УДК

ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Тимошевич К. С., студент гр. 253503, Котова К. А., студент гр. 253503, Кваченюк Я. Д., студент гр. 253502, Николайчик А. С., студент гр. 253502

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стройникова Е.Д. – старший преподаватель каф. информатики

Аннотация. В данной работе рассмотрены различные методы генерации случайных чисел (ГСЧ) на основе физически неклониуремых функций (ФНФ), такие как использование шума электромагнитных помех, оптических ФНФ, а также состояния памяти устройства. Для каждого метода были описаны основные принципы работы и процесс генерации случайных чисел (СЧ).

Ключевые слова. Генераторы случайных чисел, физически неклонируемые функции.

Генераторы случайных чисел (ГСЧ) являются одним из ключевых инструментов в области компьютерной науки и информатики. Они используются для моделирования случайных явлений в различных приложениях, таких как криптография, статистические вычисления, моделирование случайных процессов и т.д.

Одним из основных требований к ГСЧ является высокая степень случайности. Это означает, что любой потенциальный злоумышленник не должен иметь возможности предсказать следующее число в последовательности. Поэтому генераторы СЧ обычно основаны на алгоритмах, которые используют определенные математические функции для создания случайных чисел.

Однако существует риск того, что алгоритмы генерации СЧ могут быть подвержены атакам и взлому. Для повышения уровня безопасности генераторов случайных чисел (СЧ) могут использоваться физически неклонируемые функции (ФНФ), которые создают случайные значения на основе уникальных физических свойств устройства.

Генератор случайных чисел (ГСЧ) с использованием физически неклонируемых функций (ФНФ) – это метод генерации последовательности случайных чисел, который основывается на использовании уникальных физических свойств компонентов системы, таких как микрочипы, датчики, транзисторы и т.д.

Основная идея заключается в том, что каждый компонент имеет свои уникальные физические свойства, которые могут быть использованы для создания уникальных и непредсказуемых последовательностей чисел. Такие функции могут включать в себя случайные шумы, флуктуации напряжения, температуры, сопротивления, затухания и многое другое.

Физически неклонируемая функция (ФНФ) – это специальный вид функций, которые генерирует уникальный и непредсказуемый результат на основе физических характеристик конкретного компонента. Они должны удовлетворять следующим свойствам:

1. Структурная информация подобных систем может быть извлечена надежно и неоднократно путем проведения измерений для различных запросов и получения ответов.
2. Количество возможных запросов должно быть настолько велико, что значения всех соответствующих ответов не могут быть получены путем перебора всех возможных запросов за реальный временной промежуток.
3. Ввиду наличия в системе чрезмерно большого объёма структурной информации должно быть невозможным смоделировать, рассчитать или каким-либо другим математическим способом предсказать пару запрос-ответ, зная другую пару или некоторое множество таких пар.
4. Для физической системы с чрезвычайно большим объёмом структурной информации должно быть чрезвычайно сложным ее физическое воспроизведение или клонирование как аналогичной физической системы, описываемой идентичным множеством пар запрос-ответ.

Создание генератора случайных чисел с использованием оптических ФНФ

Среди окружающих нас материальных объектов сложно найти два абсолютно одинаковых предмета. Даже в серийном производстве каждый объект получается уникальным за счет погрешностей и случайностей. Эти особенности каждого отдельного объекта можно регистрировать и использовать как уникальный идентификатор, своеобразный «отпечаток пальца».

Наглядный пример — оптическая ФНФ. Возьмем расплавленное стекло, добавим в него пузырьки воздуха, остудим эту массу и разрежем на одинаковые бруски. Шанс получить два

абсолютно одинаковых бруска ничтожно мал, т.к. пузырьки воздуха внутри будут распределены неравномерно. Можно зафиксировать эти различия, отправляя на брусок пучок лазерного излучения (запрос) и получая на выходе уникальную интерференционную картину пучков излучения после преломления (ответ). В результате получится ФНФ, которая будет определять зависимость ответа от входного запроса.

Оптические ФНФ основаны на уникальных оптических свойствах материалов, которые обеспечивают высокую степень неравенства и непредсказуемости.

Оптические ФНФ могут быть реализованы на основе различных типов материалов, включая полимеры, металлы и полупроводники. Для создания оптической ФНФ необходимо использовать специальную технологию нанесения микроструктур на поверхность материала. Микроструктуры должны быть такими, чтобы они могли отражать или рассеивать световой луч в уникальный и случайный образ.

Для генерации псевдослучайных чисел на основе оптических ФНФ используется процесс чтения оптической информации с помощью лазера. Лазерное излучение позволяет получить уникальный образ, который может быть использован для генерации случайных чисел. Образы, полученные с помощью оптических ФНФ, могут быть использованы для создания последовательностей псевдослучайных чисел, которые обладают высокой степенью неравенства и непредсказуемости.

Важным преимуществом использования оптических ФНФ для генерации случайных чисел является высокая стойкость к атакам, т.к. оптические ФНФ основаны на физических свойствах материалов, которые трудно скопировать или воссоздать. Кроме того, использование оптических ФНФ позволяет получать высококачественные СЧ, которые могут применяться в различных целях.

Создание генератора случайных чисел с использованием шума

Создание генератора случайных чисел с использованием шума как источника случайности является одним из наиболее распространенных методов генерации СЧ. Шум может быть получен из различных источников, включая электрический, оптический, термальный и другие типы шумов.

В таком генераторе СЧ получаются путем измерения случайных флуктуаций в шуме. Для этого используются различные типы датчиков, которые могут быть созданы на основе различных физических явлений, таких как термальный шум, шум Джонсона – Найквиста, шум с лазера и другие.

Для обработки сигнала шума используются различные методы, включая фильтрацию, усиление, цифровую обработку и другие. После обработки сигнала получаются СЧ, которые могут быть использованы для различных целей, в том числе криптографических приложений, генерации СЧ в играх, симуляций и др.

Важным преимуществом генерации СЧ на основе шума является высокая стойкость к атакам, т.к. шум является физическим явлением, которое трудно воспроизвести и контролировать. Кроме того, использование шума как источника случайности позволяет получать высококачественные СЧ, которые могут быть использованы для различных целей.

Создание генератора случайных чисел с использованием электромагнитных помех

Создание ГСЧ с использованием электромагнитных помех как источника случайности является одним из наиболее эффективных методов генерации СЧ. Электромагнитные помехи – это случайные колебания электромагнитных полей, которые могут быть получены из различных источников, включая радиоволны, шумы силовых и сигнальных кабелей, соседних электронных устройств и т.д.

Для создания ГСЧ с использованием электромагнитных помех необходимо собрать антенну или датчик, который может измерять электромагнитные помехи в окружающей среде. Датчик может быть выполнен в различных формах и может иметь различные параметры, такие как усиление и чувствительность.

Для обработки сигнала электромагнитных помех используются различные методы, включая фильтрацию, усиление, анализ спектра и другие. После обработки сигнала получаются СЧ, которые могут быть использованы для различных целей, в том числе криптографических приложений, генерации СЧ в играх, симуляций и др.

Генерация СЧ на основе электромагнитных помех имеет ряд преимуществ:

- Высокая энтропия: электромагнитные помехи могут быть использованы для создания СЧ с высокой степенью случайности и энтропии, что обеспечивает надежную защиту от взлома и подделки данных.
- Доступность: электромагнитные помехи являются широко доступным источником случайности, который может быть использован на различных устройствах, включая компьютеры, смартфоны и другие электронные устройства.
- Эффективность: ГСЧ на основе электромагнитных помех могут быть реализованы с использованием простых схем, что делает их эффективными и экономически выгодными.

Создание генератора случайных чисел с использованием силы давления пользователя на экран смартфона

Создание ГСЧ на основе ФНФ с использованием силы давления пользователя на экран смартфона может быть эффективным способом генерации СЧ.

Экраны современных смартфонов часто оснащены датчиками давления, которые могут быть использованы для измерения силы, с которой пользователь нажимает на экран. Для создания ГСЧ с использованием ФНФ на основе силы давления пользователя на экран смартфона необходимо провести ряд измерений силы давления, которые генерируются пользователем при нажатии на экран. Эти данные могут быть использованы для создания уникального шаблона, который может быть преобразован в последовательность СЧ.

Для увеличения степени случайности генерируемых чисел можно проводить несколько измерений силы давления при каждом нажатии на экран. Также можно использовать дополнительные источники случайности, например шум в электрической цепи датчика давления или случайные задержки между нажатиями на экран.

Одним из преимуществ использования ФНФ на основе силы давления пользователя на экран смартфона является возможность применения этого генератора в качестве альтернативы традиционным методам генерации СЧ, которые могут быть уязвимы к атакам. Кроме того, использование ФНФ на основе силы давления пользователя на экран смартфона может быть полезным в случаях, когда требуется генерация СЧ без дополнительных устройств или оборудования.

Создание генератора случайных чисел с использованием памяти устройства

Создание ГСЧ на основе ФНФ с использованием состояния памяти устройства может быть эффективным способом генерации СЧ.

Многие устройства, такие как компьютеры, телефоны и другие электронные устройства, содержат микросхемы памяти, которые могут быть использованы для генерации СЧ на основе состояния памяти устройства. Эта техника может быть основана на том, что начальное состояние памяти устройства может быть уникальным и случайным.

Для создания ГСЧ на основе состояния памяти устройства, необходимо сначала получить начальное состояние памяти, которое может быть использовано для генерации последовательности СЧ. Это может быть достигнуто, например, путем чтения некоторого количества байтов из памяти устройства в определенный момент времени.

Для увеличения степени случайности генерируемых чисел можно использовать дополнительные источники случайности, например шум в электрической цепи микросхемы памяти или случайные значения таймеров и счетчиков устройства.

Одним из преимуществ использования ФНФ на основе состояния памяти устройства является то, что этот метод может быть применен для генерации СЧ без дополнительных устройств или оборудования. Кроме того, начальное состояние памяти устройства может быть изменено только случайным образом, что делает его очень сложным для воспроизведения или атаки. Однако, для достижения высокой степени случайности необходимо использовать достаточно большой объем данных и хорошо продуманную методику для генерации СЧ.

Использование физически неклонируемых функций для генерации случайных чисел в программе на языке C++

Для использования ФНФ с целью генерации СЧ в программе на C++ можно подключить библиотеку OpenSSL. Данная библиотека предоставляет функции, которые используют криптографически безопасные генераторы случайных чисел, основанные на ФНФ.

Вот пример программы на C++, которая использует библиотеку OpenSSL для генерации случайного числа:

```cpp
#include <openssl/rand.h>
#include <iostream>

int main() {
    unsigned char buffer[4];
    RAND_bytes(buffer, sizeof(buffer));

    unsigned int* random_number = reinterpret_cast<unsigned int*>(buffer);
    std::cout << "Random number: " << *random_number << std::endl;

    return 0;
}
```

Рисунок 1 — Код первой программы

Здесь генерируется массив «buffer» из 4-х случайных байтов с помощью функции «RAND_bytes». Затем эти байты интерпретируются как беззнаковое целое число с помощью приведения типа «reinterpret_cast<unsigned int*>(buffer)». Полученное число выводится на экран. Несколько примеров вывода программы:

```
Random number: 1285241114
```

```
Random number: 3152517205
```

Рисунок 2, 3 — Результаты работы первой программы

Вот пример еще одной программы на C++, использующей библиотеку OpenSSL для генерации случайного числа:

```cpp
#include <openssl/rand.h>
#include <iostream>

int main() {
    unsigned char buffer[8];
    if(RAND_bytes(buffer, sizeof(buffer)) == 0) {
        std::cerr << "Error generating random numbers!" << std::endl;
        return 1;
    }

    uint64_t random_number = *reinterpret_cast<uint64_t*>(buffer);
    std::cout << "Random number: " << random_number << std::endl;

    return 0;
}
```

Рисунок 4 — Код второй программы

В этой программе «RAND_bytes» генерирует 8 случайных байтов, которые затем интерпретируются как 64-битное беззнаковое целое число. Если при вызове «RAND_bytes» произошла ошибка, программа выведет сообщение об ошибке. В противном случае программа выведет сгенерированное случайное число.

```
Random number: 11072600854160185063
```

```
Random number: 17206203176475216913
```

Рисунок 5, 6 — Результаты работы второй программы

Если увеличить размер буфера, то и сгенерированное случайное число будет больше. Например, если использовать unsigned char buffer[8], то сгенерированное число будет 64-битным (uint64_t), что позволит представлять числа в диапазоне от 0 до $2^{64} – 1$.

В заключение можно отметить, что это направление генерации СЧ на основе ФНФ является важным для многих областей науки и технологии, включая криптографию, статистику, моделирование и другие области.

Мы рассмотрели различные методы создания ГСЧ на основе ФНФ, включая использование шума, электромагнитных помех, оптических ФНФ, а также состояния памяти устройства. Каждый из этих методов имеет свои преимущества и недостатки, и выбор метода зависит от конкретной задачи.

В целом, использование ФНФ для генерации СЧ является эффективным и надежным подходом, который может быть применен во многих областях.

Однако следует учитывать, что использование ФНФ может быть затратным с точки зрения вычислительных ресурсов и времени, что может снижать производительность системы. Кроме того, необходимо обеспечивать достаточную защиту от физических атак на генератор, т.к. любые нарушения целостности источника энтропии могут привести к компрометации всей системы.

Список использованных источников:

1.«Информатика» – научный рецензируемый журнал [Электронный ресурс]. – Режим доступа: https://inf.grid.by/jour/article/view/370/340. – Дата доступа: 02.04.2023.

2.Habr – сообщество IT-специалистов [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/343386/. – Дата доступа: 02.04.2023.

3.Интернет-портал для IT-специалистов [Электронный ресурс]. – Режим доступа: https://itnan.ru/post.php?c=1&p=343386. – Дата доступа: 02.04.2023.

4.Новости информационных технологий [Электронный ресурс]. – Режим доступа: https://www.pvsm.ru/kontrafakt/269336. – Дата доступа: 02.04.2023.

UDC

RANDOM NUMBER GENERATION BASED ON PHYSICALLY NON-CLONEABLE FUNCTIONS

Timoshevich K. S., Kotova K. A., Kvachenyuk Y. D., Nikolaychik A. S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Stroinikova E. D. – Senior Lecturer in Department of Informatics

Annotation. This work examines different methods of generating random numbers (RNGs) using physically unclonable functions (PUFs), including the utilization of electromagnetic noise, optical PUFs, and device memory states. Each method is discussed in terms of its underlying principles and the process of random number generation (RNG).

Keywords. Random number generators, physically unclonable functions.