PINGUINO и персональный генератор энтропии

Касьяник В.В.

Брестский государственный технический университет, val.tut@gmail.com

Проблема получения качественных случайных числовых последовательностей в настоящее время решается созданием различных сложных генераторов псевдослучайных чисел, однако с ростом вычислительных мощностей, повышается вероятность взлома даже таких алгоритмов. Создание достаточно простого и дешевого персонального генератора высококачественных случайных последовательностей чисел на основе свободной платформы Pinguino позволит каждому получать случайные числа для защиты своей информации или проведения квантовых исследований. На первый взгляд проблема не так уж остра, однако уже сейчас ощущается недостаток качественных последовательностей, что вызывает их активную продажу и покупку. В данной работе предлагается создание технологии производства качественной энтропии и случайных последовательностей на основе свободного программного и аппаратного обеспечения.

В последнее время широкое развитие и различное применение получили так называемые Arduino–совместимые конструкторы электронных устройств. Это универсальные контроллеры, достаточно простые в использовании и разработке, но отлично подходящие для проектирования сложных электронных устройств, тесно взаимодействующих с окружающей физической средой. Ардуино-совместимые платформы, предназначенные для «physical computing» с открытым программным кодом и открытым аппаратным обеспечением позволяют пользователю соединить виртуальность персонального компьютера и окружающую реальность.

Ардуино-совместимых платформ на сегодняшний день огромное количество. Они варьируются по функциональности, производительности, типу используемого оборудования и т.д. Они находят применение в домашнем моддинге, подходят для встраивания в автомобиль, для проведения научных исследований. Нами был рассмотрен вариант применения одной из таких свободных платформ – Pinguino – для создания простого персонального генератора энтропии (источник энтропии).

Источники энтропии используются для накопления энтропии, с последующим получением из неё начального значения, необходимого генераторам случайных чисел (ГСЧ) для формирования абсолютно случайных чисел. Отличие от генератора псевдослучайных чисел (ГПСЧ) в том, что ГПСЧ использует единственное начальное значение, откуда и получается его псевдослучайность, а ГСЧ всегда формирует случайное число, имея в начале высококачественную случайную величину, предоставленную различными источниками энтропии.

Случайные числа имеют много применений в криптографии, в частности, для создания криптографических ключей, паролей. Например, на некоторых системах на платформе UNIX можно считать данные с устройства /dev/audio без помещённого у микрофона источника звука,

либо считывать лишь низкий уровень фонового шума. Такие данные по существу являются случайным шумом, хотя им не стоит доверять без некоторой проверки. Физические процессы являются одними из самых надежных для получения последовательностей случайных чисел, поэтому применение Ардуино-подобной платформы является наиболее простым и доступным для создания источника энтропии.

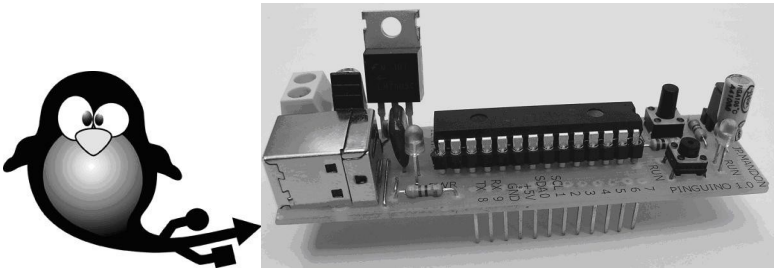

Рис. 1 – Логотип проекта и Pinguino-плата

Pinguino – это ардуино-подобная вычислительная платформа на основе микроконтроллера PIC, которая была созданна французским исследователем из лаборатории робототехники Жан-Пьером Мэндоном и группой HackingLab. Целью проекта являлось создание совместимой с ардуино вычислительной платформы, обладающей теми же свойствами кроссплатформенности, простоты, открытости кода и схематических решений. Однако большинство atmel-вариантов ардуино-платформ не имеют нативной поддержки USB- интерфейса, что затрудняет легкое подключение таких устройств к компьютеру и соответственно, не является легким в использовании. Используемый в Pinguino микроконтроллер PIC 2550 поддерживает USB-интерфейс и последовательный интерфейс на уровне чипа, что позволяет уменьшить размеры платы и кода для связи с компьютером.

Для получения самой физической энтропии с помощью Pinguino, к нему необходимо подключить датчик инфракрасного излучения (простейшая схема с излучателем и приемником) и акселерометр. Вибрации дадут возможность акселерометру накапливать случайную величину, причем более дешевый вариант датчика дает более качественный физический шум. Отражение инфракрасного излучения от объектов реального мира сильно зависит от физических свойств среды – оптической проводимости, отражающей поверхности, наличия других источников излучения, например ламп накаливания. Приемник должен обладать возможностью получения аналогового сигнала. Аналогичным образом можно применять достаточно простую схему высокоточного измерения температуры по формуле Найквиста [5].

В заключение стоит отметить, что на базе платформы Ардуино был создан необычный генератор энтропии на основе капилярного течения жикости [4]. Однако, предложенный в данной работе вариант отличается простотой и доступностью исходных деталей, малыми размерами платы

Pinguino, комбинированием различных датчиков для получения энтропии.

Со временем ценность качественных генераторов энтропии будет только расти, достаточно вспомнить известный афоризм Роберта Р. Кавью: «генерация случайных чисел слишком важна, чтобы оставлять её на волю случая».

Литература

1. Веб-сайт проекта Pinguino. Режим доступа: http://www.hackinglab.org/index.html, 9.01.2011
2. Блог проекта Pinguino. Режим доступа: http://jpmandon.blogspot.com/ , 9.01.2011
3. Группа рассылки на сайте Google. Режим доступа: http://groups.google.fr/group/pinguinocard , 9.01.2011
4. Генератор энтропии на базе Ардуино. Режим доступа: http://www.circuitlake.com/usb-hourglass-sand-timer.html, 9.01.2011
5. Высокоточное измерение температуры по формуле Найквиста. Режим доступа: http://www.shematic.net/page-17.html, 9.01.2011