УДК 004.42

ВЛАСТИВОСТІ ПОТОКОВИХ КЛЮЧІВ ШИФРУВАННЯ

Б.Л. Шрамченко, кандидат технічних наук, старший науковий співробітник
Київський національний університет технологій та дизайну

Ключові слова: регістр зсуву з лінійним зворотним зв'язком, конфігурація Фібоначчі, конфігурація Галуа, період бітової послідовності, потокові ключі шифрування.

Як відомо [1], мехатронні інформаційні системи включають у себе складову, що відноситься до захисту інформації. Тому питання розробки та дослідження засобів захисту інформації мають пряме відношення до кола питань, що вивчаються у мехатроніці.

У поданій роботі наводяться нові властивості бітових послідовностей на виході генераторів псевдовипадкових послідовностей, що мають конфігурацію Фібоначчі або Галуа. Використання цих властивостей відкриває нові можливості при розробці засобів потокового шифрування.

Традиційним засобом, що використовується при побудові генераторів потокових ключів є регістри зсуву з лінійним зворотним зв'язком (РЗЛЗЗ). Найбільш широке розповсюдження на сьогоднішній день отримали два різновиди РЗЛЗЗ: конфігурація Фібоначчі та конфігурація Галуа. У першій перетворення станів *r*-розрядного регістру при переході від поточного такту до наступного відбувається згідно з виразами

$a_{r-1}^{t+1} = \sum_{i=1}^{r} c_i a_{r-i}^{t}$, (1) (зворотний зв'язок),

$\forall i \mid 1 < i \le r,\ a_{r-i}^{t+1} = a_{r-i+1}^{t}$, (2) (зсув).

У поданих виразах a_s^t – стан комірки *s* у такті *t*, приймає значення 0 або 1. Сума обчислюється за модулем 2. Коефіцієнти зворотного зв'язку (відводи) також приймають значення 0 або 1. Тому вихідний сигнал регістру у такті *t* визначається наступним чином

$$a_0^t = a_1^{t-1} = \ldots = a_{r-1}^{t-r+1} = \sum_{i=1}^{r} c_i a_{r-i}^{t-r}.$$

І оскільки $a_i^{t-r} = a_0^{t-r+i}$, має місце наступне рекурентне співвідношення $a_0^t = \sum_{i=1}^{r} c_i a_0^{t-i}$.

Для другої конфігурації виконуються наступні співвідношення

$$a_{r-1}^{t-r+1} = g_1 a_0^{t-r},$$
$$a_{r-2}^{t-r+2} = g_2 a_0^{t-r+1} \oplus a_{r-1}^{t-r+1},$$
$$a_{r-3}^{t-r+3} = g_3 a_0^{t-r+2} \oplus a_{r-2}^{t-r+2},$$
$$a_1^{t-1} = g_{r-1} a_0^{t-2} \oplus a_2^{t-2},$$
$$a_0^t = g_r a_0^{t-1} \oplus a_1^{t-1}.$$

У поданій системі рівнянь коефіцієнти (відводи) g_i можуть дорівнювати 0 або 1. Підсумувавши рівняння останньої системи отримуємо $a_0^t = = \sum_{i=1}^{r} g_{r-i+1} a_0^{t-i}$.

Звідки переконуємося, що при умові $c_i = g_{r-i+1}$, $i = 1, \dots, r$ (3) обидві конфігурації формують на виході циклічні послідовності, які задовольняють спільному рекурентному співвідношенню.

Для того, щоб регістр Галуа видавав на виході ту ж саму послідовність, що і регістр Фібоначчі, крім відповідності між відводами, треба, щоб мала місце і відповідність між початковими станами регістрів. Визначимо початковий стан ($b_{r-1}, b_{r-2}, \dots, b_0$) регістру Галуа при поданому початковому стані ($a_{r-1}, a_{r-2}, \dots, a_0$) регістру Фібоначчі, що являє собою перші r членів послідовності на виході.

Очевидно, що $b_0 = a_0$, як перший член послідовності на виході.

Далі, з рівняння $b_1 \oplus g_1 a_0 = a_1$ отримуємо $b_1 = g_1 a_0 \oplus a_1$.

Використовуючи співвідношення $b_2 \oplus c_2 a_0 \oplus c_1 a_1 = a_2$, маємо

$$b_2 = g_2 a_0 \oplus g_1 a_1 \oplus a_2.$$

Продовжуючи аналогічно, для будь-якого $i < r$ можемо записати

$$b_i = g_i a_0 \oplus g_{i-1} a_1 \oplus \dots \oplus g_1 a_{i-1} \oplus a_i.$$

Тепер зіставимо поведінку двох регістрів Фібоначчі: RF з відводами $c_1, c_2, \dots, c_r$ та RF^1 з відводами $c_1^1, c_2^1, \dots, c_r^1$, у яких відводи задовольняють відношенню $c_i = c_{r-i+1}^1$, $i = 1, \dots, r-1$ (3). Нехай, у такті t ($t > r$) стан регістру RF – $(a_{r-1}^t, a_{r-2}^t, \dots, a_0^t)$, а RF – $(a_0^t, a_1^t, \dots, a_{r-1}^t)$. Тоді у наступних r тактах на виходах регістрів формуються взаємно інверсні послідовності (для кожного елементу наступний у одній послідовності дорівнює попередньому для цього елементу у іншій послідовності). Для того, щоб показати, що з взаємної інверсії станів у деякому такті t при умові (3) випливає повна взаємна інверсія послідовностей на виході регістрів, достатньо показати, що елемент на виході регістру RF у такті $t+r$ дорівнює елементу на виході регістру RF^1 у такті t-1.

Для регістру RF маємо $a_0^{t+r} = a_{r-1}^{t+1} = \sum_{i=1}^{r} c_i a_{i-1}^t$.

Стан регістру RF^1 у такті $t-1$ має вигляд $(a_1^t, a_2^t, \dots, a_{r-1}^t, x)$, де x – сигнал на виході. Тому для цього регістру має місце співвідношення

$$a_0^t = \sum_{i=1}^{r-1} c_{r-i+1}^1 a_{i-1}^t \oplus x.$$

Враховуючи, що $c_1 \equiv 1$, і те, що сума береться за модулем 2, можемо записати $x = \sum_{i=1}^{r} c_i a_{i-1}^t$, тобто сигнал на виході регістра RF^1 у такті $t-1$ збігається з сигналом на виході регістру RF у такті $t+r$.

Таким чином, запропонована методика визначення початкового стану регістра Галуа, еквівалентного поданому регістру Фібоначчі, показано, що з інверсії відводів у регістрах Фібоначчі випливає інверсія вихідних сигналів, що використовуються як потокові ключі.

Список використаних джерел

1. Егоров О.Д. Конструирование мехатронных модулей: Учебник. / О.Д. Егоров, Ю.В. Подураев. - М.: ИЦ МГТУ "СТАНКИН", 2004.- 360 с.