УДК 656.259, 004.056

А. Ю. Рожнев, Б. С. Сергеев, И. Г. Тильк

ПОВЫШЕНИЕ НАДЕЖНОСТИ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ТЕОРИИ ЗАПРЕТОВ БУЛЕВЫХ ФУНКЦИЙ

Предложена схема повышения надежности систем передачи информации, построенная с использованием алгоритма шифрования повышенной стойкости. Надежность алгоритма основана на работе генератора гаммы шифра, блок нелинейного усложнения которого спроектирован на базе теории запретов булевых функций.

Ключевые слова: *защита информации, теория запретов булевых функций, гамма шифра, криптоанализ генераторов псевдослучайной последовательности.*

При проектировании систем передачи данных в большинстве случаев достаточно детально исследуется помехозащищенность канала передачи информации. Для этого применяются методы, обеспечивающие увеличение отношения сигнал/шум на входе, помехоустойчивое кодирование и т.п. Однако при этом зачастую не рассматривается задача защиты системы от активного источника сбоев — злоумышленника. Основная цель защиты — предотвращение утечки информации, что возможно обеспечить путем обратимого однозначного преобразования сообщений или хранящихся данных в форму, непонятную для посторонних или неавторизованных лиц.

Для решения этой задачи предлагается построить систему шифрования передаваемой информации, основанную на методе гаммирования. К. Шенноном доказано, что если ключ является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения, причем его длина равна длине исходного сообщения и используется этот ключ только один раз, после чего уничтожается, такой шифр является абсолютно стойким, его невозможно раскрыть, даже если криптоаналитик располагает неограниченным запасом времени и неограниченным набором вычислительных ресурсов [1].

Существенный недостаток абсолютной стойкости шифра — это равенство объема основной информации и суммарного объема передаваемых сообщений. Таким образом, построить эффективный криптоалгоритм можно лишь отказавшись от абсолютной стойкости. Данный результат достигается использованием метода гаммирования, под которым понимают процедуру наложения (с помощью некоторой функции F) гаммы шифра, т.е. псевдослучайной последовательности (ПСП) с выходов генератора, на входную информационную последовательность [2].

Надежность шифрования методом гаммирования определяется качеством генератора ПСП. Один из наиболее эффективных методов криптографического анализа генераторов базируется на использовании теории запретов [3, 4]. Поэтому в целях построения алгоритма повышенной надежности в основу его разработки положен современный математический аппарат теории запретов булевых функций.

Булевы функции без запрета (совершенно уравновешенные функции) широко применяются в теории передачи информации и криптологии. Это обусловлено тем, что при их использовании в генераторах псевдослучайных последовательностей на выходе формируется последовательность, статистические свойства которой максимально приближены к свойствам равновероятной последовательности. Если функция, реализующая работу устройства, имеет запрет, это означает, что не все комбинации битов могут появиться в канале связи: таким образом криптоаналитик получает дополнительную информацию.

Пусть $f(x_1, x_2, ..., x_n) \in F_n$, т.е. f — булева функция n переменных. Пусть некоторое устройство (конечный автомат) преобразует произвольную входную двоичную последовательность в выходную двоичную последовательность по следующему закону:

$$f(x_s, x_{s+1}, ..., x_{s+n-1}) = y_s, \ s = 1, 2, ..., l, \quad (1)$$

где $f \in F_n$, l — натуральное число.

Таким образом, это устройство преобразует последовательность $x = (x_1, x_2, ..., x_{l+n-1}) \in V_{l+n-1}$ в последовательность $y = (y_1, y_2, ..., y_l) \in V_l$ для любого натурального числа l. Такое устройство называется кодирующим устройством с конечной памятью и без обратной связи.

Система уравнений (1) с фиксированной булевой функцией совместна либо для любого натурального числа l при любых значениях правых частей. Если существует такое число l^* и такой набор $\tilde{y} = (\tilde{y}_1, \tilde{y}_2, ..., \tilde{y}_{l^*})^T \in V_{l^*}$, при которых система уравнений (1) несовместна, т.е. выходная последовательность $\tilde{y} \in V_{l^*}$ не может быть получена с помощью данного кодирующего устройства ни при каких входных последовательностях $x = (x_1, x_2, ..., x_{l^*+n-1})^T$, то система уравнений (1) преобразуется к виду

$$f(x_s, x_{s+1}, ..., x_{s+n-1}) = \tilde{y}_s, \ s = 1, 2, ..., l^*. \quad (2)$$

Здесь и далее будем представлять функции в виде полинома Жегалкина.

Определение 1 [3]. Булева функция $f \in F_n$ называется функцией без запрета, если для любого натурального числа l и для любого набора $y = (y_1, y_2, ..., y_l) \in V_l$ система уравнений (1) совместна. В противном случае функция f называется функцией запрета, а набор $\tilde{y} = (\tilde{y}_1, \tilde{y}_2, ..., \tilde{y}_{l^*}) \in V_{l^*}$, для которого система уравнений (1) несовместна, называется запретом булевой функции f длиной l^*.

Определение 2 [3]. Булева функция $f \in F_n$ называется сильно равновероятной, если для любого натурального числа l и для любого набора $y = (y_1, y_2, ..., y_l) \in V_l$ система уравнений (1) имеет ровно 2^{n-1} решений.

Теорема [3]. Булева функция $f \in F_n$ не имеет запрета тогда и только тогда, когда она сильно равновероятна.

Доказательство. Рассмотрим функцию 4 переменных вида

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_1x_2 + x_2x_4 + x_1x_2x_4. \quad (3)$$

Доказательство отсутствия запрета функции (3) приведено в работе [5] на основе построения графа сдвигов [6]. Кроме того, эта функция обладает правым барьером длиной 3, что следует из работы [7].

Применим данную функцию для построения блока нелинейного усложнения генератора ПСП с использованием алгоритма шифрования ТКС-Л, входные биты будем получать с регистров сдвига с линейной обратной связью (LFSR), полиномы обратной связи выберем из числа неприводимых многочленов (таблицу неприводимых многочленов можно найти в работе [8]).

Схема алгоритма шифрования ТКС-Л представлена на рис. 1 (здесь γ — гамма шифра).

Приведем формальное описание алгоритма. Пусть $f_i(z) = \sum_{l=0}^{r_i} f_{i,l} z^l$ — известный полином обратной связи LFSR_i длиной r_i, $i = 1, 2, 3, 4$. Известно, что $r_1 = 19$, $r_2 = 22$, $r_3 = 23$, $r_4 = 17$. Известно также, что полиномы обратной связи разрежены. Пусть $S_i(0) = (x_i(t))_{t=0}^{r_i-1}$ — начальное заполнение LFSR_i и $x_i = (x_i(t))_{t=0}^{\infty}$ — соответствующая порождаемая в LFSR_i последова-

тельность максимальной длиной (М-последовательность) с периодом $2^{r_i}-1$, которая рекуррентна $x_i(t)=\sum_{l=1}^{r_i} f_{i,l}x_i(t-l),\ t\ge r_i$.

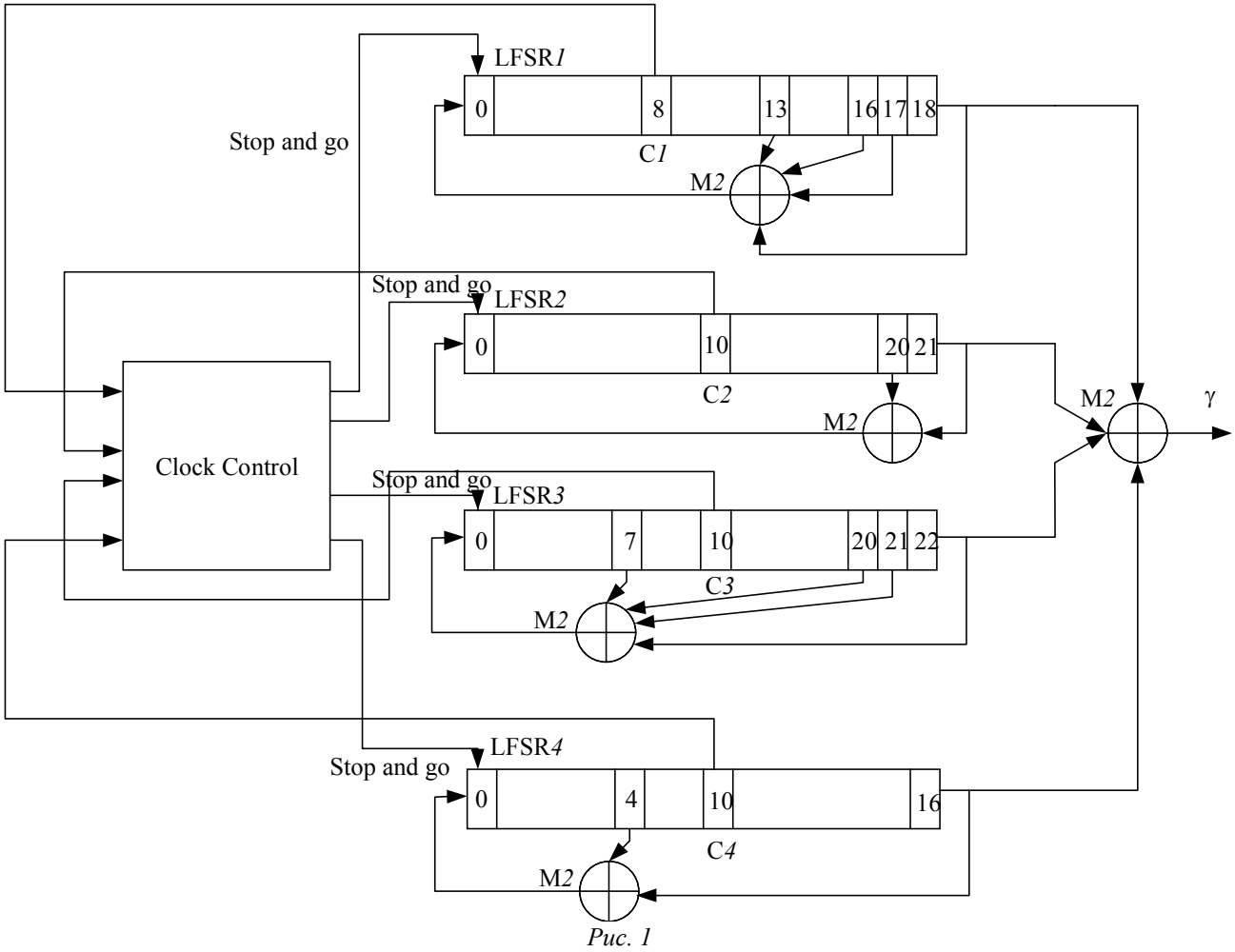

Рис. 1

Пусть $S_i(t)=(s_{i,l}(t))_{l=1}^{r_i}$ — состояние LFSR$_i$ в момент $t\ge 0$ в схеме движения “Stop and go”, а τ_i — номер ячейки в регистре LFSR$_i$, содержимое которой используется для управления движением. При этом полагается, что $\tau_1=8,\ \tau_2=10,\ \tau_3=10,\ \tau_4=10$. Тогда управляющая движением регистров последовательность $C(t)=(C(t))_{t=1}^{\infty}$ задается как

$$C(t)=g(s_{1,r_1}(t),s_{2,r_2}(t),s_{3,r_3}(t),s_{4,r_4}(t)),$$

где g — это функция $f(x_1,x_2,x_3,x_4)=x_1+x_2+x_3+x_1x_2+x_2x_4+x_1x_2x_4$ (см. формулу (3)); причем если значение управляющего бита регистра $s_{i,r_i}(t)$ совпадает с выходным значением этой функции, то такой регистр сдвигается.

О поведении блока Clock Control (см. рис. 1) можно судить по таблице истинности функции (3) (см. таблицу).

x_1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$f(x_1,...,x_4)$	0	0	1	1	1	0	0	1	1	1	0	0	1	1	0	0

Начальное заполнение LFSR определяется в терминах секретного шифра (ключа) в соответствии с уникальным номером фрейма. Уникальный номер фрейма состоит из 22 бит, генерируемых счетчиком и, следовательно, отличающихся для каждого нового сообщения. Секретный сеансовый ключ длиной 81 бит первым загружается в регистры (начальное заполнение состоит из нулей), а затем 22-битовый номер фрейма добавляется в последовательности обратной связи каждого регистра в то время, когда они сдвигаются по описанному в таблице закону. Строго говоря, если $p = (p(t))_{t=-21}^{0}$ — открытый ключ, то для каждого t, $-21 \le t \le 0$, регистры сначала сдвигаются по заданному закону "Stop and go", а затем бит $p(t)$ добавляется в последнюю ячейку каждого LFSR. После 22 таких шагов заполнения LFSR образуют секретный ключ сообщения при генерации шифрующей гаммы. Далее шифрование осуществляется по „классической" схеме гаммирования, приведенной на рис. 2, где G — генератор псевдослучайной последовательности, F — линейная функция гаммирования, F^{-1} — функция, обратная F.

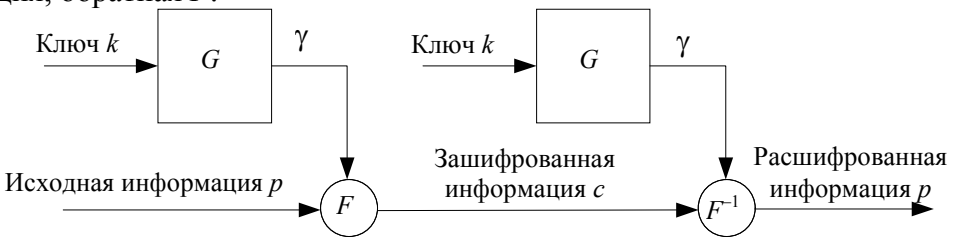

Рис. 2

Предложенный алгоритм защиты систем передачи информации построен на основе современного математического аппарата теории запретов булевых функций. Приведенная схема защиты может быть использована в различных системах передачи при необходимости защиты значимых команд или другой важной информации. В частности, на железнодорожном транспорте [9] применение такого алгоритма целесообразно в канале связи стационарного объекта с локомотивом посредством радиоканала. Информация, передаваемая по этому каналу, непосредственно влияет на безопасность движения поездов, поэтому задача системы защиты передаваемой информации от перехвата и подмены особенно актуальна.

СПИСОК ЛИТЕРАТУРЫ

1. *Шеннон К.* Теория связи в секретных системах // *К. Шеннон*. Работы по теории информации и кибернетике. М.: Изд-во иностр. лит., 1963. С. 333—369.

2. Поточные шифры / *А. В. Асосков, М. А. Иванов, А. А. Мирский, А. В. Рузин, А. В. Сланин, А. Н. Тютвин*. М.: КУДИЦ-ОБРАЗ, 2003. 336 с.

3. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. С. 470.

4. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики. 1994. Т. 1, вып. 1. С. 33—35.

5. *Рожнев А. Ю., Титов С. С.* Исследование булевых функций на запрет в системах связи на железнодорожном транспорте // Вестн. УрГУПС. 2011. № 3(11). С. 21—27.

6. *Смышляев С. В.* Построение классов совершенно уравновешенных булевых функций без барьера // Прикладная дискретная математика. 2010. № 3(9). С. 41—50.

7. *Логачев О. А., Смышляев С. В., Ященко В. В.* Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. Т. 21, вып. 2. С. 51—74.

8. *Schneier B.* Applied cryptography. N.Y.: John Wiley & Sons. 1996. P. 312.

9. *Волынская А. В., Сергеев Б. С.* Предпосылки применения псевдослучайных сигналов-переносчиков в каналах передачи информации железнодорожного транспорта // Транспорт. Наука, техника, управление: Науч.-информ. сб. ВИНИТИ РАН. 2011. № 6. С. 39—42.

Сведения об авторах

Алексей Юрьевич Рожнев — аспирант; Уральский государственный университет путей сообщения, кафедра электрических машин, Екатеринбург; E-mail: alexon@k66.ru

Борис Сергеевич Сергеев — д-р техн. наук, профессор; Уральский государственный университет путей сообщения, кафедра электрических машин, Екатеринбург; E-mail: sergeew@uralmail.com

Игорь Германович Тильк — канд. техн. наук; Уральский государственный университет путей сообщения, НПЦ „Промэлектроника“, Екатеринбург; директор; E-mail: I_Tilk@npcprom.ru

Рекомендована кафедрой автоматики, телемеханики и связи на железнодорожном транспорте УрГУПС

Поступила в редакцию 24.05.12 г.