УДК 621.39

А. С. Кривоногов
Санкт-Петербургский государственный электротехнический университет "ЛЭТИ" им. В. И. Ульянова (Ленина)
Е. О. Кривоногова
АО "Научно-инженерный центр электротехнического университета" (Санкт-Петербург)

Алгоритм идентификации вида скремблирования бинарных данных

Рассмотрена задача определения вида скремблера, примененного на передающей стороне, на основании сигнала с его выхода. Задача такого рода является актуальной для систем радиомониторинга и при создании когнитивных систем приема и обработки цифрового сигнала. Известны технические решения, позволяющие идентифицировать структуры как аддитивного, так и мультипликативного скремблера [1]–[4]. Однако публикаций, в которых приводился бы алгоритм автоматического определения вида скремблера, нет. Предлагаемая статья призвана частично восполнить этот пробел. Приведен алгоритм, обеспечивающий решение указанной задачи, и результаты его моделирования.

Скремблер, идентификация, радиомониторинг, псевдослучайная последовательность

В современных системах радиомониторинга существует необходимость демодуляции и декодирования радиосигналов сторонних систем радиосвязи без априорной информации об их передатчике [1]. Для решения этой задачи используются "слепые" алгоритмы идентификации параметров блоков обработки и формирования сигнала, использующихся на передающей стороне. В результате решения указанной задачи определяется структура передатчика, что позволяет построить соответствующую ей приемную часть и осуществить прием сигнала.

В настоящее время широко распространены цифровые системы радиосвязи. Это приводит к необходимости разработки алгоритмов определения (идентификации) блоков обработки и формирования радиосигналов, свойственных этим системам [1]. Одним из таких блоков является скремблер. Существует два вида скремблеров, различающихся способом взаимодействия с цифровым сигналом: аддитивные и мультипликативные [5]. В настоящей статье приведен алгоритм, позволяющий по результатам анализа сигнала с выхода передатчика идентифицировать вид используемого скремблера. При этом предполагается, что вся сопутствующая обработка (демодуляция, декодирование и т. д.) сигнала, предшествующая дескремблированию, успешно осуществлена.

На сегодняшний день существует множество публикаций, посвященных вопросу идентификации структуры скремблера (см., в частности [1], [2]). При этом работы, в которых решалась бы задача определения вида скремблирования, авторам настоящей статьи неизвестны. Предлагаемая статья призвана частично восполнить этот пробел.

Краткие теоретические сведения. Скремблирование используется на передающей стороне систем цифровой передачи информации для уменьшения вероятности появления длинных последовательностей нулей и единиц. Такие последовательности в передаваемом сигнале могут нарушить работу систем синхронизации на приемной стороне.

Существует два вида скремблеров – аддитивные и мультипликативные [1]. Их обобщенные структуры приведены на рис. 1, *а* и *б* соответственно. В состав обоих видов скремблеров входит регистр сдвига с линейной обратной связью (РСЛОС), описываемый порождающим полиномом [6]

$$G(x) = \sum_{i=0}^{d} g_i x^i,$$

где d – память РСЛОС и $g_i \in GF(2)$. Если коэффициент $g_i \neq 0$, соответствующий ключ в схеме РСЛОС замкнут. На практике наибольшее распространение получили порождающие полиномы с тремя или пятью ненулевыми коэффициентами.

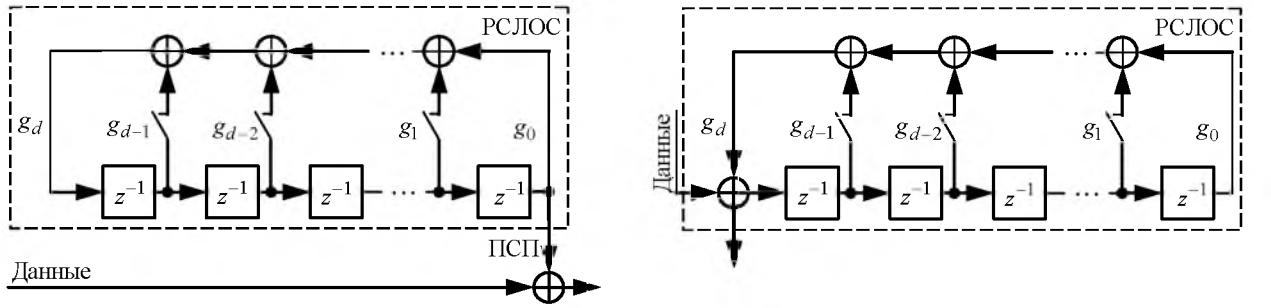

Рис. 1

В аддитивном скремблере РСЛОС используется в качестве генератора псевдослучайной последовательности (ПСП). Скремблирование в этом случае осуществляется прибавлением (в поле $GF(2)$) ПСП к скремблируемому сигналу. В мультипликативном случае скремблируемый сигнал поступает на вход РСЛОС.

Операцию скремблирования можно описать в полиномиальном виде. Если информационный сигнал, состоящий из N бит, представлен в виде полинома [6]

$$D(x) = \sum_{i=0}^{N-1} D_i x^i,$$

где D_i – соответствует $(N-1-i)$-му биту последовательности, то полином $S_{\text{mul}}(x)$, описывающий выходной сигнал мультипликативного скремблера, будет равен [6]

$$S_{\text{mul}}(x) = D(x)/G(x). \qquad (1)$$

Если сигнал скремблируется аддитивно, то полином $S_{\text{ad}}(x)$, описывающий выходной сигнал аддитивного скремблера, будет равен [6]

$$S_{\text{ad}}(x) = I(x)x^N / G(x) + D(x), \qquad (2)$$

где $I(x)$ – полином, характеризующий внутреннее состояние РСЛОС, причем его степень меньше степени полинома $G(x)$.

Также для формирования алгоритма необходимо описать в полиномиальном виде операцию мультипликативного дескремблирования. Полином $D(x)$ на выходе мультипликативного дескремблера рассчитывается как

$$D(x) = S_{\text{mul}}(x)G(x). \qquad (3)$$

Исходные данные и постановка задачи. Задача идентификации вида скремблирования формулируется для модели, представленной на рис. 2.

Генератор бинарных данных имитирует данные, передаваемые в системах радиосвязи. Он генерирует битовый поток с заданной вероятностью единицы $P(D_i = 1) = 0.5 - \tau, \quad \tau \in (0, 0.5)$. Скремблер скремблирует поступающие от генератора данные по аддитивной или мультипликативной схеме. При скремблировании используется априорно известный порождающий полином $G(x)$ степени d с t ненулевыми коэффициентами.

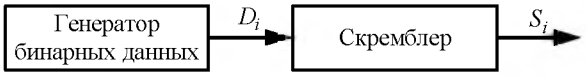

Рис. 2

Задача идентификации состоит в определении вида используемого скремблера (мультипликативный или аддитивный) на основании бинарного сигнала длины N бит, формирующегося на его выходе. Исходными данными для решения задачи являются скремблированный сигнал и порождающий полином $G(x)$, информация о котором может быть получена с использованием алгоритмов, описанных в [1], [2]. Также предполагается, что $N \gg d$.

Описание алгоритма. Алгоритм идентификации состоит в мультипликативном дескремблировании анализируемого сигнала при помощи дескремблеров, описываемых полиномами $G(x)$ и $G^{2^m}(x)$, где m – параметр алгоритма. Согласно выражению (3) это эквивалентно умножению полинома $S(x)$, описывающего сигнал с неизвестным видом скремблирования, на полиномы $G(x)$ и $G^{2^m}(x)$ соответственно. Если сигнал был скремблирован аддитивно, то с учетом (2) в результате перемножения получатся полиномы

$$A(x) = S(x)G(x) = \left[\frac{I(x)x^N}{G(x)} + D(x)\right]G(x) = I(x)x^N + D(x)G(x), \qquad (4)$$

$$B(x) = S(x)G^{2^m}(x) =$$

$$= -I(x)x^N G^{2^m-1}(x) + D(x)G^{2^m}(x). \quad (5)$$

Если сигнал был скремблирован мультипликативно, то с учетом (1) итогом перемножения будут полиномы

$$V(x) = S(x)G(x) = D(x), \quad (6)$$

$$F(x) = S(x)G^{2^m}(x) = D(x)G^{2^m-1}(x). \quad (7)$$

Для того чтобы принять решение о виде скремблирования, необходимо проанализировать статистические свойства полученных при дескремблировании последовательностей. Выражение (4) представляет собой сумму двух полиномов. Количество ненулевых коэффициентов в первом полиноме не превышает степени полинома $I(x)$ и в общем случае много меньше, чем во втором слагаемом полиноме. Поэтому влияние первого полинома на статистические свойства дескремблированной последовательности можно считать пренебрежимо малым.

Второе слагаемое в (4) описывает поток информационных данных после мультипликативного дескремблера. Вероятность появления ненулевого бита на его выходе в соответствии с [1] в этом случае составляет

$$P(A_i = 1) = \frac{1 - \left[1 - 2P(D_i = 1)\right]^t}{2}, \quad (8)$$

где A_i – i-й коэффициент полинома $A(x)$.

Выразив правую часть (8) через τ, получим отклонение вероятности $P(A_i = 1)$ от 0.5:

$$\tau_1 = \left|0.5 - P(A_i = 1)\right| = (2\tau)^t / 2. \quad (9)$$

Рассмотрим выражение (5). Первый слагаемый полином не влияет на статистические свойства дескремблированной последовательности, и им можно пренебречь, если количество ненулевых коэффициентов в нем достаточно мало по сравнению со вторым слагаемым. Это условие обеспечивается выбором значения параметра m и протяженности анализируемого отрезка сигнала.

Второе слагаемое в (5) описывает поток информационных данных, подвергнутый мультипликативному дескремблированию, причем количество отводов в дескремблере определяется числом ненулевых коэффициентов в $G^{2^m}(x)$. С учетом свойств полиномов над полем $GF(2)$ [6] количество ненулевых коэффициентов в $G^{2^m}(x)$ будет равно количеству ненулевых коэффициентов в $G(x)$. С учетом этого свойства отклонение вероятности $P(B_i = 1)$ от 0.5 для данного случая, где B_i – i-й коэффициент полинома $B(x)$, составит

$$\tau_2 = \tau_1. \quad (10)$$

Обратимся к выражениям (6) и (7). При мультипликативном дескремблировании мультипликативно скремблированного сигнала согласно (6) на выходе дескремблера сформируется информационный сигнал. При этом отклонение вероятности $P(V_i = 1)$ от 0.5, где V_i – i-й коэффициент полинома $V(x)$, составит

$$\tau_3 = \tau. \quad (11)$$

При дескремблировании с использованием полинома $G^{2^m}(x)$ на выходе дескремблера будет последовательность, описываемая (7), для которой отклонение вероятности $P(F_i = 1)$ от 0.5, где F_i – i-й коэффициент полинома $F(x)$, определится как

$$\tau_4 = \left|0.5 - P(F_i = 1)\right| = (2\tau)^r / 2, \quad (12)$$

где r – количество ненулевых коэффициентов в полиноме $G^{2^m-1}(x)$.

Для принятия решения о виде скремблирования необходимо сравнить (9), (10) и (11), (12). Если сигнал был скремблирован аддитивно, то в результате дескремблирования с использованием полиномов $G(x)$ и $G^{2^m}(x)$ отклонения вероятности будут одинаковыми.

Если же сигнал был скремблирован мультипликативно, то в результате дескремблирования с использованием полиномов $G(x)$ и $G^{2^m}(x)$ отклонения вероятности будут равны τ_3 и τ_4 соответственно, причем $\tau_3 > \tau_4$.

Таким образом, алгоритм идентификации включает следующие операции:

– мультипликативное дескремблирование сигнала с использованием полиномов $G(x)$ и $G^{2^m}(x)$;

– оценки отклонений вероятности появления ненулевого элемента $\hat{\tau}_a$ и $\hat{\tau}_b$ на выходе соответствующих дескремблеров;

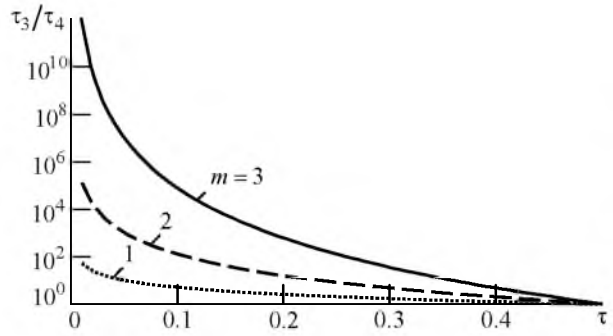

Рис. 3

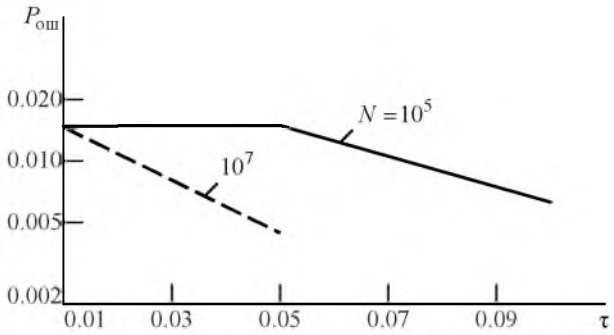

Рис. 4

– различение двух гипотез о виде скремблера по результатам сравнения полученных оценок.

Анализ результатов моделирования. Непосредственное сравнение оценок отклонений вероятности ненулевого элемента в дескремблированном сигнале $\hat{\tau}_a$ и $\hat{\tau}_b$ является некорректным. Это связано с тем, что полученный набор оценок имеет некоторый разброс значений, зависящий от объема анализируемых данных. Оптимальное правило различения двух гипотез можно сформулировать только при наличии информации о значении τ. В общем случае такой информации нет, что приводит к необходимости использования эмпирически выбранного порога различения.

Определим, насколько различаются оценки $\hat{\tau}_a$ и $\hat{\tau}_b$ при наихудших для идентификации условиях. Одним из таких условий являются экстремальные значения величины τ. В реальных системах связи значение данного параметра зачастую не меньше 0.01 и не превышает 0.4 [1]. На рис. 3 приведено семейство графиков зависимости отношения τ_3/τ_4 от величины τ для разных значений параметра m.

Из рис. 3 видно, что при $\tau = 0.01$ и $m = 1$ минимальное отношение оценок равно 50. При бóльших значениях параметра m эта разница возрастает на несколько порядков. При $\tau = 0.04$ оценки будут отличаться приблизительно в 1.25 раза при $m = 1$ и в 4.7 раза при $m = 3$. На основании этого анализа для работы алгоритма выбрано значение $m = 3$, а в качестве порога принятия решения в пользу мультипликативного вида скремблирования – соотношение $\hat{\tau}_a/\hat{\tau}_b \geq 2$.

На рис. 4 приведены результаты моделирования работы алгоритма (проводилось 100 000 экспериментов) в виде зависимости вероятности ошибки алгоритма $P_{\text{ош}}(\tau)$ для разных значений длины анализируемого сигнала.

При $\tau > 0.1$ ни одной ошибки за все время моделирования не произошло. Наличие ошибок при малых значениях τ обусловлено большой дисперсией оценок $\hat{\tau}_a$ и $\hat{\tau}_b$. При этом с увеличением объема анализируемого сигнала эта дисперсия падает, что приводит к уменьшению вероятности ошибки алгоритма.

На основании приведенных в настоящей статье данных можно утверждать, что разработанный алгоритм может быть использован для определения вида скремблера в автоматизированных системах радиомониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. Cluzeau M. Reconstruction of a Linear Scrambler // IEEE Trans. on Computers. 2007. Vol. 56, № 8. P. 1283–1291.

2. Canteaut A., Filiol E. Ciphertext only Reconstruction of Stream Ciphers Based on Combination Generators. Berlin: Springer, 2001. 16 p.

3. Johansson T., Jönsson F. Fast Correlation Attacks through Reconstruction of Linear Polynomials // Advances in Cryptology – CRYPTO 2000. 20th Ann. Int. Cryptology Conf. Santa Barbara, Aug. 20–24, 2000. Berlin: Springer, 2000. P. 300–315. (Lecture Notes in Computer Science 1807).

4. Canteaut A., Trabbia M. Improved Fast Correlation Attacks using Parity-Check Equations of Weight 4 And 5. // Advances in Cryptology – EUROCRYPT 2000, Int. conf. on the Theory and Applications of Cryptographic Techniques. Bruges, Belgium, May 14–16 2000 / Ed. by B. Preneel. Berlin: Springer, 2000. P. 579–594. (Lecture Notes in Computer Science 1880).

5. Скляр Б. Цифровая Связь. Теоретические основы и практическое применение: пер. с англ. 2-е изд. М.: Издательский дом "Вильямс", 2003. 1104 с.

6. Лидл Р., Нидеррайтер Г. Конечные поля: в 2 т. Т. 2 / пер. с англ. М.: Мир, 1988. 822 с.

Статья поступила в редакцию 26 октября 2017 г.

Для цитирования: Кривоногов А. С., Кривоногова Е. О. Алгоритм идентификации вида скремблирования бинарных данных // Изв. вузов России. Радиоэлектроника. 2017. № 6. С. 10–14.

Кривоногов Александр Сергеевич – магистр техники и технологий по направлению "Радиотехника" (2010), ассистент кафедры теоретических основ радиотехники Санкт-Петербургского государственного электротехнического университета "ЛЭТИ" им. В. И. Ульянова (Ленина), инженер Научно-исследовательского института радиотехники и телекоммуникаций указанного университета. Автор трех научных публикаций. Сфера научных интересов – цифровая связь.
E-mail: askr87@mail.ru

Кривоногова Екатерина Олеговна – магистр по направлению "Радиотехника" (2016), научный сотрудник АО "Научно-инженерный центр электротехнического университета" (Санкт-Петербург). Сфера научных интересов – цифровая связь.
E-mail: askr87@mail.ru

A. S. Krivonogov
Saint Petersburg Electrotechnical University "LETI"
E. O. Krivonogova
JSC "Research and Engineering Center of Electrotechnical University" (Saint Petersburg)

Linear Scrambler Identification

Abstract. *The article describes algorithm that allows determining scrambler type based on the signal from its output. The task of this kind is relevant for radio monitoring systems and when creating cognitive systems for digital signal receiving and processing. The identification algorithm determines the form of the scrambler both multiplicative and additive. There are no published papers providing algorithm for automatic determination of scrambler type. This article is intended to partly fill the gap. It provides a formal statement of the problem, an identification algorithm and simulation results.*

Key words: Scrambler, Identification, Radiomonitoring, Pseudorandom Sequence

REFERENCES

1. Cluzeau M. Reconstruction of a Linear Scrambler. IEEE Trans. on Computers. 2007, vol. 56, no. 8, pp. 1283–1291.

2. Canteaut A., Filiol E. Ciphertext only Reconstruction of Stream Ciphers Based on Combination Generators. Berlin, Springer, 2001, 16 p.

3. Johansson T., Jönsson F. Fast Correlation Attacks through Reconstruction of Linear Polynomials. Advances in Cryptology – CRYPTO 2000. 20th Ann. Int. Cryptology Conf. Santa Barbara, August 20–24, 2000. Berlin, Springer, 2000, pp. 300–315. (Lecture Notes in Computer Science 1807).

4. Canteaut A., Trabbia M. Improved Fast Correlation Attacks using Parity-Check Equations of Weight 4 And 5. Advances in Cryptology – EUROCRYPT 2000, Int. conf. on the Theory and Applications of Cryptographic Techniques. Bruges, Belgium, May 14–16 2000. Ed. by B. Preneel. Berlin, Springer, 2000, pp. 579–594. (Lecture Notes in Computer Science 1880).

5. Sklar B. Digital Communications. Fundamentals and Applicstions. 2nd ed. 2001, Upper Saddle River, Pren-tice Hall PTR, 2001, 1079 p.

6. Lidl R., Niederreiter H. Finite Fields. Cambridge University Press, 1985, 822 p.

Received October, 26, 2017

For citation: Krivonogov A. S., Krivonogova E. O. Linear Scrambler Identification. *Izvestiya Vysshikh Uchebnykh Zavedenii Rossii. Radioelektronika* [Journal of the Russian Universities. Radioelectronics]. 2017, no. 6, pp. 10–14. (In Russian)

Aleksandr S. Krivonogov – Master's Degree in Radio Engineering (2010), Assistant Professor of the Department of Theoretical Bases of Radio Engineering of Saint Petersburg Electrotecnical University "LETI". The author of 3 scientific publications. Area of expertise: digital communication.
E-mail: askr87@mail.ru

Ekaterina O. Krivonogova – Master's Degree in Radio Engineering (2016 JSC Research and Engineering Center of Saint Petersburg Electrotechnical University "LETI". Area of expertise: digital communication.
E-mail: askr87@mail.ru