УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
*Том 152, кн. 1* Физико-математические науки *2010*

УДК 681.326+531.19

# СТАБИЛЬНЫЕ СОСТОЯНИЯ АСИНХРОННОГО ГЕНЕРАТОРА

*В.М. Кузнецов, В.А. Песошин, Е.Л. Столов*

**Аннотация**

Объектом исследования является асинхронный генератор, составленный из сумматоров по модулю два с обратными связями. Такие устройства используются в криптографии для генерации случайных ключей. Цель исследования – выработка аналитического инструмента для выявления опасных для процесса генерации стабильных и частично стабильных состояний, из которых генератор не может выйти в процессе работы. Предлагаемая математическая модель основана на исследовании линейных уравнений над полем $GF(2)$ и матриц с неотрицательными элементами. Рассмотрены примеры применения разработанного метода.

**Ключевые слова:** аппаратный генератор ключей, стабильные состояния.

## Введение

Задача порождения случайных ключей, базирующихся на физическом процессе, остается актуальной для целей криптографии. В статье [1] был рассмотрен цифровой стохастический генератор, основанный на автономной асинхронной схеме. Устройство содержит цифровые элементы, выполняющие функции суммирования по модулю два. Генератор образуется путем соединения выходов сумматоров с их входами, при этом на некоторые входы сумматоров могут подаваться постоянные сигналы. На рис. 1 приведен пример такой схемы. Хотя каждый из сумматоров является комбинационной схемой, реальное устройство обладает некоторой случайной задержкой при срабатывании. Если в результате указанных соединений образуется один или несколько контуров обратных связей, то устройство может входить в режим генерации переменного во времени сигнала. Так как сумматоры имеют случайные задержки, то на выходе каждого сумматора формируется двухуровневый случайный процесс с непрерывным временем. Практически разработанные устройства на стандартной элементной базе требуют включения в процесс генерации нескольких десятков сумматоров.

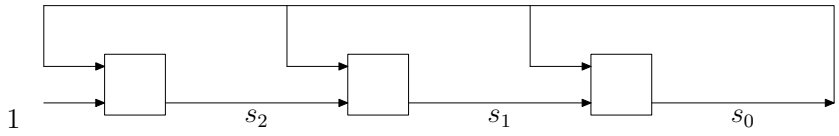


Рис. 1. Пример генератора, составленного из трех сумматоров

Нами была разработана математическая модель функционирования указанного генератора [1]. Генератор рассматривается как устройство, состояние которого в момент времени $t$ определяется вектором, составленным из выходов сумматоров

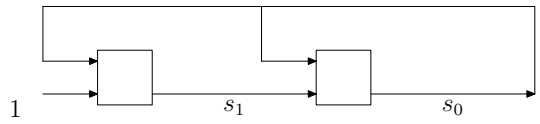


Рис. 2. Пример генератора, имеющего стабильное состояние

в этот момент. Например, состояние схемы на рис. 1 задается вектором $\delta(t) = \langle s_0(t), s_1(t), s_2(t)\rangle$. Это состояние является случайным процессом. Обозначим через $P_\delta(t)$ вероятность того, что в момент времени $t$ генератор находится в состоянии $\delta$. Предположим, что время задержки срабатывания сумматора определяется экспоненциальным законом, сами срабатывания различных сумматоров являются независимыми случайными событиями, а в любой момент времени может сработать лишь один сумматор. В [1] показано, что в этом случае процесс является марковским и $P_S(t)$ удовлетворяет уравнениям Эрланга для систем массового обслуживания. При практическом использовании указанной схемы выбирают некоторый интервал времени $\Delta t$ и снимают состояния генератора с указанным шагом. Качество генератора определяется тем, в какой степени процесс в момент времени $t+\Delta t$ «забывает» свое состояние в момент времени $t$. В свою очередь это свойство зависит от выбора структурной схемы генератора. Скорость «забывания» начального состояния решается в рамках теории Эрланга.

При рассмотрении конкретной схемы приходится решать вопрос о существовании стабильных состояний. Попав в такое состояние, генератор не может из него выйти, и процесс генерации срывается. В качестве примера рассмотрим схему на рис. 2.

Если генератор попал в состояние $\langle s_0, s_1\rangle = \langle 1, 0\rangle$, то он уже не сможет выйти из этого состояния. Особенно актуально решение этой задачи для схем большой размерности. Кроме стабильных состояний могут существовать частично стабильные состояния. Если генератор попадает в такое состояние, то в дальнейшем выходы некоторых сумматоров остаются неизменными, хотя само состояние стабильным не будет. Как следует из определения, если схема содержит $n$ сумматоров, то число состояний генератора равно $2^n$. Теоретически наличие стабильных состояний можно обнаружить, исследуя уравнения Эрланга, количество которых также будет равно $2^n$. Обнаружение частично стабильных состояний с помощью указанных уравнений представляется проблемным. Цель настоящей работы заключается в описании простого алгоритма, позволяющего обнаружить существование стабильных и частично стабильных состояний в заданной структурной схеме, используя матрицы малой размерности над полем $GF(2)$. Очевидно, что при проектировании схемы желательно исключить появление указанных состояний.

## 1. Модель генератора

Все векторы и матрицы рассматриваются над полем $GF(2)$. С основными фактами, относящимися к теории линейных пространств над этим полем, можно ознакомиться по книге [2]. Условимся обозначать греческими буквами векторы пространства, прописными латинскими буквами – матрицы, а строчными латинскими буквами – элементы поля $GF(2)$ или целые числа. Перенумеруем все сумматоры целыми числами от 0 до $n-1$. На часть свободных входов сумматоров поступают постоянные сигналы. Если это сумматор с номером $k$, то постоянный сигнал на его входе обозначим через $b_k$. На выходе сумматора с номером $k$ появляется сигнал $s_k$. Выходом всего генератора является вектор $\delta = (s_0, s_1, \ldots, s_{n-1})^T$. Предполагается,

что в каждый момент времени может сработать лишь один из сумматоров. Это дает альтернативный способ описания структуры генератора. Введем дополнительные обозначения. Если $A$ – матрица, то символ $A[i|j]$ обозначает элемент матрицы, стоящий на пересечении строки с номером $i$ и столбца с номером $j$, а символ $A[i|*]$ – строку с номером $i$.

Сигнал $s_i$ на выходе сумматора с номером $i$ определяется значениями на входах, которые порождаются другими сумматорами и некоторыми постоянными сигналами. В результате срабатывания сумматора с номером $i$ может измениться лишь сигнал $s_i$. Изменение состояния в результате срабатывания этого сумматора в матричной форме имеет вид

$$\delta' = A_i\delta + \beta_i, \tag{1}$$

Здесь векторы $\delta$ и $\delta'$ – состояния генератора до и после срабатывания сумматора с номером $i$, а вектор $\beta_i = (0,\dots,0,b_i,0,\dots,0)^T$, где компонента $b_i$ занимает позицию с номером $i$, $\quad i = 0,\dots,n-1$. Поскольку в результате срабатывания меняется лишь компонента с номером $i$ вектора $\delta$, матрица $A_i$ получается из единичной матрицы изменением лишь строки с номером $i$. В качестве примера рассмотрим схему на рис. 1. Для этого генератора матрицы $A_i$ имеют вид

$$A_0 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Набор матриц $A_i$ и векторов $\beta_i$, $i = 1,\dots,n$ определяет структуру генератора, поэтому вместо рисунка в дальнейшем будем использовать описание схемы с помощью этих матриц.

Так как матрицы $A_i$ и векторы $\beta_i$ имеют специфический вид, вместо самой матрицы $A_i$ достаточно хранить лишь строку $\alpha_i = A_i[i|*]$, а вместо векторов $\beta_i$ – набор чисел $b_i$, $i = 0,\dots,n-1$. Все дальнейшие выводы будем проводить в терминах этих строк и чисел. Будем пользоваться обозначением

$$A = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \cdots \\ \alpha_{n-1} \end{pmatrix}, \quad \overline{\beta} = \begin{pmatrix} b_0 \\ b_1 \\ \cdots \\ b_{n-1} \end{pmatrix}.$$

Матрицу $A$ назовем матрицей переходов генератора.

## 2. Стабильные состояния

Легко видеть, что при нулевом векторе $\overline{\beta}$ нулевое состояние всегда является стабильным.

**Предложение 1.** *Пусть*

$$D = A + I = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \cdots \\ \alpha_{n-1} \end{pmatrix} + I, \quad \overline{D} = \begin{pmatrix} D[0|*], & b_0 \\ D[1|*], & b_1 \\ \cdots & \cdots \\ D[n-1|*], & b_{n-1} \end{pmatrix},$$

*где $I$ – единичная матрица. Тогда генератор обладает ненулевым стабильными состояниями тогда и только тогда, когда*

$$\operatorname{rank}(D) = \operatorname{rank}(\overline{D}), \tag{2}$$

*где* $\operatorname{rank}(D)$ *означает ранг матрицы $D$.*

**Доказательство.** Условие того, что вектор $\delta = (s_0, \ldots, s_{n-1})^T$ является стабильным вектором, согласно (1) имеет вид

$$\delta = A\delta + \overline{\beta}.$$

Последнее условие эквивалентно следующему

$$\alpha_i \delta = s_i + b_i, \quad i = 0, \ldots, n-1.$$

Если $\alpha_i = (a_{i,0}, \ldots, a_{i,n-1})$, то условие стабильности состояния принимает вид

$$a_{i,0}s_0 + a_{i,1}s_1 + \cdots + a_{i,i}s_i + \cdots + a_{i,n-1}s_{n-1} = s_i + b_i,$$

или

$$a_{i,0}s_0 + a_{i,1}s_1 + \cdots + (1 + a_{i,i})s_i + \cdots + a_{i,n-1}s_{n-1} = b_i, i = 0, \ldots, n-1. \qquad (3)$$

Если среди чисел $b_0, \ldots, b_{n-1}$ имеются ненулевые числа, система (3) является неоднородной системой. Согласно теореме Кронекера–Капелли (см., например, [3, с. 167],) эта система совместна тогда и только тогда, когда выполнено условие (2). □

## 3. Частично стабильные состояния

Согласно предложению 1 выполнение неравенства $\operatorname{rank}(D) < \operatorname{rank}(\overline{D})$ гарантирует отсутствие стабильных состояний. В то же время возможна ситуация, когда состояние не является стабильным, но при этом остаются постоянными выходы некоторых сумматоров. Назовем такое состояние частично стабильным. Пусть в частично стабильном состоянии $\delta = (s_0, \ldots, s_{n-1})^T$ на выходах сумматоров с номерами $i_0, \ldots, i_k$, $0 \le k < n-1$, сигналы не меняются в процессе работы генератора. Поскольку нумерация сумматоров является произвольной, можно предложить, что в процессе работы генератора сигналы на выходах сумматоров с номерами $i = 0, \ldots, k$, не меняются. Частично стабильное состояние представим в виде $\delta = (\delta_1, \delta_2)^T$, где $\delta_1 = (s_0, \ldots, s_k)$, $\delta_2 = (s_{k+1}, \ldots, s_{n-1})$. Согласно сделанным предположениям имеют место равенства

$$\alpha_i \delta + b_i = s_i, \quad i = 0, \ldots, k \qquad (4)$$

при любых изменениях в компонентах вектора $\delta_2$.

Положим $\epsilon_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T$, где 1 занимает позицию с номером $i$. Изменение компоненты с номером $j$, $k < j < n$, на противоположный не должно влиять на компоненту с номером $i$, $0 \le i \le k$. Указанное изменение реализуется заменой вектора $\delta$ на $\delta + \epsilon_j$. Из (4) вытекает, что

$$\alpha_i \epsilon_j = 0, \quad j = k+1, \ldots, n-1; \quad i = 0, \ldots, k. \qquad (5)$$

Условие (5) означает, что при указанной нумерации сумматоров

$$A = \begin{pmatrix} C_1 & 0 \\ C_2 & C_3 \end{pmatrix},$$

где $C_1$ есть матрица размером $k+1 \times k+1$. Такая матрица называется разложимой [4, с. 165]. Таким образом, доказано

**Предложение 2.** *Для того чтобы генератор обладал частично стабильными состояниями необходимо и достаточно выполнения равенств* (4)*, из которых следует, что матрица переходов генератора является разложимой.*

Итак, условие разложимости матрицы переходов является необходимым условием для существования частично стабильных состояний генератора. Согласно [4, с. 166] матрица $A$ будет неразложимой тогда и только тогда, когда все элементы матрицы $(I+A)^{n-1}$ будут положительными (при вычислении степени матрицы все операции осуществляются в поле вещественных чисел). Это дает простой способ проверки неразложимости матрицы переходов.

Разложимость матрицы $A$ обеспечивает отсутствие влияния срабатывания сумматоров с номерами $k+1,\dots,n-1$ на выходы сумматоров с номерами $i=0,\dots,k$. Однако это условие не является достаточным для частичной стабильности состояния, поскольку не учитывается влияние срабатывания сумматоров с номерами $i=0,\dots,k$ на данное состояние.

## 4. Примеры

В приведенных выше примерах каждый сумматор имел ровно два входа, поэтому матрица переходов генератора имела не более двух единиц в каждой строке. На самом деле, это ограничение является несущественным, можно рассматривать сумматоры с числом входов больше, чем два, поэтому число единиц в каждой строке матрицы переходов может быть произвольным.

В качестве иллюстрации рассмотрим ситуацию со стабильными состояниями для схемы на рис. 1. Для этой схемы

$$A=\begin{pmatrix}1&1&0\\1&0&1\\1&0&0\end{pmatrix},\quad D=\begin{pmatrix}0&1&0\\1&1&1\\1&0&1\end{pmatrix},\quad \overline{D}=\begin{pmatrix}0&1&0&0\\1&1&1&0\\1&0&1&1\end{pmatrix}$$

Нетрудно видеть, что $\operatorname{rank}(D)=2$ и $\operatorname{rank}(\overline{D})=3$ над полем $GF(2)$, и в схеме отсутствуют стабильные состояния. Над полем вещественных чисел

$$D^2=\begin{pmatrix}1&1&1\\2&2&2\\1&1&1\end{pmatrix}.$$

Это означает, что матрица переходов является неразложимой, поэтому в схеме отсутствуют частично стабильные состояния. В данном случае справедливость полученных утверждений можно проверить непосредственно. Более сложный пример представляет кольцевая схема, состоящая из $n$ сумматоров, когда на вход сумматора с номером $i$ поступает сигнал с сумматора с номером $i+1$, $i=0,\dots,n-2$, а на вход последнего сумматора поступает сигнал с первого сумматора. Легко проверить, что

$$C=\begin{pmatrix}0&1&\cdots&0&0\\0&0&1&\cdots&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\1&0&\cdots&0&0\end{pmatrix}$$

является неразложимой. Матрица переходов $A$ генератора получается добавлением некоторого числа единиц в строки матрицы $C$, поэтому матрица $A$ также будет неразложимой. Это означает, что такая схема не может иметь частично стабильных состояний. Построим матрицу $A$ из матрицы $C$, добавив в каждую строку матрицы $C$ две единицы, причем одна из единиц помещается на главную диагональ. Сумма всех столбцов матрицы $D=I+A$ будет нулевой, поскольку в каждой строке присутствуют две единицы. Это означает, что $\operatorname{rank}(D)<n$. Всегда можно подобрать столбец $\overline{\beta}$ таким образом, чтобы $\operatorname{rank}(\overline{D})=\operatorname{rank}(D)+1$, поэтому такая схема не будет иметь стабильных состояний.

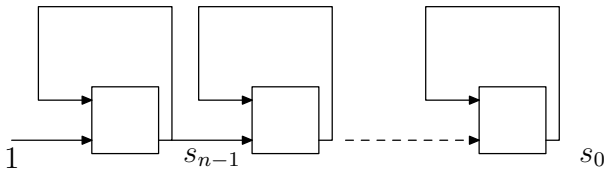


Рис. 3. Пример генератора с локальными обратными связями

Другой крайний случай – схема не имеет глобальной обратной связи (см. рис. 3). Для этой схемы

$$A = \begin{pmatrix} 1 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

В этом случае матрица

$$D = A + I = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Нетрудно проверить, что $\operatorname{rank}(D) = n-1$, $\operatorname{rank}(\overline{D}) = n$, поэтому схема не имеет стабильных состояний. Матрица $A$ будет разложимой, однако и для этой схемы не существует частично стабильных состояний. Действительно, для $i < n-1$ уравнение (4) принимает форму

$$s_i + s_{i+1} = s_i.$$

Отсюда следует, что $s_{i+1} = 0$, поэтому из стабильности сигнала $s_i$ следует стабильность сигнала $s_{i+1}$. В то же время сигнал $s_{n-1}$ не может быть постоянным.

Рассмотрим ситуацию с частично стабильными состояниями. Пусть

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

Легко видеть, что $\operatorname{rank}(D) = 3$. Аналогом уравнений (5) в этом случае являются уравнения

$$\alpha_i \epsilon_j = 0, \quad i = 0, 3; \quad j = 1, 2.$$

Это означает, что выполнены необходимые условия для существования состояния со стабильными битами в позициях 0 и 3. Для выяснения достаточности этих условий надо рассмотреть уравнения (4):

$$\alpha_i \delta = s_i + b_i, \quad i = 0, 3.$$

В данной ситуации эти уравнения имеют решения для любых значений $b_0, \ldots, b_3$. Выберем эти значения таким образом, чтобы было выполнено неравенство $\operatorname{rank}(D) < \operatorname{rank}(\overline{D})$. Достаточно положить их равными 1,0,0,0. В этом случае не будет стабильных состояний, но состояние $(1, *, *, 1)^T$ будет частично стабильным, поскольку не меняются биты в позициях 0 и 3.

**Summary**

*V.M. Kuznetzov, V.M. Pesoshin, E.L. Stolov.* Stable States of Asynchronous Generator.

Asynchronous generators assembled of XOR elements with feedback are under consideration. Such generators are used for random keys production for cryptographic purposes. The goal of the research is to present an analytical procedure for detecting the presence of stable and partly stable states. If the generator is set in one of such states, it stops producing the correct keys. A mathematical model which is based on the theory of linear equations over $GF(2)$ and on the theory of matrices with non-negative elements is suggested. Some examples of implementation of the developed methods are presented.

**Key words:** hardware key generator, stable states.

**Литература**

1. *Кузнецов В.М., Песошин В.А., Столов Е.Л.* Марковская модель цифрового стохастического генератора // Автоматика и Телемеханика. – 2008. – № 9. – С. 62–68.
2. *Гилл А.* Линейные последовательностные машины. – М.: Наука. 1974. – 287 с.
3. *Воеводин В.В.* Линейная алгебра. – М.: Наука, 1974. – 336 с.
4. *Маркус М., Минк Х.* Обзор по теории матриц и матричных неравенств. – М.: Наука, 1972. – 232 с.

Поступила в редакцию
18.01.10

**Кузнецов Валерий Михайлович** – кандидат технических наук, профессор кафедры компьютерных систем Казанского государственного технического университета им. А.Н. Туполева.
E-mail: *Kuznet@evm.kstu-kai.ru*

**Песошин Валерий Андреевич** – доктор технических наук, заведующий кафедры компьютерных систем Казанского государственного технического университета им. А.Н. Туполева.
E-mail: *Pespshin@evm.kstu-kai.ru*

**Столов Евгений Львович** – доктор технических наук, профессор кафедры системного анализа и информационных технологий Казанского государственного университета.
E-mail: *Yevgeni.Stolov@ksu.ru*