DOI 10.37882/2223-2966.2024.8.05

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ВЫСОКОСКОРОСТНЫХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ АУТЕНТИФИКАЦИИ ДОСТУПА И РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

PROSPECTS OF APPLICATION OF HIGH-SPEED RANDOM NUMBER GENERATORS FOR ACCESS AUTHENTICATION AND KEY DISTRIBUTION

S. Arvanova

Summary. The main prospects of application of high-speed random number generators for access authentication and key distribution are considered. The main advantages of using superlattices based on physically unclonable functions are presented. An approximate algorithm of software realization of the presented idea is also presented.

Keywords: quantum key distribution, quantum random number generator, authentication, superlattices.

Арванова Саният Мухамедовна
Старший преподаватель, ФГБОУ ВО «Кабардино-Балкарский государственный университет им. Х.М. Бербекова»;
Аспирант, ФГАОУ ВО «Южный федеральный университет»
sani_07@mail.ru

Аннотация. Рассматриваются основные перспективы применения высокоскоростных генераторов случайных чисел для аутентификации доступа и распределения ключей. Представлены основные преимущества применения сверхрешеток на основе физически неклонируемых функций. Также представлены примерный алгоритм программной реализациии представленной идеи.

Ключевые слова: квантовое распределение ключей, квантовый генератор случайных чисел, аутентификация, сверхрешетки.

Схемы аутентификации доступа и распределения ключей являются первой линией защиты сети и являются важной технологией для предотвращения нелегальных терминалов и обеспечения безопасности.

Высокая мобильность, низкое время задержки и ограниченные ресурсы предъявляют более высокие требования к вопросам безопасности, включая безопасность идентификации и данных. Кроме того, доступ в любое время означает высококачественные сетевые услуги, такие как динамический доступ и плавный механизм идентификации передачи, вызванный перемещением спутников.

Аутентификация доступа и распределение ключей (ADK) играют важную роль в обеспечении безопасности сетей и являются первой линией защиты от нелегального доступа и атак. Актуальность ADK обусловлена следующими причинами (схема 1):

1. Усиление киберугроз: киберугрозы становятся все более изощренными и многочисленными. Атаки на сети и системы совершаются с целью кражи данных, нарушения работы или получения несанкционированного доступа. ADK позволяет предотвратить нелегальный доступ к сети и защитить ее от неавторизованных пользователей.
2. Рост числа подключенных устройств: С развитием Интернета вещей (IoT) и мобильных технологий количество устройств, подключенных к сети, постоянно растет. Это увеличивает площадь распространения атаки и делает сети более уязвимыми для несанкционированного доступа. ADK позволяет обеспечить безопасный доступ для всех подключенных устройств и предотвратить нелегальный доступ к сети.
3. Необходимость соответствия нормативным требованиям: Многие организации обязаны соблюдать нормативные требования, которые требуют внедрения надежных механизмов аутентификации и распределения ключей. ADK позволяет организациям соответствовать этим требованиям и защитить свои сети от несанкционированного доступа.

Схема 1. Актуальность ADK

4. Повышение эффективности и удобства использования: Современные технологии ADK обеспечивают высокую эффективность и удобство использования. Они позволяют пользователям легко и быстро проходить аутентификацию, не тратя много времени на ввод паролей или других идентификационных данных.
5. Интеграция с другими системами безопасности: ADK может быть интегрирована с другими системами безопасности, такими как межсетевые экраны, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). Это позволяет создать многоуровневую систему безопасности, которая обеспечивает надежную защиту сети от различных угроз.

Таким образом, актуальность ADK обусловлена необходимостью защиты сетей от нелегального доступа, соответствием нормативным требованиям, повышением эффективности и удобства использования, а также интеграцией с другими системами безопасности.

Применение сверхрешеток в области аутентификации доступа и распределения ключей может быть связано с использованием их уникальных физических свойств для обеспечения безопасности информации. Например, сверхрешетки могут обладать особыми оптическими, электрическими или магнитными свойствами, которые можно использовать для создания новых методов аутентификации и шифрования.

Применение сверхрешеток при аутентификации доступа и распределении ключей может иметь несколько потенциальных преимуществ:

— Физическая безопасность: Сверхрешетки могут быть использованы для создания уникальных физических меток аутентификации, которые трудно скопировать или подделать. Это обеспечивает дополнительный уровень безопасности при идентификации пользователей или устройств.
— Устойчивость к взломам: из-за уникальных свойств сверхрешеток, таких как особые оптические или электрические характеристики, системы, основанные на них, могут быть более устойчивы к различным видам атак, включая попытки взлома или подделки ключей.
— Сложность взлома: Использование сверхрешеток для распределения ключей может усложнить задачу злоумышленников при попытке взлома системы. Это связано с особыми свойствами сверхрешеток, которые могут создавать уникальные ключи или механизмы шифрования.
— Устойчивость к квантовым атакам: Некоторые сверхрешетки могут обладать свойствами, которые делают их более устойчивыми к атакам, основанным на квантовых вычислениях. Это может быть важно при разработке криптографических методов, устойчивых к будущим квантовым технологиям.
— Инновационные методы шифрования: Применение сверхрешеток может способствовать разработке новых инновационных методов шифрования и аутентификации, которые могут быть более эффективными и безопасными по сравнению с традиционными подходами.

Генераторы случайных чисел на полупроводниковых сверхрешётках (PRNG) — это устройства, которые используют квантово-механические эффекты в полупроводниковых сверхрешётках для генерации случайных чисел. Сверхрешётка — это структура, состоящая из чередующихся слоёв двух или более полупроводниковых материалов.

PRNG работают следующим образом:

Электрический ток пропускается через сверхрешётку, что приводит к генерации носителей заряда (электронов и дырок). Носители заряда движутся по сверхрешётке, сталкиваясь с дефектами и носителями заряда. Эти столкновения приводят к случайным изменениям в движении носителей заряда, которые преобразуются в случайную последовательность бит с помощью электронных схем.

Генераторы на полупроводниковых сверхрешётках являются перспективным направлением в области генерации случайных чисел. Они обладают высокой скоростью генерации, не требуют использования внешних источников случайности и могут быть легко интегрированы в электронные устройства. Это делает их идеальными для использования в различных приложениях, где требуется генерация случайных чисел.

В [1] исследована аутентификация доступа и распределения ключей на основе SSL-PUF для интегрированной сети «космос-воздух-земля», которая может защитить от атак «маскарадов» с и атак типа «злоумышленник посередине».

В [2] описана реализация и тестирование генератора случайных чисел и доказана их высокая стойкость к возможным атакам. А в [3] приводится, что если в классических системах симметричного шифрования секретные ключи меняются на передающей и приемной сторонах при помощи оператора, то частая смена ключей, например, раз десятки секунд, практически невозможна. Если секретные ключи меняются не столь часто, то они используются как мастер-ключи для получения производных от них сеансовых ключей, что в принципе может приводить к понижению криптостойкости системы.

В [5] изложены этапы развития формирования теории квантовой криптографии. Освещены два основных направления развития систем квантового распределения ключей. Дан сравнительный анализ существующих протоколов распределения ключей: BB84, B92, 4+2, с шестью состояниями, Гольденберга-Вайдмана, Коаши-Имото и ЭПР. Приведены типовые структуры систем квантового распределения ключей на основе кодирования информации в поляризационных, фазовых и временных состояниях фотонов. Сформулированы перспективы развития систем квантового распределения ключей.

Генераторы случайных чисел на полупроводниковых сверхрешётках в данном случае более чем актуальны.

Полупроводниковые сверхрешетки могут использоваться для шифрования данных в пост-квантовой криптографии, используя технику обмена ключами на основе одиночных фотонов. В таком случае полупроводниковые сверхрешетки могут использоваться для генерации и детектирования одиночных квантов. Они могут создавать фотоны с определенным спином, который является своего рода «ключом» для шифрования данных. Этот спин может изменяться в зависимости от состояния сверхрешетки.

Шифрование происходит следующим образом: отправитель и получатель обмениваются одиночными фотонами, где состояние спина сверхрешетки используется для шифрования информации. Отправитель передает фотоны с различными спинами, которые являются «ключом», и получатель использует свой собственный набор сверхрешеток, чтобы определить спин каждого фотона и восстановить информацию.

Полупроводниковые сверхрешетки обеспечивают высокую эффективность генерации и детектирования одиночных фотонов, что делает их привлекательными для пост-квантовой криптографии. Они также обладают преимуществами в виде высокой скорости передачи данных и потенциала интеграции с другими полупроводниковыми элементами, что делает их перспективной технологией для будущих систем шифрования.

Алгоритм работы полупроводниковых сверхрешеток определяется их структурой и функциональностью. В основе работы сверхрешеток лежит использование квантовых эффектов, таких как квантовая яма или квантовая проволока, для создания уникальных электронных состояний.

Один из самых распространенных алгоритмов работы сверхрешетки — это туннелирование электронов между квантовыми состояниями внутри структуры. Когда сверхрешетка подвергается воздействию электрического поля или освещению, происходит просачивание электронов через энергетические барьеры между состояниями. Это создает эффект переноса заряда или генерацию фотоэлектрической энергии.

У полупроводниковых сверхрешеток также существуют другие алгоритмы работы, связанные с применением их в оптических и электронных устройствах, таких как лазеры, фотодиоды, фототранзисторы и другие. Эти алгоритмы могут быть связаны с взаимодействием с электрическими полями или другими формами энергии, которые предоставляются внешними источниками.

Использование сверхрешеток для шифрования иллюстрируется следующей программой:

```
import numpy as np.
# Задаем сверхрешетку
supergrid = np.array([[1, 2, 3],
 [4, 5, 6],
 [7, 8, 9]])
# Вводим сообщение для шифрования
message = input(«Введите сообщение для шифрования: «)
# Преобразуем сообщение в числовой массив
message_nums = np.array([ord(char) for char in message])

# Шифруем сообщение
encrypted_message = np.dot (message_nums, supergrid) % 26
# Выводим зашифрованное сообщение
print («Зашифрованное сообщение: », «». join ([chr(num + 65) for num in encrypted_message]))
```

Программа работает следующим образом:

- сверхрешетка задается в виде двумерного массива. supergrid;
- пользователю предлагается ввести сообщение для шифрования;
- сообщение преобразуется в числовой массив, где каждой букве соответствует числовое значение. message_nums;
- производится умножение числового массива на сверхрешетку по модулю 26, чтобы получить зашифрованное сообщение;
- зашифрованное сообщение выводится на экран в виде буквенной строки.

Надо заметить, что использование сверхрешеток SLP (Stochastic Logic Processor) в качестве метода шифрования с использованием физически неклонируемых функций позволит проводить генерацию уникальных ключей

Использование физически неклонируемых функций SLP решетки может сделать систему более устойчивой к различным видам атак, включая атаки на основе перебора ключей или полного доступа к системе.

Применение сверхрешеток для аутентификации доступа и распределения ключей может обеспечить дополнительный уровень безопасности, особенно в контексте устойчивости к квантовым атакам. Надежность сверхрешеток при аутентификации и распределении ключей зависит от конкретного типа сверхрешетки, ее свойств и применяемых криптографических протоколов

ЛИТЕРАТУРА

1. Li Wei Xu, Han Wu, Jian Guo Xie, Qiong Yuan, Ying Sun, Guo Zhen Shi, Shou Shan Luo Схема аутентификации доступа и распределения ключей на основе SSL-PUF для интегрированной сети «космос-воздух-земля» // Journal. Entropy (ISSN 1099–4300)
2. Беспалов Д.Б., Белим С.В. Реализация генератора случайных чисел на базе звуковой карты // МСиМ. 2010. №1 (21). URL: https://cyberleninka.ru/article/n/realizatsiya-generatora-sluchaynyh-chisel-na-baze-zvukovoy-karty (дата обращения: 08.02.2024).
3. Балыгин К.А., Зайцев В.И., Климов А.Н., Кулик С.П., Молотков С.Н. Квантовый генератор случайных чисел, основанный на пуассоновской статистике фотоотсчетов, со скоростью около 100 МБИТ/С// Журнал экспериментальной и теоретической физики. 2018. Т. 126. № 6. С. 728–740.
4. Архангельская А.В. Некоторые аспекты разработки генераторов случайных чисел / А.В. Архангельская // Безопасность информационных технологий — 2004 — № 3 — С 45–48.
5. К.Е. Румянцев, Д.М. Голубчиков Квантовая криптография: принципы, протоколы, системы //Учебное пособие. — Таганрог: Изд-во ТТИ ЮФУ, 2009. — 122 с.

Журнал «Современная наука: актуальные проблемы теории и практики»