

2. Липницкий В. А., Конопелько В. К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.

ОСОБЕННОСТИ КОРРЕКЦИИ ОШИБОК КОДАМИ С МАЛЫМ КОНСТРУКТИВНЫМ РАССТОЯНИЕМ

В.А. ЛИПНИЦКИЙ, А.О. ОЛЕКСЮК

В современных инфокоммуникационных системах защита информации стоит на одном из первых мест. Проблему составляют не только конфиденциальность передаваемой информации, но и защита ее от помех. Реальные каналы связи неизбежно содержат различного рода шумы и помехи, что сказывается на точности и достоверности передаваемой информации.

Современные ИКС, как правило, снабжены устройствами, применяющими помехоустойчивые коды. Экспоненциальный рост информационных потоков предъявляет все более жесткие требования к применяемым помехоустойчивым кодам, в сторону увеличения кратности корректирующих и повышения скорости работы декодирующих устройств.

Массовые применения в высокоскоростных системах связи приобрели БЧХ-коды (сотовая связь, диспетчерские службы и др.), как правило, примитивные [1]. Однако декодеры на их основе слабо адаптируются к повышению кратности корректируемых ошибок [1, 2].

Проведенные исследования показали, что существуют, и в достаточно большом количестве, не примитивные БЧХ-коды, имеющие невысокое конструктивное расстояние, но существенно большее реальное минимальное расстояние.

в докладе обсуждаются алгоритмы быстрого декодирования многократных ошибок не примитивными БЧХ-кодами с конструктивным расстоянием 5.

Литература

1. MacWilliams F.J., Sloane N.J.A. The Theory of Error-Correcting Codes. North-Holland Mathematical Library. 1977. Vol.16. 762 p.
2. Липницкий В. А., Конопелько В. К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.

АНАЛИЗ АНАЛОГО-ЦИФРОВОЙ СИСТЕМЫ ФАЗОВОЙ СИНХРОНИЗАЦИИ

С.А. ГАНКЕВИЧ

Анализируется цифровая система фазовой синхронизации (ЦСФС) с астатизмом второго порядка, с управляемым генератором, выполненным в виде аналоговой системы фазовой автоподстройки частоты (ФАПЧ), включенной в основной контур ЦСФС. Эталонный сигнал для ФАПЧ формируется высокостабильным задающим генератором (ЗГ). Формирование эталонного и опорного сигналов в управляемом генераторе производится методом нониуса, что позволяет уменьшить дискрет подстройки фазы без увеличения частот ЗГ и генератора, управляемого напряжением (ГУН), и за счет этого повысить точность синхронизации. Коррекция фазы опорного сигнала, формируемого ГУН, производится по сигналу ЗГ и сигналу фазовой ошибки в основном контуре. Фильтрующие свойства ЦСФС обеспечиваются основным узкополосным контуром

слежения. В качестве ФНЧ используются изотропное звено в основном контуре и пропорционально-интегрирующее звено в контуре управляемого генератора.

Приводятся результаты анализа математической модели по основным показателям качества и результаты моделирования. Определены требования к параметрам контуров слежения с целью обеспечения заданных показателей устойчивости, точности и быстродействия. Обеспечивая более высокие показатели точности по сравнению с системой с астатизмом первого порядка [1], анализируемая система более критична к выбору ФНЧ, удовлетворяющему требованиям устойчивости. В частности, ФНЧ в виде апериодического звена в контуре управляемого генератора не удовлетворяет этим требованиям.

Литература

1. Ганкевич С.А. Технические средства защиты информации: Тезисы докладов IX Белорусско-российской научно технической конференции, 28–29 июня 2011 г., Минск. Минск: БГУИР, 2011. С. 26.

МЕТОДИКА ПОЛУЧЕНИЯ ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ

К.В. ГУБЧИК, А.А. ИВАНЮК

Последовательности случайных чисел (СЧ) являются необходимым инструментом решения многих задач защиты информации (протоколы аутентификации, генерация сессионных ключей, защита авторских прав и др.). В работе [1] был предложен метод реализации физически неклоняемой функции (ФНФ) на базе статического ОЗУ (СОЗУ), который основан на анализе начального состояния памяти при включении питающего напряжения. Недостаток разработанного метода: большинство ячеек СОЗУ принимают одно из состояний чаще, чем другое, поэтому нарушается требование непредсказуемости данного физического отпечатка [1]. Чтобы обойти эту проблему, предлагается методика использования сигнатуры памяти вместо физического отпечатка памяти. При этом, зная сигнатуру, практически невозможно предсказать исходный физический отпечаток памяти. Это происходит за счет сжатия с потерями исходной ЧП при помощи алгоритма формирования сигнатур (LFSR-анализатор, CRC-анализатор, адаптивный сигнатурный анализатор [2]). Полученная сигнатура может использоваться в качестве начального состояния генератора СЧ, когда не требуется высокой скорости генерации СЧ. Создание ГИСЧ (генератора истинно случайных чисел) является актуальной проблемой в областях защиты информации, т. к. в них требуются истинно случайные и невоспроизводимые числа, при этом сами генераторы должны обладать свойством неклоняемости как для различных технологий, так и для идентичных устройств, выполненных по единой технологии. В качестве источника случайности предлагается использовать сигнатуру состояния памяти, что позволит обеспечить высокие требования к качеству ЧП, формируемых при помощи ГИСЧ.

Литература

1. Holcomb D.E., Burlison W.P., Fu K. IEEE Transactions on Computers, September 2009. P. 1198–1210.
2. Иванюк А.А., Петроненко Д.С. Доклады БГУИР. 2004. № 4. С. 84–92.