УДК 519.876.5 : 621.391

Магістрант Жураховський В.І., магістрант Тарасенко К.В.

**Національний технічний університет України
«Київський політехнічний інститут»**

ПОРІВНЯЛЬНИЙ АНАЛІЗ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Abstract

Volodymyr Zhurakhovskyi, student; Kostiantyn Tarasenko, student
Comparative analysis of pseudorandom number generators

The article is devoted to the analysis of existent methods and charts of generation PCS of GMW. The new simple method of generation of binary sequences of GMW is offered on the basis of generation of the moved copies binary m-sequence of that length. Advantage of this method as compared to the known method of Welch-Scholtz is rotined, based on the generation of q-th m-sequence.

Вступ

Актуальність дослідження існуючих та розробки нових способів генерації псевдовипадкових послідовностей (ПВП) викликана широким спектром їх використання в різних галузях техніки, зокрема, в системах рухомого зв'язку, криптографії та ін. Вони складають основу технології систем широкосмугового мобільного зв'язку з кодовим розділенням каналів. Прикладом реалізації такої технології є система CDMA (*Code Division Multiple Access*) [1]. Крім забезпечення розширення спектру і кодового розділення каналів, ще однією важливою вимогою, яка пред'являється до систем радіозв'язку, є забезпечення конфіденційності передачі. Рішення цієї задачі пов'язане із застосуванням ПВП з великим періодом і великою лінійною складністю [2].

Постановка задачі

Задачею є дослідження основних методів та пошук нових способів побудови ПВП з метою розширення періоду генерації та покращення криптографічних властивостей.

Термінологія

Значність кодової послідовності – це кількість розрядів, які утворюють цю послідовність.

Метод розв'язку

Досить широкого (і чи не найбільшого) поширення в широкосмуговому зв'язку набули сімейства ПВП типу Адамара, або *m*-послідовності, оскільки генерація цих послідовностей простіша, а їх властивості в порівнянні з іншими вивчені набагато краще [2]. Ці ПВП характеризуються близькою до ідеальної автокореляцією, період генерації складає величину 2^N-1 (N – розрядність регістра циклічного зсуву, на основі якого будуються генератори ПВП). Проте, будучи лінійними, *m*-послідовності характеризуються малим значенням лінійної складності.

Цього недоліку позбавлені, зокрема, послідовності Гордона, Мілза, Велча, (надалі – послідовності GMW) [2, 3]. Крім того, чисельність сімейства послідовностей GMW при великих значеннях N у багато разів перевищує число *m*-послідовностей. Використання таких послідовностей в системах CDMA істотно розширює число підмножин ПВП з прийнятним рівнем взаємної кореляції, а значить і завадостійкості. Останній фактор дозволяє в одних випадках збільшувати число користувачів при заданій завадостійкості, а в інших – знижувати рівень взаємних завад при фіксованому числі користувачів.

Перші схеми генераторів послідовностей GMW були побудовані та описані ще в 70 р. Принцип роботи генераторів послідовностей GMW ґрунтувався на декомпозиційній властивості самих послідовностей GMW, що дозволяє, теоретично, отримувати всі можливі варіанти послідовностей. Однак, апаратна реалізація таких універсальних генераторів надто складна: в залежності від N складність таких генераторів зростає по експоненціальному закону [2, 3].

В подальшому (1984 р.) був запропонований метод формування класів послідовностей GMW, заснований на генерації q-ї *m*-послідовності [4]. Було показано, що даний метод може бути поширений на інші класи ПВП. В [5] було запропоновано новий клас послідовностей з хорошими авто- і взаємокореляційними властивостями, названими авторами *m*-подібними шифрованими послідовностями. В було показано, що за принципами формування і побудови вони теж належать до класу послідовностей GMW.

В результаті подальших досліджень був запропонований новий метод генерації двійкових послідовностей GMW, який полягає у використанні зсунутих копій двійкової *m*-послідовності [2, 3]. Метод базується на

використанні тільки двійкової логіки, що істотним чином спрощує розробку генераторів як в апаратному, так і в програмному виконанні.

Структурна схема пристрою для генерації ПВП представлена на рис.1.

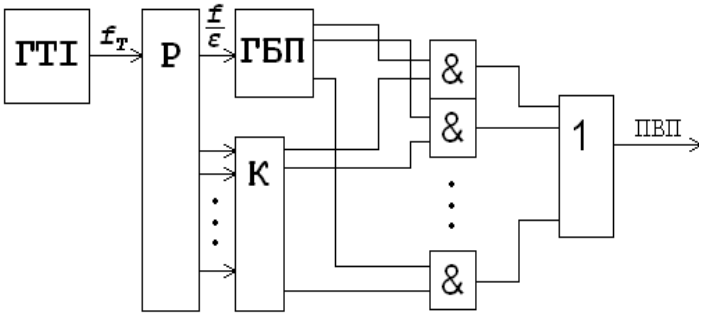

Рис.1. Структурна схема генератора ПВП GMW

Він складається з генератора тактових імпульсів ГТІ, розподілювача Р, комутатора К, генератора базисної послідовності ГБП, елементів І та АБО. Під дією тактових імпульсів з частотою f_T записана в регістрі розподілювача "1" зсувається і, проходячи через комутатор К, відкриває один із елементів І, тим самим, пропускаючи двійковий сигнал з виходу відповідного розряду регістра ГБП на вхід елементу АБО. Вихідні імпульси розподілювача з частотою $\frac{f_T}{\varepsilon}$ поступають на тактовий вхід ГБП, здійснюючи циклічний зсув інформації в цьому регістрі. Таким чином, за один період базисної послідовності на виході елементу АБО формуються сигнали всіх 2^N-1 двійкових символів послідовності, що генерується пристроєм. На комутаторі здійснюється розподіл виходів розрядів регістра розподільника на певні групи, що відповідають різним розрядам регістра ГБП і, відповідно, різним зсувам базисної послідовності. Таким чином із зсувів базисної і нульової послідовностей відповідно до особливостей структури ПВП GMW здійснюється формування сукупності з ε послідовностей.

Перші ε двійкових символів генерованої послідовності збігаються з всіма першими двійковими символами сформованої сукупності. Наступні ε двійкових символів – зі всіма другими двійковими символами тієї ж сукупності і т.д. В результаті такої циклічної процедури в пристрої формуються всі 2^N-1=εΩ двійкових символів ПВП GMW, де ε – кількість двійкових символів в групі, а Ω - кількість груп.

У порівнянні з відомими аналогами розглянутий пристрій для формування двійкових ПВП GMW дозволяє отримувати одну або декілька форм ПВП при значно менших технічних витратах. При суттєвому зменшенні апаратних витрат все-таки отримуємо незначний програш в числі форм, що генеруються [3].

Приклад побудови генератора ПВП GMW значності 63 показаний на рис. 2. У шістнадцятковій системі числення ця послідовність має вигляд A359A3A203DCF49B. Вона відповідає твірному поліному

$$\Omega(x) \equiv (1+x^2y^6+x^3y^3+x^4y^4+x^5y^4+x^6+x^7y^6+x^8y^4) \bmod (x^{63}-1), \quad \text{де} \quad y = x^9.$$

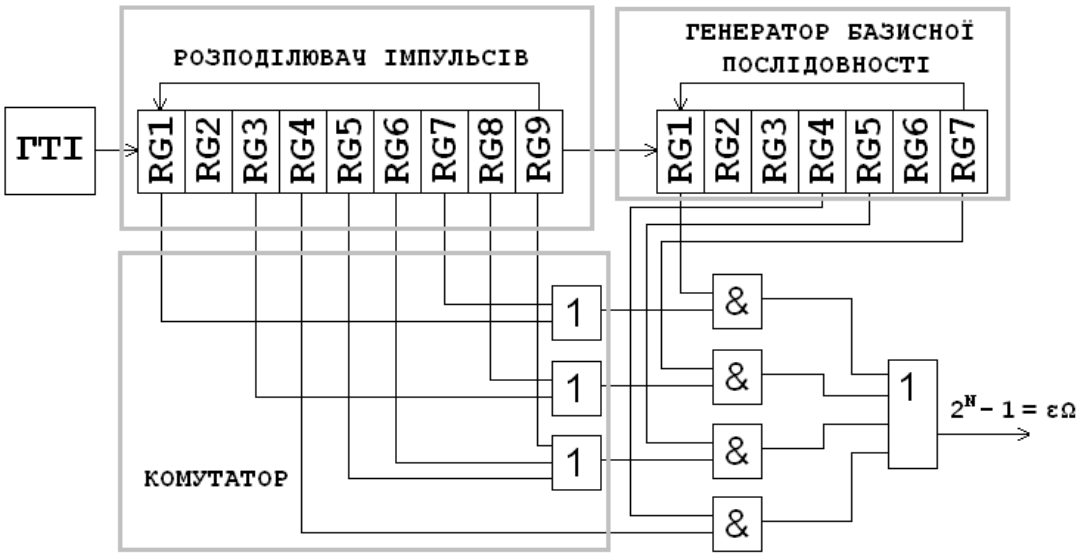

Рис.2. Пристрій для генерації ПВП GMW значності 63

Члени полінома $\Omega(x)$ визначають структуру комутатора пристрою [2, 3], а саме: члени з різними степенями y відповідають різним елементам АБО комутатора; члени з однаковими степенями y відповідають входам одного елемента АБО комутатора; вихід певного розряду розподілювача з'єднується з певним входом одного з елементів АБО комутатора таким чином, що вихід розряду з номером, на одиницю більшим показника ступеня x, з'єднується з входом елементу АБО, відповідного степеню y в члені, що містить цей степінь x; вихід кожного елементу АБО підключається до входу схеми І з номером, на одиницю більшим величини показника відповідного степеня y.

Наведена схема пристрою містить генератор тактових імпульсів ГТІ; комутатор, що складається з 3-х елементів АБО: 2-х двовходових і 1-го тривходового; розподільник імпульсів (9-розрядний циклічний регістр зсуву), генератор базисної послідовності (7-розрядний циклічний регістр зсуву), чотири схеми І, чотиривходовий елемент АБО. Загальне число генерованих цим пристроєм ПВП дорівнює числу існуючих базисних послідовностей, причому ці послідовності належать різним класам ПВП GMW. Так, наприклад, для N=14 пристрій генерує 80 ПВП з різних класів.

Описаний генератор має наступну особливість: якщо регістри розподільника імпульсів і генератора базисної послідовності формувача зробити реверсивними, то число ПВП може бути збільшене удвічі. При цьому, якщо зсув інформації відбувається вправо, пристрій генерує одні ПВП, а при зсуві вліво – ПВП, "зворотні" до перших.

Висновок

Проведено порівняльний аналіз основних відомих схем генераторів послідовностей GMW. Запропоновано просту структуру пристрою генерації двійкових послідовностей GMW на основі генерації зсунутих копій двійкової *m*-послідовності тієї ж довжини.

Література

1. *Стельмашенко Б.Г., Тараненко П.Г.* Нелинейные псевдослучайные последовательности в широкополосных системах передачи информации. – Зарубежная радиоэлектроника. – 1988. –№9.
2. *Фількін К.М.* Декомпозиційний генератор послідовності GMW. – Наукові записки УНДІЗ. – 2008. – №1(3).
3. *Мешковский К.А., Кренгель Е. И.* Генерация псевдослучайных последовательностей Гордона, Милза, Велча. – Радиотехника. –1998. – №5.
4. *Scholtz R.A., Welch L.R. GMW sequences.* – IEEE Trans. Inform. Theory. – 1984. – Vol. IT-30, №9.
5. *Quynh L.C., Prasad S.* Class of binary ciper sequences with best possible autocorrelation function. – IEE Proc. – 1985. – Vol. 132-F, №7.