УДК 681.324.067

А.А. Торба

Харьковский национальный университет радиоэлектроники, Харьков

МЕТОДЫ СТАТИСТИЧЕСКОЙ ОБРАБОТКИ СЛУЧАЙНЫХ СИГНАЛОВ

Теоретические исследования скрытности криптографических систем указывают на необходимость формирования ключевых данных с разностью вероятностей случайных битов не более $\Delta P = 10^{-6}$, поэтому рассматриваются методы статистической обработки случайных сигналов в аппаратных генераторах случайных последовательностей на основе физических датчиков шума с целью уменьшения разности вероятностей формируемых случайных битов. Применение метода объединения случайных независимых потоков на отводах сдвигающего регистра позволяет уменьшить разность вероятностей формируемых случайных битовых последовательностей до значений $\Delta P < 10^{-10}$.

Ключевые слова: *физический датчик шума, случайный поток, статистическая обработка.*

Постановка проблемы

Известные методы генерации случайных последовательностей на основе физических датчиков неопределенности (датчиков шума) включают преобразование аналоговых случайных импульсных сигналов в логические уровни и последующие алгоритмы обработки цифровых случайных сигналов с целью увеличения скорости формирования и улучшения статистических параметров случайных последовательностей.

Применение детерминированных алгоритмов обработки случайных сигналов, введение детерминированных сигналов синхронизации в случайный поток приводят к нежелательным эффектам типа «метастабильные состояния» в логических интегральных схемах и, как следствие, к непредсказуемым состояниям в моменты совпадения фронтов случайных и детерминированных сигналов при формировании выходных случайных логических битов.

Экспериментально установлено, что в аппаратных генераторах случайных последовательностей (АГСП) на основе физических датчиков шума указанные эффекты приводят к увеличению разности вероятностей ΔP формируемых случайных битовых последовательностей до величины

$$\Delta P = P(1) - P(0) = 0{,}01 \div 0{,}001.$$

Теоретические исследования скрытности криптографических систем указывают на необходимость формирования ключевых данных с разностью вероятностей случайных битов не более

$$\Delta P = 10^{-6}.$$

Поэтому целью проведенных теоретических и экспериментальных исследований являлась разработка методов статистической обработки случайных сигналов, которые позволяют уменьшить разность вероятностей формируемых случайных битовых последовательностей.

Методы объединения статистически независимых случайных потоков

В патенте [1] предложен метод обработки случайных сигналов для повышения быстродействия АГСП.

Случайные импульсные сигналы с выхода физического источника шума NS компаратором напряжения на основе триггера Шмита TS преобразуются в последовательность случайных логических сигналов с частотой Fш. Для выравнивания вероятностей случайных логических сигналов используется счетный триггер Т.

Последовательность случайных битовых сигналов на выходе счетного триггера может рассматриваться как поток, у которого между битами, разнесенными во времени на значительные расстояния, отсутствуют статистические связи.

Было предложено сдвигать во времени случайные биты многоразрядным сдвигающим регистром RG (рис. 1).

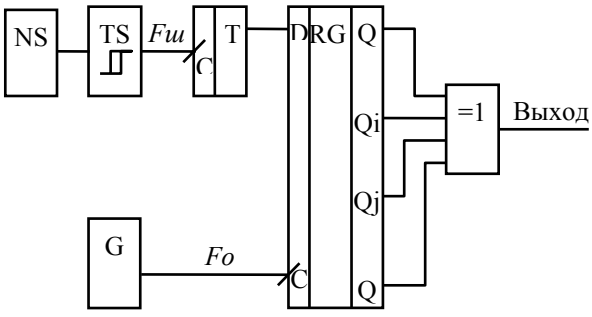

Рис. 1. Объединение потоков случайных независимых сигналов

Объединение элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» разнесенных во времени статистически независимых случайных битов от одного датчика шума можно рассматривать, как объединение нескольких статистически независимых случайных потоков.

Сигнал на выходе элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» описывается выражением:

$$L(t) = s(t) \oplus s\left(t + n_i \frac{1}{Fo}\right) \oplus s\left(t + n_i \frac{1}{Fo} + n_j \frac{1}{Fo}\right) \oplus .., \quad (1)$$

где $n_i \frac{1}{Fo}$, $n_j \frac{1}{Fo}$ – временные задержки распространения сигналов между отводами регистра Q0, Qi и Qi, Qj .

Количество разрядов между отводами *n* сдвигающего регистра определяется по формуле [2]:

$$n \geq m_{гр} \bullet Fo / Fш, \quad (2)$$

где $m_{гр} = 7 \div 9$ – граничное значение безразмерного параметра m, при котором отсутствуют корреляционные связи между соседними битами.

С учетом соотношения (2) перепишем соотношение (1):

$$L(t) = s(t) \oplus s\left(t + \frac{m_{гр}}{Fш}\right) \oplus s\left(t + \frac{m_{гр}}{Fш} + \frac{m_{гр}}{Fш}\right) \oplus .., \quad (3)$$

т.е. временные задержки сигналов между отводами сдвигающего регистра определяются частотой шума Fш источника неопределенности и граничным значением безразмерного параметра $m_{гр}$, соответствующим свойству независимости случайных сигналов.

В результате экспериментов было подтверждено, что объединение элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» независимых потоков случайных сигналов позволяет не только увеличить скорость формирования пропорционально количеству объединяемых потоков, но и улучшает такой важный статистический параметр, как разность вероятностей генерируемых случайных битов

$$\Delta = P(0) - P(1).$$

Для сдвигающего регистра с двумя отводами разность вероятностей случайных битов ΔP на выходе двухвходового элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» равна [3]:

$$\Delta = \delta^2, \quad (4)$$

где δ – разность вероятностей случайных битов на выходах сдвигающего регистра (или на входах элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ»).

Поэтому такой метод назван «Дельта-квадрат» [3].

Для сдвигающего регистра с тремя отводами обозначим вероятность единичного бита на отводах регистра:

$$P(1) = p.$$

Вероятность нулевого бита на отводах регистра обозначим:

$$P(0) = q = 1 - p.$$

Разность вероятностей:

$$p - q = \delta.$$

Поэтому:

$$P(0) = q = p + \delta.$$

Запишем в табл. 1 для регистра с тремя отводами (и трехвходового элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ») все вероятности появления комбинации случайных битов на отводах регистра.

Таблица 1

Вероятности появления комбинаций битов

Q0	Qi	Qj	Вероятности
0	0	0	(p + δ) • (p + δ) • (p + δ)
0	0	1	(p + δ) •(p + δ) • p
0	1	0	(p + δ) • p • (p + δ)
0	1	1	(p + δ) • p • p
1	0	0	p • (p + δ) • (p + δ)
1	0	1	p • (p + δ) • p
1	1	0	p • p • (p + δ)
1	1	1	p • p • p

На выходе элемента «ИСКЛЮЧАЮШЕЕ ИЛИ» формируется логический нуль при комбинациях, соответствующих четному количеству единичных битов на отводах регистра (нулевая, третья, пятая и шестая строки табл. 1). Поэтому вероятность «нулевого» бита на выходе трехвходового элемента «ИСКЛЮЧАЮШЕЕ ИЛИ» равна:

$$P'(0) = (p+\delta)^3 + p^2 \bullet (p+\delta) + p^2 \bullet (p+\delta) + p^2 \bullet (p+\delta). \quad (5)$$

Нечетному количеству единичных битов на отводах сдвигающего регистра соответствует логическая единица на выходе элемента «ИСКЛЮЧАЮШЕЕ ИЛИ» (первая, вторая, четвертая и седьмая строки табл. 1).

Поэтому вероятность «единичного» бита на выходе трехвходового элемента «ИСКЛЮЧАЮШЕЕ ИЛИ» равна:

$$P'(1) = p \bullet (p + \delta)^2 + p \bullet (p + \delta)^2 + p \bullet (p + \delta)^2 + p^3. \quad (6)$$

Разность вероятностей на выходе трехвходового элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» равна:

$$\Delta = P'(0) - P'(1) =$$

$$(p + \delta)^3 + 3 \bullet p^2 \bullet (p + \delta) - 3 \bullet p \bullet (p + \delta)^2 - p^3 = \delta^3. \quad (7)$$

Четырехвходовой логический элемент «ИСКЛЮЧАЮШЕЕ ИЛИ» для объединения независимых случайных потоков на рис. 1 можно преобразовать к виду на рис. 2.

В этой схеме на выходах логических элементов «ИСКЛЮЧАЮЩЕЕ ИЛИ» ЛЭ1 ЛЭ2 разность вероятностей уменьшается в соответствии с алгоритмом «Дельта квадрат»: $\Delta = \delta^2$.

После объединения выходных случайных сигналов элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» ЛЭ3 разность вероятностей еще уменьшается до значения

$$\Delta = (\delta^2)^2 = \delta^4. \quad (8)$$

В общем случае можно утверждать, что разность вероятностей на выходе элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» равна:

$$\Delta = \delta^n, \quad (9)$$

где n – количество объединяемых независимых случайных потоков или количество отводов сдвигающего регистра (или количество входов элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ»).

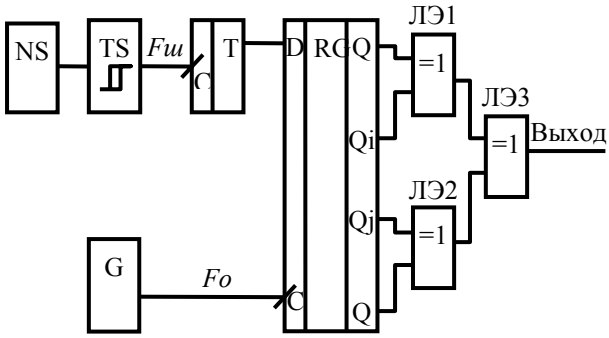

Рис. 2. Объединение случайных потоков четырехвходовым элементом «ИСКЛЮЧАЮШЕЕ ИЛИ»

В аппаратных генераторах случайных последовательностей «Гряда 3» и «Электронный ключ» [4] применены методы обработки случайных сигналов с объединением не менее 6-ти случайных потоков элементами «ИСКЛЮЧАЮЩЕЕ ИЛИ» для увеличения скорости формирования случайных последовательностей. Эти методы позволяют также уменьшить разность вероятностей формируемых случайных битовых последовательностей:

$$\Delta P < 10^{-12}.$$

Однако экспериментально проверить такой результат практически невозможно, т.к. известные методы монобитного тестирования [5] случайных последовательностей с точностью:

$$\Delta P = 10^{-n}$$

требуют формирования случайной выборки длиной не менее $s = 10^{2n}$ бит.

При скорости генерации случайных последовательностей V =10 ÷ 16 Мбит/с рассчитано время формирования случайных выборок длинной $s = 10^{10} \div 10^{20}$ бит [5]. Сделан вывод о том, что измерение разности вероятностей случайных битовых последовательностей с точностью $\Delta P = 10^{-8}$ или менее (при $s \geq 10^{16}$) не имеет практического смысла, так как занимает время более 30 лет.

Выводы

Применение метода объединения случайных независимых потоков на отводах сдвигающего регистра позволяет уменьшить разность вероятностей формируемых случайных битовых последовательностей до значений $\Delta P < 10^{-10}$.

Такой результат значительно лучше необходимой разности вероятностей случайных битов ($\Delta P = 10^{-6}$) для формирования ключевых данных с теоретически обоснованным уровнем скрытности.

Список литературы

1. Патент Украины № 68912 А, Бюл. № 8 от 16.08.2004.

2. Торба А.А. Принципы построения аппаратных генераторов случайных последовательностей / А.А. Торба, В.А. Бобух, А.А. Торба // КИП и АВТОМАТИКА. Массовый ежемесячный научно-производственный журнал. – 2005. – № 8. – С. 10-15.

3. Торба А.А. Генерация равновероятных случайных последовательностей на основе физических датчиков / А.А. Торба, С.Г. Елаков, А.З. Степченко // Радиотехника. Всеукр. межвед. науч.-техн. сб., 2001. – Вып. 119. – С. 108-113.

4. Торба А.А. Аппаратные генераторы квазислучайных последовательностей / А.А. Торба, В.А. Бобух, А.А. Торба // Радиотехника. Всеукр. межвед. науч.-техн. сб., 2008. – Вып. 152. – С. 144-149.

5. Торба А.А. Критерии качества генераторов квазислучайных последовательностей / А.А. Торба, Е.Г. Качко, А.А. Торба // Прикладная радиоэлектроника. – 2007. – Т. 6, № 2. – С. 310-314.

Поступила в редколлегию 20.02.2009

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет воздушных сил имени Ивана Кожедуба, Харьков.

МЕТОДИ СТАТИСТИЧНОЇ ОБРОБКИ ВИПАДКОВИХ СИГНАЛІВ

А.А. Торба

Теоретичні дослідження скритності криптографічних систем указують на необхідність формування ключових даних з різницею імовірностей випадкових бітів не більш: $\Delta P = 10^{-6}$, тому розглядаються методи статистичної обробки випадкових сигналів в апаратних генераторах випадкових послідовностей на основі фізичних датчиків шуму з метою зменшення різниці імовірностей формованих випадкових бітів. Застосування методу об'єднання випадкових незалежних потоків на відводах регістра, що зрушує, дозволяє зменшити різницю імовірностей формованих випадкових бітових послідовностей до значень $\Delta P < 10^{-10}$.

Ключові слова: *фізичний датчик шуму, випадковий потік, статистична обробка.*

METHODS OF THE STATISTICAL PROCESSING RANDOM SIGNAL

A.A. Torba

The basic researches to secretiveness of the cryptographic systems point to need forming key with difference of probability random bits less: $\Delta P = 10^{-6}$, so methods of the statistical processing random signal are considered in hardware generator of the random sequences on base physical sensor noise for the reason reduction of the differences of probability formed random bits. Using the method of the association random independent threads on tap shifting register allows to reduce the difference of probability formed random bit sequences till values $\Delta P < 10^{-10}$.

Keywords: *physical sensor of noise, casual stream, statistical treatment.*