПОЛЬЗОВАНИЯ АРИФМЕТИКИ ФИБОНАЧЧИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В статье рассматривается целесообразность использования аппарата арифметики Фибоначчи в области криптографии. Показана перспективность этого направления исследований в рамках совершенствования статистических показателей симметричных криптографических преобразований информации. Выдвинута и доказана гипотеза о гомоморфизме p-чисел и Q_p-матриц Фибоначчи, разработанных проф. А.П. Стаховым, в кольце целых чисел по модулю q, что позволило избежать возникновения избыточности при использовании арифметики Фибоначчи в различных приложениях. Проведен анализ целесообразности использования умножения на матрицу Фибоначчи в схемах обмена криптографических шифров, который показал ускорение диффузионных процессов по сравнению с обычной схемой Фейстеля.

Введение

Важной составляющей практически любой компьютерной информационной системы является система защиты информации. Радикальное решение проблем защиты электронной информации может быть получено на базе использования криптографических методов, которые позволяют решать важные задачи защищенной автоматизированной обработки и передачи информации (конфиденциальности и целостности). Основным из средств защиты информации в телекоммуникационных системах и сегодня являются симметричные шифры.

В Украине и других странах СНГ с начала 90-х годов прошлого столетия отчетливо прослеживалась тенденция опережения расширения масштабов и областей применения информационных технологий над развитием систем защиты данных. Использование систем защиты зарубежного производства не может выправить этот перекос, поскольку поступающие на рынок Украины продукты этого типа не соответствуют современным требованиям из-за существующих экспортных ограничений, принятых в США – основном производителе средств защиты информации. К тому же сам факт использования зарубежного системного и программного обеспечения создает повышенную потенциальную угрозу информационным ресурсам. Поэтому, перед Украиной остро стоит проблема создания и принятия национального стандарта симметричного шифрования. Сам процесс разработки и создания стандарта приведет к освоению новых технологий и идей защиты информации. Основой для этого являются прошедшие конкурсы на принятие нового стандарта США – Advanced Encryption Standard (AES) и европейский конкурс – NESSI, в процессе открытого обсуждения которых был осуществлен важный прорыв в развитии новых подходов к разработке и построению современных алгоритмов шифрования.

Целью работы является освоение и развитие современных технологий симметричного шифрования, изучение и определение перспективных подходов, которые могут стать основой для разработки новых симметричных шифров, в частности, изучение перспектив и возможностей использования для построения процедур криптографических преобразований свойств арифметики Фибоначчи.

Как известно, современные шифры строятся как итерационные, и основное внимание исследователей сосредоточено на исследовании свойств булевых функций и нестойких процедур перестановок с целью улучшения показателей перемешивания (по Шеннону). В данной работе сосредоточено внимание на возможностях улучшения показателей

перемешивания на основе использования математического аппарата арифметики Фибоначчи. И ставится цель исследовать целесообразность применения арифметики чисел и матриц Фибоначчи при построении симметричных алгоритмов криптографического преобразования информации.

Для достижения поставленной цели в работе ставятся и решаются следующие задачи:

1) изучение возможности применения и разработка математического аппарата арифметики Фибоначчи, разработанной украинским ученым Алексеем Стаховым, для выполнения операций криптографических преобразований;
2) разработка практических принципов и свойств криптографических преобразований информации при использовании математического аппарата арифметики Фибоначчи для процедур шифрования;
3) анализ и исследование показателей статистической безопасности при использовании арифметики *p*-чисел Фибоначчи (А.П. Стахов) для построения симметричных алгоритмов криптографических преобразований.

I. Базовые понятия арифметики Фибоначчи

В ходе решения первой задачи выполнен анализ эффективности применения арифметики Фибоначчи при построении криптографических преобразований и показана перспективность этого направления для криптографии.

Основным объектом исследований этого направления стали обобщенные числа Фибоначчи [1], называемые *p*-числами Фибоначчи (А.П. Стахов), которые являются линейной рекуррентной последовательностью порядка $k = p+1$ с законом рекурсии:

$$F_p(i+p+1) = F_p(i+p) + F_p(i), \tag{1}$$

где $p \in Z \cap p \geq 0$ и $k \in Z$. При начальных условиях:

$$F_p(1) = F_p(2) = \ldots = F_p(p+1) = 1. \tag{2}$$

Традиционным подходом к описанию ЛРП является характеристические многочлены. Как показали исследования, для обобщенных p-чисел Фибоначчи характеристические многочлены имеют вид:

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

При анализе линейных рекуррентных последовательностей *p*-чисел Фибоначчи были выделены последовательности *p*-чисел Фибоначчи максимального периода для $p = \overline{1,152}$ [2]. Анализ основных свойств последовательностей p-чисел Фибоначчи с максимальным периодом показал:

1. Период М-последовательностей p-чисел Фибоначчи равен $T = 2^{p+1} - 1$.

2. Для заданного $f(x)$ существует $2^{p+1} - 1$ различных последовательностей, которые являются $2^{p+1} - 1$ различными сдвигами М-последовательности $F_p(\cdot)$ и имеют вид $F_p(\cdot), Q_p F_p(\cdot), Q_p^2 F_p(\cdot), \ldots, Q_p^p F_p(\cdot)$.

3. Число единичных символов на периоде М-последовательности p-чисел Фибоначчи равно $N\left(F_p(i)=1\right) = 2^p$, а нулевых – $N\left(F_p(i)=0\right) = 2^p - 1$, т.е. вес Хемминга $wt\left(F_p(0,1,\ldots,T-1)\right) = 2^p$. Вероятности появления 1 и 0 определяются выражениями:

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

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

и при увеличении p достигают значений сколь угодно близких к 1/2.

4. В последовательности p-чисел Фибоначчи максимальной длины серии из одного символа (единицы или нуля) встречаются 2^{p-1} раз, из двух единиц или нулей – 2^{p-2} раз и т.д. Серии из p нулей и $p+1$ единиц встречаются только по одному разу. Сравнивая выражения для оценки вероятности появления серий из l одинаковых символов для случайной последовательности с соответствующей вероятностью для М-последовательности, можно убедиться в их практической эквивалентности.

5. Свойство сдвига и сложения. Для каждого целого $s\left(1 \le s \le 2^{p+1}-1\right)$ существует такое целое $r \ne s\left(1 \le r < 2^{p+1}-1\right)$, что $\{F_p(i)\}+\{F_p(i-s)\}=\{F_p(i-r)\}$.

6. Двухуровневая автокорреляционная функция:

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

7. Среди T ненулевых М-последовательностей p-чисел Фибоначчи, формируемых на основе порождающего полинома $f(x)$, имеется одна, обладающая свойством $F_p(i)=F_p(2i), i \in Z$ [2]. Из вида начальных векторов характеристических последовательностей p-чисел Фибоначчи для заданного $f(x)$ можно сделать вывод, что

$$F_p(0,1,2,\ldots,p)=\begin{cases} 10^p, p=2k \\ 01^p, p=2k+1 \end{cases}, \qquad (7)$$

где $k \in N$.

8. Децимацией последовательности p-чисел Фибоначчи по индексу $q(q \in N)$ называется формирование новой последовательности $G_p(i)=F_p(iq), i \in Z$. Любая М-последовательность периода $T=2^{p+1}-1$ может быть получена путем децимации по некоторому нечетному индексу q. При децимации последовательности $F_p(\cdot)$ по индексу $q=T-1=2^{p+1}$ получена обратная последовательность $G_p(i)=F_p(i(T-1))=F_p(-i)$ с обратным полиномом $g(x)=x^{p+1}f\left(x^{-1}\right)=x^{p+1}+x+1$.

В работе обосновывается подход, который строится на использовании понятия обобщенной Q_p-матрицы Фибоначчи [1]. Она представляет собой квадратную $(p+1)\times(p+1)$-матрицу вида:

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

При анализе основных свойств матриц Фибоначчи показано, что при использовании в криптографических преобразованиях умножения матрицы данных на Q_p^n-матрицу Фибоначчи вычислительная сложность преобразования $C(p)$, оцененная числом операций умножения, снижается на $(p+1)^3$, т.к. операция умножения произвольной матрицы M размером $(p+1)\times(p+1)$ на Q_p^n-матрицу Фибоначчи (и, соответственно, операция возведения матрицы Фибоначчи в степень) сводятся к простым операциям сложения и сдвига.

Отмечено важное свойство матриц, которое состоит в том, что матрицы Фибоначчи являются невырожденными, т. к. детерминант матрицы Q_p^n равен $(-1)^{pn}$ [1]. Это свойство

определяет возможность использования матриц Фибоначчи для многих приложений, и в частности, для криптографических преобразований информации.

Свойство сохранения по модулю значения детерминанта произвольной матрицы после умножения на Q_p^n-матрицу Фибоначчи

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

дает возможность не только обнаруживать ошибки без предварительной операции обратного преобразования, но и исправлять их, что может быть использовано в методах аутентификации информации.

Линейность операции умножения на матрицу Фибоначчи определила применение арифметики Фибоначчи в схемах обмена подблоками симметричных методов преобразования, а в качестве оценки эффективности – показатели перемешивания.

Анализ свойств матриц Фибоначчи выявил основное препятствие, стоящее на пути их использования для операций криптографического преобразования – операции умножения на матрицу Фибоначчи и вычисления детерминанта приводят к большой избыточности информации. С помощью проведенных исследований были получены оценки абсолютной избыточности

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

где k_i – абсолютная избыточность одной строки информационной матрицы после преобразования, и относительной избыточности

$$R_k = \frac{k_i}{(p+1) \cdot w + k_i}, \qquad (11)$$

где p – порядок Q_p-матрицы Фибоначчи; w – длина слова в битах (стандартными являются 8, 16 и 32 бита).

Исследования показали, что избыточность, возникающая при использовании в преобразованиях информации арифметики Фибоначчи, обратно пропорциональна порядку p матрицы Фибоначчи, но быстро возрастает при увеличении значения степени n матрицы.

Установлено, что проведения вычислений в кольце целых чисел $Z/(q)$ устраняет проблему возникновения избыточности информации при использовании обобщенных матриц Фибоначчи. Достоверность этого факта была установлена путем строгого математического доказательства выдвинутой гипотезы о гомоморфизме p-чисел и Q_p-матриц Фибоначчи в кольце целых чисел $Z/(q)$ [3].

Основным результатом здесь можно показать то, что сохранение свойств чисел и матриц Фибоначчи в кольце целых чисел по модулю q позволило избежать возникновения избыточности при использовании арифметики Фибоначчи в различных приложениях, в том числе в алгоритмах криптографического преобразования.

II. Анализ процедур криптографического преобразования информации на основе арифметики Фибоначчи

В ходе исследование был предложен вариант реализации симметричного шифра на основе модифицированной сети Фейстеля с использованием арифметики Фибоначчи.

Необходимым условием стойкости шифра является достижение полной диффузии. Важную роль в процессе диффузии в блоковых шифрах играют схемы обмена (СО) подблоками и F-функции. В традиционной схеме Фейстеля (СФ) F-функция является наиболее (в вычислительном смысле) дорогой операцией в раунде и также играет ключевую роль в диффузионном процессе из-за ее свойства полноты. Поэтому, оценка полной диффузии проводилась в терминах объема требуемых вычислений F-функций.

В результате проведенного анализа наиболее подходящей структурой СФ (с точки зрения диффузионного процесса) была выбрана схема смешивания функций с замкнутой цепочкой F-функций, зависящих от двух подблоков (предыдущего текущему подблока и последующего). Первый цикл делает три последних подблока полными, следующий раунд делает все другие подблоки полными. Следовательно, достаточно только двух раундов для полной диффузии, или более конкретно – вычисления $2n$-3 F-функций.

В соответствии с целью работы была исследована целесообразность использование в СО умножения на матрицу Фибоначчи [4].

Были проведены исследования схем преобразования информации с использованием матриц Фибоначчи 1-го порядка с 4 подблоками, аналогично RC6 (рис. 1), 2-го порядка с 9 подблоками, и сделано обобщение для схемы с N подблоками.

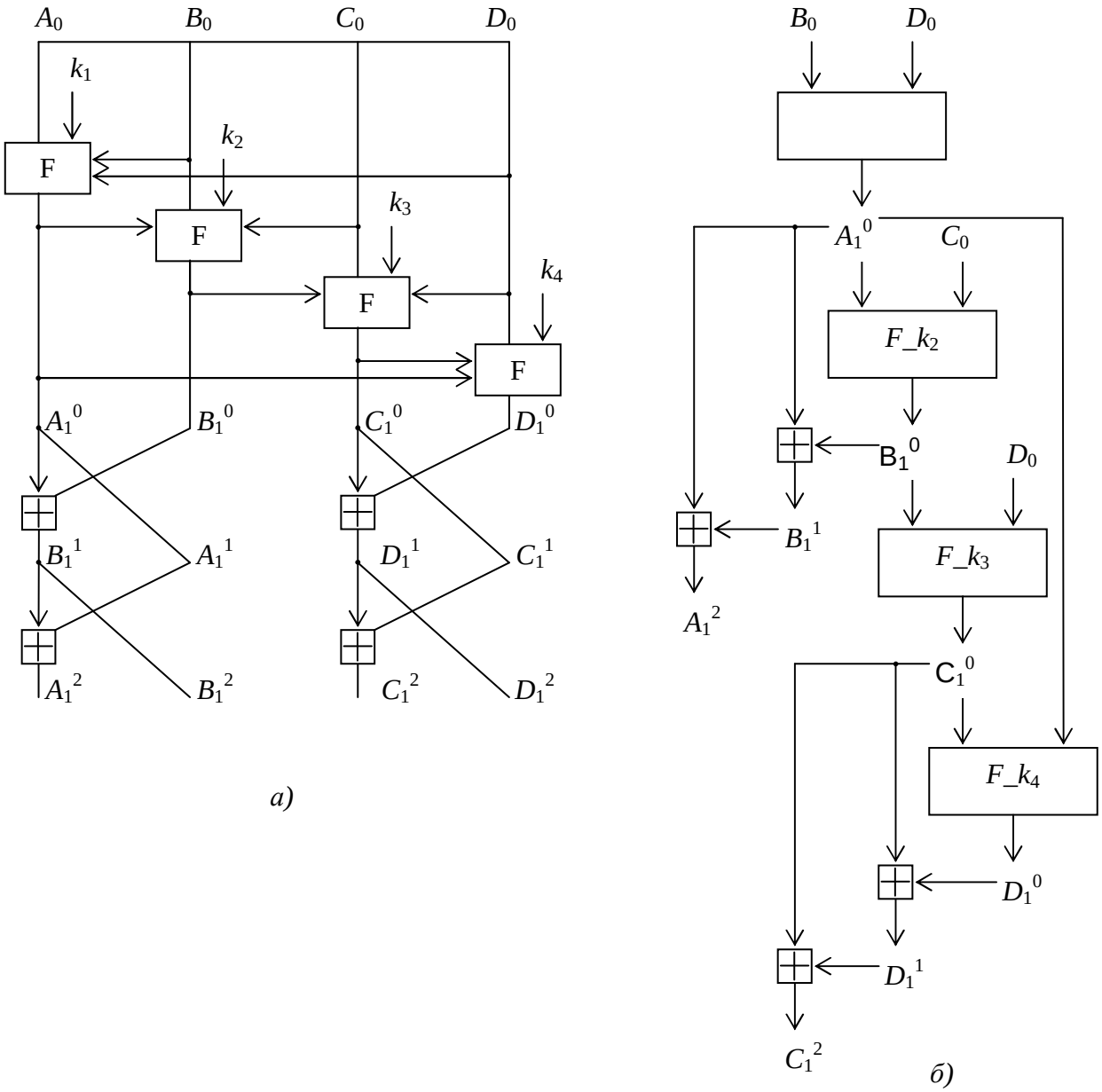

Рис. 1. Схема диффузии MDEM при p = 1 и n = 1 и n = 2:
а) схема метода;
б) прямая схема диффузии

Проведенный анализ показал, что при $p=1$ и $n=1$ для достижения полной диффузии требуется выполнение шести F-функций (аналогично RC6, которая достигает полной диффузии после вычисления шести функций). Однако, при степени матрицы Фибоначчи $n=2,\ n=-1$ и $n=-2$ все подблоки достигают полной диффузии за один раунд, т. е. для достижения полной диффузии требуется выполнение четырех F-функций, что меньше, чем в RC6 и в СФ с аналогичной схемой смешивания F-функций.

При порядке матрицы Фибоначчи $p>1$ полная диффузия достигается за два раунда, однако даже за один раунд в каждом кластере значительно увеличивается относительная диффузия, так как охватывается не только текущий кластер, но и все предшествующие. А так как количество подблоков в каждом кластере сравнимо и даже больше (3 подблока в каждом кластере при $p=2$, при $p=3$ – 4 подблока, при $p=4$ – 5 подблоков и т. д.), чем количество подблоков в современных блочных шифрах ($2\div4$ подблока в блоке), то такое распространение диффузии совместно с недетерминированностью способствует усилению криптостойкости метода.

Усиление процесса диффузии позволяет создавать на основе этого метода алгоритмы, быстродействие которых может быть увеличено за счет уменьшения количества итераций.

По разработанной схеме при порядке матрицы Фибоначчи $p=1$ с использованием нелинейной функции циклического сдвига шифра RC6 был построен алгоритм криптографического преобразования информации MDEM [5]. Статистические исследования строгого лавинного критерия подтвердили повышение скорости диффузии по сравнению с аналогом (шифром RC6) благодаря использованию в сети Фейстеля схемы обмена на основе умножения на матрицу Фибоначчи. MDEM при порядке матрицы Фибоначчи $p=1$ и всех степенях матрицы удовлетворяет СЛК после 2 раундов (табл. 1), что аналогично четырем раундам RC6, а последний – только после пяти раундов.

Таблица – Результаты частотного теста для проверки строгого лавинного критерия (минимальное значение пропорции равно 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

Результаты статистического анализа критериев сбалансированности, корреляции между входом и выходом алгоритма и корреляционного иммунитета подтвердили сохранении статистической стойкости метода. Выходная последовательность MDEM имеет свойства случайной последовательности после 1 раунда (2 раунда RC6), что на 2 раунда быстрее, чем у метода RC6. Таким образом, более быстрое протекание диффузионных процессов в MDEM, по сравнению с RC6, дает возможность уменьшения числа итераций и, как следствие, увеличения скорости обработки данных.

Выводы

В результате исследования математического аппарата теории чисел Фибоначчи был выделен ряд свойств, анализ которых показал целесообразность использования арифметики обобщенных чисел Фибоначчи, разработанной А.П. Стаховым, для выполнения операций криптографических преобразований. Такими свойствами, прежде всего, являются:

– правила умножения произвольной матрицы на матрицу Фибоначчи, которые сводятся к простым операциям сложения и сдвига, что приводит к значительному снижению вычислительной сложности;

– правило вычисления детерминанта матрицы Фибоначчи, которое позволяет провести контроль и даже исправление данных произвольной матрицы, помноженной на матрицу

Фибоначчи, без проведения умножения на обратную матрицу. Это свойство может быть использовано при создании методов аутентификации.

Также, определены свойства ЛРП обобщенных чисел Фибоначчи, которые имеют большое прикладное значение для многих подсистем АСУ (систем защиты информации, синхронизации, передачи информации, измерения параметров движения, испытаний и контроля и других).

Линейность операции умножения на матрицу Фибоначчи определила применение арифметики Фибоначчи в схемах обмена подблоками симметричных методов преобразования, а в качестве оценки эффективности – показатели перемешивания.

В ходе исследований было обнаружено существенное препятствие для использования арифметики Фибоначчи в области криптографии (и многих других областях) – возникновение избыточности информации, существенно возрастающей при увеличении степени матрицы Фибоначчи. В работе была выдвинута и доказана гипотеза о гомоморфизме p-чисел и Q_p-матриц Фибоначчи в кольце целых чисел по модулю q, что позволило избежать возникновения избыточности при использовании арифметики Фибоначчи в различных приложениях, в том числе в алгоритмах криптографического преобразования.

В соответствии с темой работы была исследована целесообразность использования в СО умножения на матрицу Фибоначчи. Анализ показал ускорение диффузионных процессов при использовании в СО умножения на матрицу Фибоначчи по сравнению с СФ, использующей аналогичную схему смешивания F-функций, и шифром RC6.

По разработанной схеме с использованием нелинейной функции циклического сдвига шифра RC6 был построен алгоритм криптографического преобразования информации. Экспериментально проверена и подтверждена эффективность использования арифметики Фибоначчи, с точки зрения улучшения показателей перемешивания, при разработке систем симметричного криптографического преобразования информации. Статистические исследования подтвердили повышение скорости диффузии по сравнению с аналогом (шифром RC6) благодаря использованию в сети Фейстеля схемы обмена на основе умножения на матрицу Фибоначчи.

Таким образом, более быстрое протекание диффузионных процессов при использовании арифметики Фибоначчи в схемах обмена по сравнению с другими методами, дает возможность создания симметричных блочных шифров с меньшим числом раундов с условием сохранения криптографической стойкости и, как следствие, возможность увеличения скорости обработки информации.

Литература:

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 Фибоначчи над конечным полем $GF(q^m)$ // Материалы 7-го Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», ХТУРЕ. – Харьков. – 2003. – С. 417.

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

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.

5. Уфимцева В.Б. Метод и алгоритмы хеширования информации на основе обобщенных матриц Фибоначчи // Научно-технический сборник «Коммунальное хозяйство городов". – К.: Техніка. – 2003. – Вып. 53.– С. 275 – 279.