УДК 681.3.06

Є.В. Яремчук, аспір.
Вінницький державний технічний університет

ПРО ОДИН З КРИТЕРІЇВ ОЦІНКИ ПОСЛІДОВНОСТЕЙ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Описаний критерій дослідження послідовностей псевдовипадкових чисел. Він характеризує середню кількість розрядів характеристичного багаточлена, що змінюються при збільшенні послідовності на один елемент, до загальної їх кількості.

Вступ

В поточних криптографічних алгоритмах в якості гами часто використовуються послідовності псевдовипадкових чисел (*ПВЧ*). Оскільки в якості закону накладання гами використовується, як правило, проста операція, наприклад, порозрядне додавання за модулем 2, то стійкість усього алгоритму визначається якістю гами. Відомо, що алгоритм буде криптографічно стійким, якщо послідовність є *непредикативною вліво* [1].

На сьогодні основною характеристикою, яка використовується для дослідження послідовностей *ПВЧ*, є *лінійна складність* [2]. Чисельне значення останньої визначається як довжина *найкоротшого циклічного регістра зсува* (*НЦРЗ*), за допомогою якого може бути відтворена дана послідовність. Причому, для знаходження $НЦРЗ_r$ довжиною r необхідно щонайменше $2r$ елементів послідовності [2].

В даній статті пропонується оригінальна методика визначення криптографічної якості послідовності *ПВЧ* на основі відомих k елементів (при $k << T$, де T – період послідовності). Основою методики є *критерій непредикативності*.

Опис критерію непредикативності

Припустимо, що відомо k елементів послідовності *ПВЧ*, для яких можна побудувати $НЦРЗ_k$. Доведемо, що при достатньо великому T ймовірність того, що за допомогою побудованого $НЦРЗ_k$ можна точно відновити послідовність повністю, прямує до нуля.

Теорема 1. Якщо відомо k елементів послідовності *ПВЧ* і $k << T$, то ймовірність $P(НКРЗ_k = НКРЗ_T)$ прямує до нуля.

Доведення.

Нехай маємо k відомих елементів послідовності *ПВЧ* за модулем m з періодом T. Представимо їх у вигляді двійкової послідовності довжиною $n = k \lg_2 m$

$$\{S_n\} = s_0 s_1 \dots s_{n-1}, \tag{1}$$

якій відповідає характеристичний багаточлен

$$h(x) = c_{p+1}x^{p+1} + c_p x^p + \dots + c_1 x + 1, \tag{2}$$

де $c_i \in \{0, 1\}$.

Припустимо, що відомі характеристичний багаточлен $h(x)$, що відповідає відомим k елементам, і побудований на його основі $НЦРЗ_k$ довжиною r.

Для доведення теореми використаємо характеристику d [3, 4], яка має назву "*наступне відхилення (next discrepancy)*" і визначається як

$$d = \left(s_r + \sum_{i=1}^{r-1} c_i s_{r-i} \right) mod\, 2. \tag{3}$$

Для побудови *НЦРЗ*, що відповідає послідовності (1), необхідно послідовно підраховувати значення (3), починаючи з найпершого і закінчуючи k-м елементом. Як правило, для знаходження характеристики d застосовують відомий алгоритм *Берлекемпа–Мессі* [3, 4].

Характеристичний багаточлен $h(x)$ зміниться, якщо для деякого j характеристика d буде дорівнювати одиниці, і, відповідно, якщо $d = 0$, то характеристичний багаточлен не зміниться. Тобто для того, щоб характеристичний багаточлен не змінився, для $k+1$, $k+2$... елементів необхідно, щоб $d = 0$ для цих послідовностей.

Ця вимога буде виконуватись при умові, якщо $s_n = 0$ і значення суми у формулі (3) дорівнює парному числу, або якщо $s_n = 1$ і значення суми – непарне число.

Таким чином, маємо дві події A і B, які позначають відповідно отримання $d = 0$ і $d = 1$. Припустимо, що ймовірності подій A і B однакові та дорівнюють:

$$P_i(A) = P_i(B) = \frac{1}{2}.$$

Звідси, ймовірність події C така, що для решти $w = T - k$ елементів послідовності *ПВЧ* характеристичний багаточлен не зміниться, тобто ймовірність появи послідовності подій *AAAAAA*... дорівнює:

$$P(C) = \prod_{i=0}^{n-1} P_i(A) = 2^{-n}, \tag{4}$$

де $n = w \log_2 m$.

При достатньо великому періоді T і незначному k для ймовірності (4) має місце рівність:

$$\lim_{n \to \infty} 2^{-n} = 0.$$

Теорему доведено.

Іншими словами, *Теорема 1* твердить, що, маючи k елементів послідовності, криптоаналітик може встановити залежність між її елементами, так як при $0 < k < T$ ймовірність $P(C) > 0$, і побудувати алгоритм для відновлення усієї послідовності. Але якщо послідовність *непредикативна вліво*, то скільки б елементів послідовності не було відомо криптоаналітику, цього було б недостатньо для побудови *ефективного* алгоритму відтворення усієї послідовності. Якщо ж $k = T$, то криптоаналітик вже має усі елементи послідовності та необхідність у такому алгоритмі відпадає.

Позначимо вектор коефіцієнтів характеристичного багаточлена, що відповідає $НЦРЗ_k$, як $C_k = [c_1, c_2, \ldots, c_{p+1}]$. Введемо функцію $f_\Omega(C_k)$, яка визначає кількість елементів $c_i = 1$. Якщо відомо C_u і C_{u+1}, то кількість розрядів, в яких вони приймають різні значення, знаходиться як

$$v_u = f_\Omega(C_u \oplus C_{u+1}). \tag{5}$$

Введемо *критерій непредикативності вліво* K_1, який є мірою складності відновлення усієї послідовності за відомими k елементами. Враховуючи (5), значення K_1 будемо знаходити за формулою:

$$K_1 = \frac{\sum_{i=0}^{k-1} v_i}{\sum_{i=0}^{k-1} p_i}, \tag{6}$$

де p_i – степінь характеристичного багаточлена для послідовності з i елементів.

На рис. 1. зображено залежності довжини $НЦРЗ_k$ (верхній графік) та v_k (нижній графік) від довжини послідовності k для деякої послідовності, побудованої за допомогою *SM*-генератора [5] з параметрами $m = 27$, $p = 2$, $S_0 = 31$ та $T = 72$.

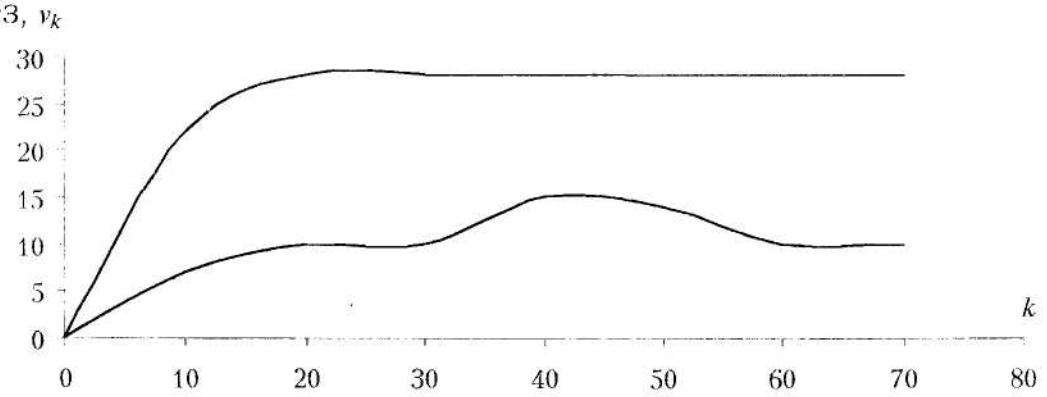

Рис. 1. Залежність довжини НЦРЗ та v від довжини послідовності k

Враховуючи (6), дамо визначення *непредикативності*.

Визначення. Послідовність *ПВЧ* є *непредикативною вліво*, якщо коефіцієнт K_1 задовольняє умові $0{,}3 < K_1 \le 1$.

Нижня межа критерію встановлена приблизно і означає, що *непредикативною* будемо вважати послідовність, характеристичний багаточлен якої змінюється в середньому не менше ніж у 30 % розрядів при збільшенні послідовності на один біт.

Методика дослідження послідовності ПВЧ

Запропонуємо методику дослідження якості послідовності *ПВЧ*, виходячи з припущення 1.

Припущення 1. Нехай маємо k відомих елементів. Якщо послідовність є рівномірною, то різниця значень *критерію непредикативності* для цих k елементів та для усієї послідовності буде менша деякого малого числа ξ:

$$|K_1 - K_1'| < \xi,$$

де K_1 – значення критерію для k елементів, а K_1' – для усієї послідовності.

Наведемо алгоритм обчислення числового значення критерію K_1:

```
L = 1;
K = 0;
C[l] = 0;
for (i = 0; i < k; i++)
 {
  // Виконуємо алгоритм Берлекемпа-Мессі
  // для послідовності з і елементів
   w = f(C, l);
  K = K + w/l;
 }
```

Отримане значення критерію характеризує якість k елементів послідовності. Беручи до уваги *Припущення 1*, можна прийняти, що отримане значення буде характеризувати і всю послідовність.

Дана методика має недолік, який полягає в тому, що можливий випадок, коли для деякого j-того елемента інвертуються певні u розрядів характеристичного багаточлена, а для $j+1$ знову інвертуються ті самі u розрядів. Тобто за цих два переходи змінюється $2u$ розрядів, хоча при цьому характеристичний багаточлен для $j+1$ має такий самий вигляд, як і для $j-1$.

Висновки

1. Запропонований критерій дозволяє дослідити послідовність *ПВЧ* на предмет непредикативності на основі відомих k елементів.
2. Він може бути використаний як альтернатива для лінійної складності або як додаткова характеристика для дослідження якості послідовностей *ПВЧ*.

ЛІТЕРАТУРА:

1. *Brassard J.* "Modern Cryptology", Springer-Verlag, Berlin – Heidelberg, 1988. – 107 p.
2. *Мессі Дж.М.* Введение в современную криптологию // ТИИЭР, 1988. – № 5. – С. 24–42.
3. *Menezes A., van Oorschot P., Vanstone S.* Handbook of Applied Cryptography, CRC Press, 1996.
4. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. – М.: Мир, 1989. – 448 с.
5. *Яремчук Є.В., Азаров О.Д.* Дослідження генераторів послідовностей псевдовипадкових чисел на основі p-чисел Фібоначчі та циклічної маски // Вісник ЖІТІ, 1999. – № 11 / Технічні науки. – С. 173–178.

ЯРЕМЧУК Євген Вікторович – аспірант кафедри обчислювальної техніки Вінницького державного технічного університету.

Наукові інтереси:

- криптографічний захист інформації;
- теорія чисел.

Подано 1.11.1999