УДК 656.259, 004.056

ТЕОРИЯ ЗАПРЕТОВ МНОГОБИТОВЫХ ФУНКЦИЙ И ЕЕ ПРИМЕНИМОСТЬ В СИСТЕМАХ СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Рожнев А. Ю.[1]

[1]*ФГБОУ ВПО «Уральский государственный университет путей сообщения», Екатеринбург, Россия (620034, Екатеринбург, ул. Колмогорова, 66), e-mail: alexon@k66.ru*

Показана необходимость повышения информационной безопасности систем передачи данных на железнодорожном транспорте. Проанализирована система передачи данных *GSM-R* по критерию защищенности передаваемой информации от действий злоумышленника, доказана актуальность применения теории запретов для разработки надежных алгоритмов шифрования. Проведено обобщение и развитие существующей теории запретов булевых функций до теории запретов многобитовых функций. Введено понятие обратимости кодирующего автомата с многобитовой функцией *f*, понятие сильной равновероятности и уравновешенности многобитовой функции. Доказано ряд теорем, касающихся различных свойств многобитовых функций в рамках теории запретов. Показана актуальность и необходимость применения теории запретов для построения модуля защиты информации в точечном канале связи с локомотивом (ТКС-Л). Предложена схема построения алгоритма шифрования с использованием метода гаммирования. Также для использования в блоках нелинейного усложнения генераторов псевдослучайных последовательностей предложены функции, у которых доказано отсутствие запретов. При этом дано два варианта таких функций – в случае применения битовой или многобитовой логики. Полученные результаты могут быть использованы при построении модуля защиты информации от действий злоумышленника в ТКС-Л.

Ключевые слова: запрет булевой функции, *GSM-R*, уязвимости систем передачи данных, ТКС-Л, шифрование.

THEORY OF PROHIBITIONS OF MULTIBIT FUNCTIONS AND ITS APPLICABILITY IN THE COMMUNICATION SYSTEMS ON RAILWAY TRANSPORT

Rozhnev A. U.[1]

[1]*Ural State University of Railway Transport, Ekaterinburg, Russia (620034, Ekaterinburg, street Kolmogorova, 66), e-mail: alexon@k66.ru*

In this article is shown the necessity of improving security of the communication systems on railway transport. System of data transmission GSM-R is analysed by criteria of security information transmitted from the deliberate actions of the attacker, proved the relevance of the theory of prohibitions for design of reliable algorithms. A generalization of the theory and development of existing restrictions of Boolean functions to the theory of multi-bit functions of the prohibitions is done. The notion of reversibility coding machine with a multi-bit function *f*, a strong notion of equiprobability and balance multi-bit functions is given. Proved several theorems concerning various properties of multi-bit functions in the framework of prohibitions. The urgency of the theory of prohibition to build an encryption algorithm to isolate the communication channel with a locomotive (TCS-A). A scheme for the construction of an encryption algorithm using XOR is given. Also, for use in blocks of more complex nonlinear generators of pseudorandom sequences, proposed functions, which proves the absence of prohibitions. Thus given two options – in the case of multi-bit or a bit logic. The results obtained can be used in the construction of the security module information on the actions of the attacker in the TCS-A.

Key words: prohibition of Boolean function, GSM-R, vulnerability of data communication systems, TCS-A, encryption.

Введение

Обеспечение безопасности и защиты информационных систем железнодорожного транспорта от несанкционированных вмешательств и воздействий – необходимое условие совершенствования транспортного производства. Наряду с устойчивостью систем передачи информации к естественным и техногенным помехам, что всегда было актуально для железнодорожного транспорта, сегодня требуется защищать их и от умышленных воздействий. В VII разделе Концепции многоуровневой системы управления и обеспечения безопасности движения подчеркнуто, что информационная безопасность является одним из важнейших факторов обеспечения безопасности движения поездов [2]. С использованием систем связи на ОАО «РЖД» передаются значительные объемы информации. В данной работе рассматриваются вопросы защиты той информации, которая непосредственно влияет на безопасность перевозок и обладает коммерческой или иной ценностью.

Природа информации двойственна – она и материальна и нематериальна, однако передаваться информация может только с помощью материальных носителей – сигналов. Сигналы передаются по линиям связи, которые образуют телекоммуникационную сеть. При организации транспортного производства используется более двух десятков видов связи. Все шире внедряются беспроводные технологии, такие как GSM-R, TETRA, CDMA и др. При этом важно отметить, что именно беспроводные технологии наиболее уязвимы с точки зрения информационной безопасности. Перехват информации в беспроводных системах не требует физического контакта с линией связи, что существенно упрощает задачу несанкционированного доступа к информации. В связи с этим непременным условием внедрения беспроводных технологий на ОАО «РЖД» является их многосторонний анализ на предмет выполнения требований информационной безопасности.

1. Анализ системы передачи данных GSM-R.

В устройствах связи ОАО «РЖД» предполагается применение системы GSM-R как основной системы технологической радиосвязи на участках высокоскоростного и скоростного движения, а также на основных транспортных магистралях. К защищаемым информационным активам относится информация, циркулирующая в различных сечениях системы, – ответственные команды, определяющие функциональную безопасность; управленческая и технологическая информация, составляющая коммерческую тайну ОАО «РЖД», служебная информация системы [3]. При этом известно, что система GSM-R обладает рядом уязвимостей и угроз ее информационной безопасности, в частности, прямой перехват сообщений, анализ трафика, несанкционированное декодирование и дешифрование сообщений.

За последние годы в Интернете и СМИ не раз вспыхивали дискуссии как вокруг самой защиты системы мобильной связи GSM, так и вокруг многочисленных уже случаев ее компрометации. В системах GSM, GSM-R в качестве алгоритмов шифрования используются шифры семейства A5. Как показал анализ литературных источников, в основном зарубежных, на каждый из алгоритмов, входящих в семейство, уже существует порядка пяти различных видов атак [1, 9, 10]. Кроме этого, анализ блока нелинейного усложнения стандарта шифрования A5/1, основанный на теории запретов булевых функций, также подтвердил уязвимость этой системы [5]. Работа [5] показала важность такого критерия булевой функции, как запрет, и его влияние на криптографическую стойкость системы шифрования. Наличие запрета у булевой функции *f*, по которой работает блок нелинейного усложнения, свидетельствует о том, что выходная последовательность кодирующего устройства с булевой функцией f не может считаться близкой к реализации последовательности независимых одинаково распределенных случайных величин, принимающих значения 0 или 1 с вероятностями ½ [4]. Дальнейший анализ архитектуры систем шифрования и систем передачи данных показал необходимость обобщения существующей теории запретов булевых функций до теории запретов для многобитовых функций, т.е. функций, аргументы которых определены над полем $GF(2^m)$.

Стандарт шифрования A5/1, используемый в GSM-R, можно считать примером кодирующего аппарата с обратной связью и без памяти, в то время как теория запретов булевых и многобитовых функций применима для всех кодирующих аппаратов без памяти. В настоящей работе приводится математический аппарат теории запретов многобитовых функций.

Математический аппарат теории запретов многобитовых функций

Пусть некоторое устройство (конечный автомат) перерабатывает произвольную входную *m*-битовую последовательность в выходную *m*-битовую последовательность по следующему закону:

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

где $f \in T_n$, l – натуральное число. Таким образом, это устройство перерабатывает последовательность $x = (x_1, x_2, ..., x_{l+n-1}) \in V_{l+n-1}$ в последовательность $y = (y_1, y_2, ..., y_l) \in V_l$, $V_l = GF(2^m)^l$, для любого натурального числа *l*. Такое устройство назовем многобитовым кодирующим устройством с конечной памятью и без обратной связи [6].

Определение 1 [6]. *Функцию* $f \in T_n$ *назовем многобитовой 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 с запретом, а набор $\tilde{y}=(\tilde{y}_1,\tilde{y}_2,...,\tilde{y}_{l^*})\in V_{l^*}$, для которого система уравнений* (1) *не совместна, называется запретом многобитовой функции f длины l^*.*

В работе [5] подробно рассмотрен метод доказательства отсутствия запрета булевой функции, основанный на построении графа сдвигов. В продолжение этого исследования необходимо отметить, что алгоритм построения графа сдвигов целиком основан на понятии обратимости кодирующего устройства. Введем понятие обратимости кодирующего устройства с многобитовой функцией $f\in T_n$, которое перерабатывает произвольную входную *m*-битовую последовательность в выходную *m*-битовую последовательность, и проанализируем его свойства в рамках теории запретов многобитовых функций.

Определение 2. *Кодирующее устройство с многобитовой функцией $f\in T_n$ называется необратимым, если существуют две различные входные последовательности $x=(x_1,x_2,...,x_t)\in V_t$, $z=(z_1,z_2,...,z_t)\in V_t$, $V_t=GF(2^m)^t$, $t > 2n$, такие, что $x_1=z_1, x_2=z_2,...,x_n=z_n, x_{t-n+1}=z_{t-n+1},...,x_r=z_r$ и обе последовательности перерабатываются этим кодирующим устройством в одну и ту же выходную последовательность. В противном случае кодирующее устройство с многобитовой функцией $f\in T_n$ называется обратимым.*

Знание выходной последовательности, а также начала (длины *t*) и конца (длины *t*) входной последовательности определяет всю входную последовательность [4]. Таким образом, можно сделать вывод, что теорема 9.65, приведенная в книге [4], справедлива и для многобитовых функций.

Определение 3. *Многобитовая функция $f\in T_n$ 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 $(2^m)^{n-1}$ решений.*

В случае, когда многобитовая функция $f\in T_n$ является функцией без запрета, ответ на вопрос о близости выходной последовательности кодирующего устройства с этой функцией к реализации последовательности случайных величин, дает следующая теорема.

Теорема 1. *Многобитовая функция $f\in T_n$ не имеет запрета тогда и только тогда, когда она сильно равновероятна.*

Доказательство теоремы аналогично тому, которое приведено в [4] на странице 420, лишь с той разницей, что область определения и множество значений системы уравнений определены над $GF(2^m)$.

Следствие 1. *Многобитовая функция* $f \in T_n$ *называется уравновешенной, если при l=1 система уравнений (1) имеет ровно* $(2^m)^{n-1}$ *решений.*

Обозначим через $\gamma(f,l)$ максимальное по всем возможным наборам правых частей число решений системы (1).

Теорема 2. *Если многобитовая функция* $f \in T_n$ *имеет запрет, то для любого натурального числа M найдется такое натуральное число t=t(M), что* $\gamma(f,t(M)) > M$.

Доказательство. Так как многобитовая функция *f* имеет запрет, то по теореме 1 она не является сильно равновероятной, т.е. найдется такое натуральное число l и такой набор $y = (y_1, y_2, ..., y_l) \in V_l$, $V_l = GF(2^m)^l$, что система уравнений (1) имеет $(2^m)^{n-1} + \alpha$ решений, где $\alpha \geq 1$. Для набора *y* построим наборы длины $(k + 1)l + k(n - 1)$ вида

$$\begin{array}{l} y_1, ..., y_l, \tilde{y}_{l+1}, ..., \tilde{y}_{l+n-1}, y_1, ..., y_l, \tilde{y}_{2l+n-1}, ..., \tilde{y}_{2l+2(n-1)}, \cdots \\ ..., \tilde{y}_{(kl+(k-1)(n-1)+1)}, ..., \tilde{y}_{(kl+k(n-1))}, y_1, ..., y_l, k = 1, 2... \end{array} . \qquad (2)$$

Значение переменных, помеченных волной, выбираются произвольно из $GF(2^m)$. Обозначим через μ_k среднее число входных последовательностей, преобразуемых в одну и ту же выходную последовательность вида (2). Поэтому имеем $\mu_k = (2^m)^{n-1}(1+\frac{\alpha}{(2^m)^{n-1}})^{k+1}$. Из этого следует, что при $k \to \infty, \mu_k \to \infty$. Значит, для любого натурального числа *M* найдется такое натуральное число $k = k(M)$, что $\mu_k > M$, т.е. некоторая последовательность вида (2) длины $t(M) = = (k(M) + 1)l + k(M)(n - 1)$ имеет более чем *M* прообразов, и соответствующая ей система из $t(M)$ уравнений имеет более чем *M* решений. Поэтому для системы (1) выполнено неравенство $\gamma(f,t(M)) > M$.

Теорема 3. *Многобитовая функция* $f \in T_n$ *имеет запрет тогда и только тогда, когда кодирующее устройство с этой функцией необратимо.*

Доказательство. Если кодирующее устройство обратимо, то величина $\gamma(f,l)$ ограничена при $l \to \infty$. Если кодирующее устройство необратимо, то для любого натурального *M* найдется натуральное число $l = l(M)$, что $\gamma(f,t(M)) > M$. Теорема доказана.

Подробные доказательства теорем 1–3 для булевых функций приведены в книге [4].

2. Применимость теории запретов многобитовых функций в точечном канале связи с локомотивом (ТКС-Л).

Автоматическая локомотивная сигнализация с использованием радиоканала (АЛСР) является альтернативой другим функционально аналогичным устройствам. В системе АЛСР для передачи информации используется высокоскоростной радиоканал – точечный канал связи с локомотивом, с соответствующими средствами кодирования, стабильность и надежность которого существенно выше, чем у рельсовых цепей [8]. Вопросы структуры ТКС-Л, а также методы повышения помехоустойчивости передаваемой в ТКС-Л информации рассмотрены в работе [7]. Рассмотрим вопрос защиты информации. Для защиты информации предлагается использовать алгоритм шифрования, основанный на методе гаммирования.

Определение 4 [1]. *Гаммированием называют процедуру наложения (с помощью некоторой функции F) на входную информационную последовательность гаммы шифра, т.е. псевдослучайной последовательности (ПСП) с выходов генератора ПСП.*

Определение 5 [1]. *Последовательность называется псевдослучайной, если, по своим статистическим свойствам, она неотличима от истинно случайной последовательности, но, в отличие от последней, является детерминированной, т.е. знание алгоритма ее формирования дает возможность ее повторения необходимое число раз.*

Схема гаммирования приведена на рис. 1.

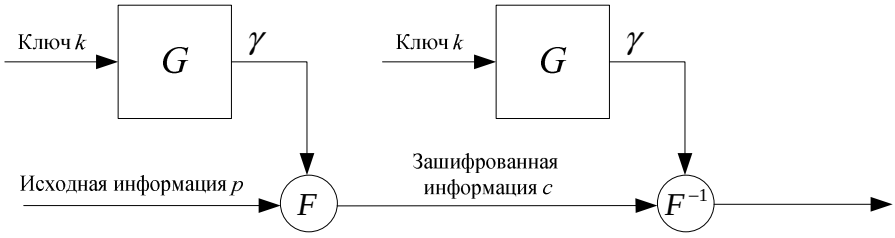

Рис. 1. Шифрование информации методом гаммирования. G – генератор ПСП, F – линейная или нелинейная функция гаммирования, F^{-1} – функция, обратная F, γ – гамма шифра [1]

Надежность шифрования методом гаммирования определяется качеством генератора ПСП. Сами генераторы ПСП состоят из регистров обратной связи (LFSR) и блока нелинейного усложнения. Наиболее значимым при этом с точки зрения криптографической стойкости является блок нелинейного усложнения, т.к. он «перемешивает» криптографически слабые линейные рекуррентные последовательности, получаемые на выходе регистров обратной связи. Как было сказано выше, если функция, по которой работает блок нелинейного усложнения, имеет запрет, то выходная последовательность

этого блока не может считаться близкой к реализации последовательности независимых, одинаково распределенных случайных величин, принимающих значения 0 или 1 с вероятностями ½. В качестве функции блока нелинейного усложнения мы предложим два варианта – для двузначной и многобитовой логики. В качестве первого варианта можно предложить булеву функцию 4-х переменных:

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_1x_2 + x_2x_4 + x_1x_2x_4. \quad (2)$$

Функция (2) записана в форме полинома Жегалкина, $x, y \in GF(2)$.Отсутствие запретов у (2) детально доказано с использованием графа сдвигов [5]. В случае необходимости применения в блоке нелинейного усложнения многобитовой логики можно использовать функцию, линейную по крайней переменной. Для примера, предложим отображение вида

$$f(x_1, x_2, x_3) = x_1 + x_2x_3, \quad (3)$$

где $x, y \in GF(2^m)$. Отсутствие запрета у функций данного класса детально доказано в работе [6].

Таким образом, использование при разработке системы защиты информации в ТКС-Л схемы гаммирования и функции (2) позволит значительно повысить устойчивость системы для исключения возможности криптоанализа и подмены передаваемой информации на локомотив.

Заключение

По итогам проведенных исследований можно сделать вывод, что теория запретов необходима при построении систем защиты передаваемой информации на железнодорожном транспорте. Развитие этой теории для функций различных классов позволит применять полученные результаты при построении генераторов псевдослучайных последовательностей повышенной надежности. В разрабатываемом точечном канале связи с локомотивом (ТКС-Л) теория запретов может быть использована при разработке системы шифрования передаваемой информации на локомотив, что существенно повысит надежность и защищенность этой системы от преднамеренных действий злоумышленника.

Список литературы

1. Асосков А. В., Иванов М. А., Мирский А. А. и др. Поточные шифры. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

2. Концепция информационной подсистемы многоуровневой системы управления и обеспечения безопасности движения поездов (АСУ МС) / Под ред. Н. Г. Шабалина. – М.: Изд-во ВНИИУП, 2003. – 56 с.

3. Корниенко А. А., Диасамидзе С. В. Информационная безопасность системы стандарта GSM-R // Автоматика, связь, информатика. – 2008. – № 12. – С. 32–33.

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

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

6. Рожнев А. Ю. Обобщение теории запретов булевых функций для многобитовых последовательностей // Транспорт XXI века: исследования, инновации, инфраструктура: материалы начн.-техн. конф., посв. 55-летию УрГУПС. – Т. 1. – 2011. – С. 395–399.

7. Рожнев А. Ю. Исследование основных характеристик декодера точечного канала связи с локомотивом // Электроника и электрооборудование транспорта. – 2011. – № 5–6. – С. 13–16.

8. Тильк И. Г., Сергеев Б. С. Анализ работы автоматической переездной сигнализации // Транспорт: наука, техника, управление. – 2006. – № 11. – С. 24–27.

9. Kaliski B.S., Robshaw M. J. B. Linear cryptanalysis using multiple approximations // In Proceedings of Advances of Cryptology – CRYPTO’94. Lect. Notes in Comp. Sci. Springer-Verlag. – 1994. Vol. 950. – P. 26–39.

10. Kuzmin A. S., Kurakin V. L., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules. (Contemporary Math. and its Appl. Thematic surveys. 1994. V. 10. Algebra 2. Moscow) // J. of Math. Sciences. – 1995. V. 76. No. 6. – P. 2793–2915.

Рецензенты:

Нестеров В. Л., д.т.н., профессор, профессор кафедры «Автоматика, телемеханика и связь» Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург.

Сергеев Б. С., д.т.н., профессор, профессор кафедры «Электрические машины», Уральский государственный университет путей сообщения, г. Екатеринбург.