12. *Мешковский К.А., Кренгель Е.И.* Генерация псевдослучайных последовательностей Гордона, Милза, Велча. – Радиотехника, №5, 1998.

13. *Scholtz R.A., Welch L.R.*. GMW sequences. – IEEE Trans. Inform. Theory, vol. IT-30, №9, 1984.

14. *Скопа О.О., Фількін К.М.* Генератор послідовностей GMW на основі слідів полів Галуа / Наукові записки УНДІЗ. – 2008. – №2(4). – С. 77-82.

15. *Скопа О.О., Фількін К.М.* Нова послідовність GMW для підвищення безпеки радіосистем з кодовим розділенням каналів / Захист інформації. – Спец. випуск (40), 2008. – К.: ДУІКТ. – С.100-103.

16. А.с. №632067, кл. НОЗ К/84 с приоритетом от 03.05.1977. Генератор псевдослучайных последовательностей двоичных сигналов / К. А. Мешковский, Е. И Кренгель.

17. А.с. №674204, кл. НОЗ К/84 с приоритетом от 05.07.1977. Генератор псевдослучайных последовательностей двоичных сигналов / К. А. Мешковский, Е. И Кренгель.

18. *Маракова И.И., Скопа А.А., Сыропятов А.А.* Защита информации в беспроводных системах связи // Матер. IV наук.-техн. конф. «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні», 1-3 березня 2006 р

УДК 621.391.001.12/18:621.391:519.72

С.Л. Волков

Міжнародний гуманітарний університет

МЕТОД ШВИДКОГО РОЗРАХУНКУ ВЗАЄМОКОРЕЛЯЦІЙНИХ ВЛАСТИВОСТЕЙ ЧИСЛОВИХ ПОСЛІДОВНОСТЕЙ З ВИКОРИСТАННЯМ ІЗОМОРФНИХ КОЕФІЦІЄНТІВ

Для оцінки взаємокореляційних властивостей послідовностей, які використовуються для кодування та шифрування інформації, часто використовують пікові значення їх періодичних (парних) взаємно-кореляційних функцій (ПВКФ) і меандро-інвертованих (непарних) взаємно-кореляційних функцій (МІВКФ). У роботі [1] в загальному вигляді запропонований метод дослідження кореляційних функцій періодичних двійкових послідовностей, що будуються на основі різницевих множин. Подальший розгляд та аналіз ідей [1] дав можливість встановити, що метод ґрунтується на можливості застосування до всіх класів таких послідовностей понять ізоморфізму і немножників, введених для різницевих множин. Оскільки такі немножники в [2] названі ізоморфними коефіцієнтами, то такий метод дослідження ПВКФ можна назвати *методом ізоморфних коефіцієнтів*. Подальші викладки показують, що він дозволяє істотно прискорити розрахунок на ЕОМ ПВКФ та МІВКФ.

Нехай $\alpha=(\alpha_1, \alpha_2,...,\alpha_v)$ і $\beta=(\beta_1, \beta_2,...,\beta_v)$ є послідовності довжини $v=2^N-1$, які належать одному класу, і нехай t – деяке позитивне ціле, взаємно просте з v. Оскільки за визначенням t є немножник, то послідовності $a^t=(a_{i_1}, a_{i_2},...,a_{i_v})$ і $b^t=(b_{i_1}, b_{i_2},...,b_{i_v})$, де $i_k=(t(l-1)+1)\bmod v$ для всіх $l=\overline{1,v}$, також належатимуть цьому класу. Очевидно, що ізоморфізм $t:\alpha\to\alpha^t$ є унітарним оператором в евклідовому просторі R^v. Через властивості цього оператора маємо:

$$(\alpha,\beta)=(a^t,b^t). \qquad (1)$$

Позначимо спектр взаємної кореляції послідовностей α і β через $S(\alpha,\beta)$. Тоді, згідно (1),

$$S(\alpha,\beta)=S(a^t,b^t) \qquad (2)$$

і, отже, має місце рівність їх кореляційних максимумів, тобто:

$$\max S(\alpha,\beta) = \max S(a^t, b^t). \qquad (3)$$

Застосовуючи співвідношення (3) до обчислення ПВКФ послідовностей з одного класу еквівалентності, отримаємо, що достатньо дослідити ПВКФ однієї довільно узятої послідовності з тими всіма, що залишилися. Більш того, використовуючи результати теорії чисел [3], можна показати, що множина ізоморфних коефіцієнтів, що складається з представників суміжних класів приведеної групи T вирахувань по модулю v по її мультиплікативній підгрупі H автоморфних коефіцієнтів (множників), також є групою щодо операції множення. Тому для будь-якого немножника t завжди знайдеться такий немножник l, що $t \times l \equiv 1 \bmod v$. Звідси отримаємо, що $\max S(\alpha, a^t) = \max S(\alpha, a^l)$. Це означає, що число досліджуваних пар послідовностей може бути зменшено майже удвічі.

Знайдена властивість дозволяє значно спростити процес обчислення матриці максимальних значень викидів ПФКФ. Як випливає з (2), рядки цієї кореляційної матриці є деякими різними підстановками будь-якого довільно вибраного рядка. Проте в загальному випадку не можна безпосередньо по одному рядку матриці відновити вид всієї матриці, оскільки для цього необхідно провести досить трудомістку роботу за визначенням відповідності елементів початкового рядка елементам решті рядків. Крім того, виникають незручності з запам'ятовуванням такої матриці, зважаючи на її громіздкість. Проте, всіх цих труднощів можна уникнути завдяки перетворенню кореляційної матриці до одного з наступних видів:

1) коли кожний подальший рядок цієї матриці є циклічним зрушенням попередньої;

2) коли сама матриця складається з циклічних зрушень деякої сукупності u квадратних матриць порядку $p < M$, де $up = M$, а M – число всіх ізоморфних кодових послідовностей, тобто потужність коду. При цьому рядки твірних матриць також володіють циклічними властивостями.

При такому уявленні, знаючи тільки перші рядки твірних матриць і порядок їх проходження, можна досить просто відновити будь-який з рядків кореляційної матриці.

Для доказу викладеного, серед множини різних ізоморфних коефіцієнтів виберемо коефіцієнт з максимально можливим порядком. Нагадаємо, що під порядком ізоморфного коефіцієнта t розуміється найменший, відмінний від нуля, показник ступеня l для якого $t^l \bmod v$ є множником. Не порушуючи спільності міркувань, завжди можна вибрати t таким, що $t^l \equiv 1 \bmod v$.

Розглянемо дві можливі ситуації: $l = M$ і $l < M$. У першому випадку l співпадає з потужністю ансамблю. Тому на основі однієї довільно вибраної послідовності за допомогою ізоморфних коефіцієнтів $t, t^2, ..., t^{l-1}$ будуємо систему решти послідовностей цього класу, присвоюючи кожній отриманій послідовності порядковий номер i, де $1 \le i \le l$. Потім, розташувавши послідовності у порядку зростання їх номерів, обчислимо перший рядок кореляційної матриці. Внаслідок того, що $t^{\frac{l}{2}+i} t^{\frac{l}{2}-i} \equiv 1 \bmod v$, досить знайти тільки перші $\frac{l}{2}+1$ її значень. Тепер розглянемо другий рядок кореляційної матриці, що складається з максимальних значень викидів ПВКФ пар послідовностей: $(t,1), (t,t^2), ..., (t,t^{l-1})$. Неважко перевірити, що дані пари послідовностей ізоморфні наступним парам: $(1,t^{l-1}), (1,1), (1,t), ..., (1,t^{l-2})$. Останнє означає, що другий рядок є циклічним зрушенням вправо першого рядка. Аналогічно можна показати, що третій рядок є зрушенням другого рядка і т.д.

Тепер перейдемо до розгляду другого, складнішого і частішого випадку, який зустрічається, коли максимальний порядок, взятий по всій множині ізоморфних коефіцієнтів, менше M. Аналогічно попередньому, також будуємо мультиплікативну групу ізоморфного коефіцієнта t_1 максимального порядку l_1. Припустимо, що існує така мультиплікативна група ізо-

морфного коефіцієнта t_2, яка не належить групі $\{t_1^i\}$ порядку l_2, що $l_1 l_2 = M$. Тоді поступаємо таким чином. Привласнюємо номер 1 будь-якій довільно вибраній кодовій послідовності класу і на її основі за допомогою ізоморфних коефіцієнтів вигляду $t_1^k t_2^i$, де $0 \le k \le (l_1 - 1)$, $0 \le i \le (l_2 - 1)$, будуємо l_2 різних множин, що складаються з l_1 впорядкованих послідовностей. Розташувавши впорядковані таким чином послідовності по рядках і стовпцях, отримуємо кореляційну матрицю K вигляду:

$$K = \begin{bmatrix} A_1 & A_{t_2} & A_{t_2^2} & \dots & A_{t_2^{l_2-1}} \\ A_{t_2^{l_2-1}} & A_1 & A_{t_2} & \dots & A_{t_2^{l_2-2}} \\ \dots & \dots & \dots & \dots & \dots \\ A_{t_2} & A_{t_2^2} & \dots & \dots & A_1 \end{bmatrix},$$

де $A_{t_2^i}$, $0 \le i \le (l_2 - 1)$ – кореляційна матриця порядку $l_1 \times l_2$, стовпці якої відповідають послідовностям вигляду t_l^k, а рядки – послідовностям $t_1^k t_2^l$. При цьому, в силу побудови, рядки матриць $A_{t_2^l}$ також володіють циклічними властивостями.

Відмітимо, що для випадків, коли M є перемноженням великого числа співмножників, побудова проводиться аналогічним чином. Таким чином, отриманана проста процедура побудови кореляційної матриці по її першому рядку, яка дозволяє в $M-1$ раз прискорити розрахунок кореляційних параметрів на комп'ютері.

Як ілюстрацію сказаного розглянемо побудову кореляційної матриці для послідовностей GMW довжини v=63 і v=255. Ці послідовності (по одній з кожного ансамблю) приведені нижче.

1). Послідовність довжини 63:
101000110101100110100011101000100000001111011100 1П101001011011.

2). Послідовність довжини 255:
100001000010111110001011001000110101010110000101011101101111111100010011
001111010111000100101100100011011100111000010001100010001111100111110111
101010111110100100011101001000000110111110001100101110000101100100100110
100100100000001010011011100001111011010.

Для випадку v=63 (M=6) вибираємо ізоморфний коефіцієнт $T = 5$ порядку $l = 6$. По початковій послідовності та множині $\{5^i\}$, $1 \le i \le 5$ будуємо інші п'ять послідовностей ансамблю, яким привласнюємо номери з 2-го по 6-ий. Оскільки $l = M = 6$, то відповідно до вищевикладеного, кореляційна матриця K визначається її першим рядком і має вигляд:

$$K = \begin{bmatrix} 63 & 15 & 23 & 15 & 23 & 15 \\ 15 & 63 & 15 & 23 & 15 & 23 \\ 23 & 15 & 63 & 15 & 23 & 15 \\ 15 & 23 & 15 & 63 & 15 & 23 \\ 23 & 15 & 23 & 15 & 63 & 15 \\ 15 & 23 & 15 & 23 & 15 & 63 \end{bmatrix}.$$

Легко перевірити, що ця матриця повністю співпадає з кореляційною матрицею, отриманою в результаті обчислень звичайним способом.

Для випадку v=255 (M=16) як ізоморфний коефіцієнт, що має максимально можливий порядок, вибираємо $t_1 = 7$ з $l_1 = 8$. Тоді $t_2 = -1$, а $l_2 = 2$, тобто має місце випадок $m = l_1 l_2$. Тому для побудови кореляційної матриці K досить знайти лише перші рядки двох матриць A_1 і

A_{-1}. В результаті розрахунків отримуємо, що матриця $K = \begin{bmatrix} A_1 & A_{-1} \\ A_{-1} & A_1 \end{bmatrix}$ має вигляд:

$$K = \begin{bmatrix}
255 & 47 & 47 & 63 & 63 & 63 & 47 & 47 & 31 & 31 & 63 & 63 & 95 & 63 & 63 & 31 \\
47 & 255 & 47 & 47 & 63 & 63 & 63 & 47 & 31 & 31 & 31 & 63 & 63 & 95 & 63 & 63 \\
47 & 47 & 255 & 47 & 47 & 63 & 63 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 95 & 63 \\
63 & 47 & 47 & 255 & 47 & 47 & 63 & 63 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 95 \\
63 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 95 & 63 & 63 & 31 & 31 & 31 & 63 & 63 \\
63 & 63 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 95 & 63 & 63 & 31 & 31 & 31 & 63 \\
47 & 63 & 63 & 63 & 47 & 47 & 255 & 47 & 63 & 63 & 95 & 63 & 63 & 31 & 31 & 31 \\
47 & 47 & 63 & 63 & 63 & 47 & 47 & 255 & 31 & 63 & 63 & 95 & 63 & 63 & 31 & 31 \\
31 & 31 & 63 & 63 & 95 & 63 & 63 & 31 & 255 & 47 & 47 & 63 & 63 & 63 & 47 & 47 \\
31 & 31 & 31 & 63 & 63 & 95 & 63 & 63 & 47 & 255 & 47 & 47 & 63 & 63 & 63 & 47 \\
63 & 31 & 31 & 31 & 63 & 63 & 95 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 63 & 63 \\
63 & 63 & 31 & 31 & 31 & 63 & 63 & 95 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 63 \\
95 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 63 & 63 & 47 & 47 & 255 & 47 & 47 & 63 \\
63 & 95 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 63 & 63 & 47 & 47 & 255 & 47 & 47 \\
63 & 63 & 95 & 63 & 63 & 31 & 31 & 31 & 47 & 63 & 63 & 63 & 47 & 47 & 255 & 47 \\
31 & 63 & 63 & 95 & 63 & 63 & 31 & 31 & 47 & 47 & 63 & 63 & 63 & 47 & 47 & 255
\end{bmatrix}$$

У багатьох випадках множники різницевих множин і утворених на їх основі послідовностей утворюють мультиплікативну групу по модулю v. Це справедливо для багатьох класів послідовностей, зокрема для послідовностей Лежандра, Хола, а також m- і GMW-послідовностей.

Покажемо, що число цілочисельних точок, в яких необхідно обчислити значення ПВКФ таких послідовностей може бути зменшено з v до v_l, де v_l – число суміжних еквівалентних класів, що отримуються при розбитті повної системи вирахувань по модулю v по мультиплікативній групі H множників різницевої множини. Для доказу цього твердження скористаємося теоремою Джонса-Мана про фіксуючий множник різницевої множини.

Стосовно послідовностей на основі різницевих множин, теорема Джонса-Мана доказує існування такого циклічного зрушення послідовності, яке фіксується кожним її множником [4]. Позначимо це зрушення як α. Тоді $\alpha^h = \alpha$, де $h \in H$. Очевидно, що якщо $b = \alpha^t$, то $b = b^h$. Можна показати, що для будь-якого r взаємно простого з v справедлива рівність: $(\alpha_\tau b) = \left(\left(\alpha^r\right)_{\tau_l} b^r\right)$, де $\tau \equiv \tau_1 r \bmod v$. Звідси витікає, що $(\alpha_\tau b) = (\alpha_{\tau_1} b)$ для всіх $\tau_1 \equiv \tau h \bmod v$ і $\forall h \in H$. Таким чином, ми довели, що значення ПВКФ досить обчислювати не в усіх точках (зрушеннях), а тільки в тих, які є представниками класів суміжності, отриманих при розбитті повної системи вирахувань по модулю v по мультиплікативній групі H.

Як приклад розглянемо обчислення ПВКФ послідовностей символів Лежандра. Ці послідовності існують для всіх простих чисел вигляду $v = 4t - 1$ і мають $M = 2$. З властивостей послідовностей Лежандра слідує, що їх множники співпадають з множиною квадратичних вирахувань по модулю v, при цьому порядок групи H дорівнює $\frac{v-1}{2}$. На цій основі, розбивши числа від 0 до $v-1$ на суміжні класи по множині H, в результаті отримаємо три суміжні класи, представниками яких є елементи {0}, {1} і {–1}. В результаті число точок, в яких досить обчислювати значення ПВКФ, може бути зменшено з v до 3.

Аналогічним чином можна показати, що число точок, необхідних для розрахунку ПВКФ послідовностей Холу, дорівнює 7. Це, безумовно, не означає, що число різних значень

в кореляційному спектрі в точності рівне числу класів суміжності. Воно може бути і меншим як, наприклад, у разі трирівневих *m*-послідовностей.

Висновок. Для дослідження взаємокореляційних властивостей послідовностей, побудованих на основі різницевих множин типу Адамра, розроблений метод ізоморфних коефіцієнтів, який дозволяє істотно прискорити їх розрахунок на ЕОМ і, отже, побудову ФМ-систем з заданими кореляційними властивостями. Перспективним шляхом подальших досліджень є аналіз застосування запропонованого методу для дослідження взаємокореляційних властивостей послідовностей, які не є різницевими множинами типу Адамра.

Список літератури

1. *Кренгель Е, И.* Метод исследования корреляционных функций периодических последовательностей. – Техника средств связи, сер. ТРС, вып.3, 1980.

2. *Свердлик М.Б.* Оптимальные дискретные сигналы. – М.: Советское радио, 1975.

3. *Виноградов И. М.* Основы теории чисел. – М.: Наука, 1972.

4. *Кренгель Е.И.* Исследование и разработка новых классов псевдослучайных последовательностей и устройств их генерации для систем с кодовым разделением каналов. – Дис. канд. техн. наук: 05.12.13: Москва. – М.: РГБ. – 2000 (Из фондов Российской государственной библиотеки).

УДК 519.72:621.391.037.372; 621.396.946

К.Б. Нікіфоренко
ДП «Київський коледж зв'язку»
Н.М. Согіна
ДАТ КБ «Дніпровське»

ДИФЕРЕНЦІЮВАННЯ ВИМОГ, ЩО ПРЕД'ЯВЛЯЮТЬСЯ ДО ГЕНЕРАТОРІВ ПВП, ВИКОРИСТОВУВАНИХ В СТІЛЬНИКОВИХ СИСТЕМАХ ЗВ'ЯЗКУ

Основні положення, які торкаються декомпозиції вимог, що пред'являються до датчиків випадкових і псевдовипадкових чисел, на основі класифікації спеціальних даних, приведені [1...4]. В зазначених джерелах також можна знайти вимоги і до генераторів псевдовипадкових кодових послідовностей (ПВП), які побудовані на основі зазначених датчиків. Проте, слід зазначити, що в згаданих роботах аналіз і систематизація вимог виконані стосовно такої області техніки, як криптографічні методи захисту інформації в технічних системах. Разом з тим сформульовані вимоги достатньо легко переносяться на інші сфери, у тому числі і на алгоритми і пристрої генерації ПВП для систем зв'язку з кодовим розділенням каналів. Численні дослідження, наприклад [5...8], показують, що побудова хороших генераторів випадкових (ВП) і ПВП є не простим завданням. У системах зв'язку з кодовим розділенням каналів, ПВП, як вже наголошувалося, є основою для побудови підсистем управління ключовими структурами, одним з основних завдань якої є формування спеціальних даних.

Різноманітність вирішуваних за допомогою ПВП завдань (для синхронізації роботи крайових пристроїв радіотракту, для ідентифікації абонентських терміналів, безпосередньо для передачі корисної інформації, а також криптозахисту даних) вимагає сумісного застосування в єдиній системі відмінних за природою алгоритмів. Це, у свою чергу, приводить до використання різних спеціальних даних. Очевидно, що алгоритм формування ПВП за умовчанням має на увазі його скритність і високу криптозахищеність. З урахуванням цього для кожного криптографічного перетворення (тобто формування ПВП) потрібні характерні спе-