Д. А. К о л ч и н (Москва, ТВП)**. Об одном методе построения каскадов «прыгающих» регистров сдвига.**

В качестве генераторов псевдослучайных последовательностей (ГПСП) широко используются регистры сдвига, закон функционирования которых зависит от знаков управляющей последовательности. Например, в [1] предложено использовать «прыгающие» линейные регистры сдвига длины n над полем GF(2) с индексом «прыжка» J, где под индексом «прыжка» J линейного регистра сдвига понимается такая степень A^J его сопровождающей матрицы A, что $A^J = A + E$, $J < 2^n - 1$, где E — единичная матрица, в каждый такт работы регистр сдвига осуществляет либо сдвиг на один такт вперед, либо совершает «прыжок» на J шагов по цикловой структуре. Реализация «прыжка» представляет собой умножение на матрицу $A + E$. В [1] показано, что характеристический многочлен полноциклового регистра сдвига с заданным индексом прыжка $J = 2^{n/2} - \delta$, где δ — небольшое фиксированное натуральное число, делит многочлен $(x^{\delta+1} + x^\delta)^{\delta+1} + (x^{\delta+1} + x^\delta)^\delta + x$. Впоследствии данная идея была развита в работах [2]–[4].

С целью увеличения количества вырабатываемых знаков в каждый такт работы ГПСП, автором предлагается использовать каскад из 2^k «прыгающих» полноцикловых регистров сдвига длины n с одинаковыми характеристическими многочленами. Каждый регистр сдвига в каждый такт работы осуществляет либо сдвиг на один такт вперед, либо совершает прыжок на $2^{(n-k)/2} - \delta$ шагов (малый «прыжок» по цикловой структуре), $A + E = A^{2^{(n-k)/2}-\delta}$. При этом характеристический многочлен полноциклового регистра сдвига с заданным индексом «прыжка» делит полином $(x^{\delta+1} + x^\delta)^{2^k(\delta+1)} + (x^{\delta+1} + x^\delta)^{2^k\delta} + x$.

Предлагается способ задания начального заполнения каскада «прыгающих» регистров с гарантированным отсутствием повторов их внутренних состояний в течение $2^{(n-k)/2} - \delta$ тактов. Для этого начальное заполнение первого регистра должно быть ненулевым, начальное состояние $i + 1$ регистра вырабатывается из начального состояния i регистра с использованием большого «прыжка» по цикловой структуре на $2^{n-k} - \delta^2$ шагов, $i = 1, 2, \ldots, 2^k - 1$.

Способ реализации «большого прыжка» может быть выведен из соотношения $A^{2^{n-k}-\delta^2} = (A^\delta + E)^{\delta+1}A^\delta + (A + E)^\delta$. В качестве иллюстрации рассмотрим два простых примера.

Если $\delta = 2^i$, то формула «большого прыжка» принимает вид $A^{2^{n-k}-\delta^2} = E + A^{\delta+1} + A^{2\delta} + A^{2\delta+1}$. При этом для получения состояния регистра сдвига через $2^{n-k} - \delta^2$ тактов требуется проработка регистра в течение $2\delta+1$ тактов с подсуммированием состояний в заданный массив памяти в такты $0, \delta + 1, 2\delta, 2\delta + 1$.

Если $\delta = 9$, то полученная выше формула «большого прыжка» имеет вид $A^{2^{n-k}-81} = A^{19} + A^{17} + A^{11} + A^8 + A + E$.

СПИСОК ЛИТЕРАТУРЫ

1. *Jansen C. J. A.* Modern stream cipher design: A new view on multiple clocking and irreducible polynomials. — In: Gonzalez S., Martinez C., eds.: Actas de la VII Reunion Espanola sobre Criptologia y Seguridad de la Informacion. Volume Tomo I. Servicio de Publicaciones de la Universidad de Oviedo, 2002, p. 11–29.
2. *Jansen C. J. A.* Partitions of polynomials: Stream ciphers based on jumping shift registers. — In: Cardinal J., Cerf N., Delgrange O., Markowitch O., eds.: 26th Symposium on Information Theory in the Benelux, Enschede, Werkgemeenschap voor Informatieen Communicatietheorie, 2005, p. 277–284.
3. *Babbage S., Dodd M.* Finding characteristic polynomials with jump indices, 2006.
4. *Jansen C. J. A.* Stream cipher design based on jumping finite state machines, 2005.