УДК 004056

Собінов О.Г., Коломієць Д.О.
Кіровоградський національний технічнтй університет

Програмно-апаратний генератор псевдовипадкових чисел на основі мікроконтролерів

Світ все сильніше і сильніше обплутує мережею комунікацій. Список загроз безпеки передачі даних продовжує зростати. У нього постійно додаються нові способи злому, шахрайства, нові шкідливі програми і нові типи вірусів. У сьогоднішньому, перевантаженому комунікаціями, світі можливості для шахрайства або крадіжки часто реалізуються одним кліком мишки або одним дотиком сенсорного екрану портативного комп'ютера. Важлива персональна і конфіденційна інформація, розташована в мережі інтернет, щодня передається через бездротові з'єднання мільйонами людей по всьому світу. Крім того через бездротові з'єднання передається інформація від великої кількості датчиків телеметричних систем збору і обробки інформації, а також сигнали управління промисловими об'єктами та процесами і транспортними засобами.

Багато виробників ARM-процесорів додають в свої вироби спеціальні апаратні блоки - криптографічні прискорювачі, які працюють окремо від основного ARM-ядра. Таким чином, ядро ARM може практично не брати участь в криптографічних процесах, зберігаючи свої ресурси для виконання тих завдань, з якими воно справляється найкращим чином. До таких завдань можна віднести обслуговування обміну з периферійними пристроями, обробку даних, реалізацію бездротового обміну з іншими пристроями, що управляють і інші прикладні алгоритми.

Компанія STMicroelectronics, відповідно до світових тенденцій, додала в свої новітні мікроконтролери STM32F415/STM32F417 з 32-розрядних ядром ARM Cortex-M4F криптографічний прискорювач, перевірений на мікроконтролерах STM32F215/STM32F217 з ядром ARM Cortex-M3. Прискорювач дозволяє шифрувати дані за алгоритмами DES/TDES/AES, обчислювати хеш-функції SHA-1/MD5/HMAC і генерувати випадкові числа. Підвищення максимальної тактової частоти з 120 МГц (для STM32F2xx) до 168 МГц (для STM32F4xx) дозволило підвищити і продуктивність криптографічного прискорювача.

Було запропоновано будувати генератор псевдо випадкових чисел на базі математичного більярду. Ідея генератора псевдовипадкових чисел полягає в тому, що на площині m x n запускається під кутом «кулька» яка по закону - кут падіння дорівнює коту відбивання відбивається від чотирьох поверхонь. Такий псевдо генератор має особливість - через певний час траєкторія руху починає циклічно повторюватися. Для зміни циклічності повторення траєкторії введемо в систему додатковий елемент, який умовно назвемо «каструлею» і який має набагато більший радіус ніж у кульки, з деякою інерційною масою. При зустрічі з кулькою «каструля» починає повільно рухатися за напрямком вектора заданого кулькою при цьому і кулька змінює траєкторію руху. Таким чином ми отримаємо псевдо генератор в якому траєкторія жодним чином не буде повторюватися, і відповідно координати відбиття будуть створювати гарний псевдо генератор випадкових чисел.

На базі запропонованого алгоритму генерації псевдо випадкових чисел пропонується створити апаратно програмні модулі на базі мікроконтролерів. Пристрій повинен складатися за пари окремих мікроконтролерних модулів, які пов’язані між собою засобами мережі Кожна пара має програмно “вшиті” початкові дані однакові для кожної пари: початкові координати кульок (двох і більше); кути початкових нахилів руху кульок; координати «каструлі»; розмір поля mxH. Таким чином с точки зору математики таких пар можна створити нескінченну множину з зауваженням того, що розрахунки ведуться в дійсних числах маємо нескінченну множину пар таких пристроїв.

Особливістю даного генератора створення ключів є те, що після кожного включення псевдовипадковий ряд постійно буде повторюватися, тому для запобігання передачі даних побудованих на однаковому ключі використовуються початковий відкритий ключ побудований на засадах RTC. Ключ здійснює синхронізацію даних та виконує зміну початкових даних на задані «дельта. Для підвищення надійності в систему псевдо генератора вводяться додатково декілька кульок кожна з яких генерує програмно свій псевдо ряд випадкових чисел. Виходячи з часу синхронізації виконується перемикання за простим алгоритмом рядів.