УДК 681.325

Семеренко В.П.
ВНТУ
vpsemerenko@mail.ru

О ВЗАИМОСВЯЗИ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ, КРИПТОГРАФИИ И ТЕХНИЧЕСКОЙ ДИАГНОСТИКИ

Аннотация. Показано, что используемый в помехоустойчивом кодировании код CRC, хеш-функция на основе циклического избыточного контроля и сигнатура в технической диагностике – это разные наименования результата одной и той же математической операции. Рассмотрены способы использования теоретических и практических результатов одних дисциплин для других.

Основной задачей помехоустойчивого кодирования, криптографии и технической диагностики является проверка ошибок в используемых данных. Каждая из указанных дисциплин имеет свою специфику, обусловленную причиной возникающих ошибок: либо непреднамеренными ошибками в каналах передачи данных, либо преднамеренно вводимыми искажениями, либо же неисправностями радиоэлектронной аппаратуры [1].

Однако имеется много сфер приложения, где эти дисциплины взаимно дополняют друг друга, используя похожие теоретические основы и схемную реализацию. Очень интересной в этом плане является задача проверки целостности данных, для решения которой используется идентичный математический аппарат.

В различных системах передачи данных широко используется циклический избыточный контроль (Cyclic Redundancy Check – CRC) [2]. Суть метода состоит в проверке отсутствия ошибок в информационной последовательности I произвольной длины h с помощью r-разрядной ($r << h$) контрольной суммы Σ, получаемой путем деления последовательности I на некоторый заданный примитивный многочлен $g(x)$ над полем Галуа $GF(2)$.

Такая контрольная сумма Σ отвечает всем основных требованиям, которые предъявляются к хеш-функциям в криптографии: односторонность, стойкость к коллизиям, одинаковая длина для всех последовательностей I.

Наконец, появившийся в 70-х годах прошлого века сигнатурный анализ вычисляет сигнатуры путем деления тестовой последовательности сигналов на заданный примитивный многочлен $g(x)$ [3].

Таким образом, рассмотренные выше CRC, хеш-функция и сигнатура – это разные наименования результата одной и той же математической операции.

Однако получаемый практический результат не всегда является удовлетворительным с позиций каждой из дисциплин.

Например, CRC позволяет лишь обнаружить независимые ошибки нечетной кратности или пакеты ошибок длины не более r. Для обеспечения возможности исправления ошибок следует ввести некоторые ограничения. Если для некоторого положительного числа $m \geq 4$ длина n последовательности I не превышает $2^m - 1$, длина контрольной суммы Σ равна $m+1$, а многочлен $g(x)$ имеет вид

$$g(x) = (1+x)\, p(x),$$

где $p(x)$ – примитивный многочлен степени m,

тогда в последовательности I можно исправить все одиночные ошибки и все смежные пакеты ошибок длины 2. В итоге мы получаем $(2^m - 1, 2^m - m - 2)$-код CRC (Cyclic Redundancy Code), который более правильно именовать, как циклический код Абрамсона.

В результате дальнейшего усложнения многочлена $g(x)$ получаются код Файра, код БЧХ и другие виды циклических кодов с улучшенными корректирующими свойствами.

Рассмотренный ранее способ формирования хеш-функции является очень уязвимым с позиций защиты информации. Для анализа криптостойкости хеш-функции очень удобным

является используемый в помехоустойчивом кодировании математический аппарат линейных последовательностных схем (ЛПС) [4]. В этом случае легко доказать, что надежной защитой потоковых хеш-функций от криптоатак является добавление к исходному сообщению двух r -разрядных секретных ключевых последовательностей символов [5].

Наконец, классический сигнатурный анализ также не совсем оптимален для контроля современных сложных цифровых устройств, поскольку гарантированно обнаруживает лишь одиночные ошибки и некоторые виды других. Используя аналогию между передачей данных в системах связи и преобразованием входных данных в цифровом автомате можно с успехом использовать различные виды корректирующих кодов в технической диагностике.

Выбор корректирующего кода должен осуществляться с учетом конкретных особенностей диагностируемого устройства. Например, в запоминающих устройствах из-за отсутствия эффекта размножения неисправностей возможно использование кодов с исправлением независимых ошибок невысокой кратности. Для уменьшения времени контроля целесообразно использовать коды с мажоритарным декодированием.

Наиболее сложными для задач диагностирования являются цифровые автоматы. Для них ошибки на контролируемых выходах являются зависимыми, кратность ошибки определяется топологией функциональной схемы. В таких случаях необходимо подавать тесты на входы устройства в такой последовательности, чтобы влияние отдельных элементов устройства было по возможности сосредоточено в пределах одного временного интервала. Тогда неисправности отдельных элементов будут представляться в виде пакетов ошибок в выходном векторе, следовательно, для диагностики отказавших элементов можно использовать кодов Файра и Рида-Соломона. Полезным будет также и многоканальный сигнатурный анализ с одновременным контролем по множеству выходов, теоретической основой которого является многоканальная ЛПС.

Перспективным направлением в современной схемотехнике является надежностный синтез цифровых автоматов с введением информационной избыточности на основе помехоустойчивого кодирования.

Таким образом, имеются разделы, в которых помехоустойчивое кодирование, защита информации и техническая диагностика полностью совпадают, что позволяет использовать как теоретические достижения, так и практические результаты одних дисциплин для других. Такой взаимообмен возможен и полезен даже на тех этапах, когда учитываются специфика каждой из дисциплин.

Список литературы:

1. Семеренко В.П. Интегрированная защита информации: криптография плюс помехоустойчивое кодирование / В.П. Семеренко. // Захист інформації — 2011. — №3. — С. 44-52.

2. Вернер М. Основы кодирования. Учебник для вузов: / М. Вернер. — М : Техносфера, 2004. — 286 с.

3. Ярмолик В.Н. Контроль и диагностика цифровых узлов ЭВМ: / В.Н. Ярмолик. — Мн. : Наука и техника, 1988. — 240 с.

4. Гилл А. Линейные последовательностные машины: / А. Гилл. — М.: Наука, 1974. — 288 с.

5. Семеренко В. П. Разработка хэш-функции на основе поточного шифрования / В.П. Семеренко, П.В. Ширшова. // Защита информации — Сборник научных трудов НАУ — Киев, НАУ, 2008. — Вып.15. — С.163-166.