ЦИФРОВЫЕ ГЕНЕРАТОРЫ ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ

Губчик К.В.
Кафедра вычислительных методов и программирования
Научный руководитель: Иванюк А.А., д.т.н., доцент, зав.каф. ВМиП
e-mail: gubchikkv@gmail.com

***Аннотация* — Последовательности случайных чисел (СЧ) являются необходимым инструментом решения многих задач криптографии, имитационного моделирования, защиты авторских прав, осуществления случайного тестирования цифровых устройств и др. В работе рассматривается задача получения последовательностей истинно СЧ.**

Ключевые слова: генераторы истинно случайных чисел, физически неклонируемая функция (ФНФ)

В зависимости от способа формирования числовой последовательности (ЧП) существующие генераторы СЧ можно разделить на два основных типа: генераторы псевдослучайных чисел (ГПСЧ) и генераторы истинно случайных чисел (ГИСЧ). Преимущества ГИСЧ: невоспроизводимость, уникальность и непредсказуемость [1,2]. ГИСЧ могут реализовываться в цифровых, аналоговых и аналогово-цифровых схемах. ГИСЧ, основанные на аналоговых схемах, требуют новой технологии производства, что повышает конечную стоимость продукта и время вывода продукта на рынок. ГИСЧ, основанные на цифровых схемах, лишены этих недостатков, что уменьшает стоимость и увеличивает область применения [3]. В качестве источника энтропии в ГИСЧ можно использовать ФНФ, которые основаны на использовании непредсказуемых, невоспроизводимых отклонений в физической структуре интегральной схемы при ее изготовлении [4]. Поэтому реализация одинаковых по функциональности ГИСЧ будет уникальной, неповторимой и неклонируемой, что и является преимуществом цифровых генераторов.

В работе [5] был предложен метод реализации ФНФ на базе статического ОЗУ (СОЗУ), который основан на анализе начального состояния памяти при включении питающего напряжения. В силу того, что часть ячеек СОЗУ принимает одно из двух состояний фиксировано, а часть ячеек "плавают" под воздействием шума, последовательность битов, считанных из памяти (физический отпечаток памяти) может использоваться в качестве источника СЧ. Недостаток разработанного метода: большинство ячеек СОЗУ принимают одно из состояний чаще, чем другое, поэтому нарушается требование абсолютной непредсказуемости данного физического отпечатка [5]. Физический отпечаток всей памяти нерационально использовать в качестве источника случайности за счет большого объема данных и малого количества энтропии. Чтобы обойти эту проблему, предлагается методика использования сигнатуры памяти вместо физического отпечатка памяти. При формировании сигнатуры происходит сжатие исходной ЧП, и как следствие уменьшается объем хранимой ЧП. Кроме того, в сформированной сигнатуре невозможно разделить стабильную и случайную части. Если известен один или несколько физических отпечатков, то с большой степенью вероятности можно предсказать следующий физический отпечаток. Сигнатуру в отличие от физического отпечатка практически невозможно предсказать. Это происходит за счет того, что становится невозможным определить, какие именно биты изначально являются случайными, а какие - относительно стабильными, а каждый бит сигнатуры формируется несколькими битами физического отпечатка памяти. Полученная сигнатура может использоваться в качестве начального состояния генератора СЧ, когда не требуется высокой скорости генерации СЧ.

Наиболее подходящей платформой для реализации ГИСЧ являются ПЛИС. ПЛИС выигрывают по сравнению с заказными СБИС, т. к. в специализированной схеме эксплуатационная гибкость достигается только за счет написания нового кода, а в ПЛИС есть возможность конфигурирования аппаратуры под конкретную задачу. Например, можно будет изменять интервал, в котором требуется генерировать СЧ, возможна реализация ГДСЧ, которая каждый раз при включении, будет задавать различный диапазон генерации СЧ и алгоритм формирования сигнатур. Для формирования сигнатур для ОЗУ можно использовать LFSR-анализатор, CRC-анализатор, адаптивный сигнатурный анализатор [6, 7]. Поэтому желательно спроектировать ГИСЧ реконфигурируемым и не требующим дополнительной аппаратуры.

В работе показано, что создание ГИСЧ является актуальной проблемой, т. к. существует много областей, где требуются истинно случайные и невоспроизводимые числа. В качестве источника случайности предложено использовать сигнатуру состояния памяти, что позволит обеспечить высокие требования к качеству ЧП, формируемых при помощи ГИСЧ.

[1] Ярмолик В. Н. Генерирование и применение псевдослучайных сигналов в системах испытаний и контроля – Наука и техника, Минск, 1986. – 200 с.

[2] Kohlbrenner P., Gaj K. An Embedded True Random Number Generator for FPGAs – 12th international symposium on Field programmable gate arrays, New York, 2004. – p. 71-78.

[3] Vasyltsov I., Hambardzumyan E., Kim Y.-S., Karpinskyy B. Fast Digital TRNG Based on Metastable Ring Oscillator – CHES '08, Berlin, 2008. – p. 164-180.

[4] Иванюк А. А. Применение конфигурируемых генераторов импульсов для идентификации ПЛИС – Информатика №4(32), Минск, октябрь-декабрь 2011. – с. 35-46.

[5] Holcomb D. E., Burleson W.P., Fu K. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers – IEEE, September 2009. – p. 1198-1210.