Квантовая магия случайности:

как частицы создают числа

Олег Иванов

Менеджер продуктов

инфотекс ТЕХНОФЕСТ

Синий поток

Что такое и зачем нужен КГСЧ ?

Квантовый генератор случайных чисел (QRNG) – это устройство, создающее истинно случайные последовательности на основе непредсказуемых квантовых явлений

На практике используются оптоэлектронные схемы, формирующие и измеряющие квазиоднофотонные состояния в квантовой системе

В отличие от псевдослучайных программных датчиков, QRNG обеспечивает абсолютную непредсказуемость, что критически важно как для любого СКЗИ, но и для систем квантового распределения ключей

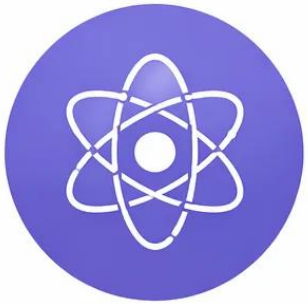
Существует много примеров атак и компрометации на криптографических решений, построенные на слабых ПДСЧ/ФДСЧ

Типы квантовых генераторов случайных чисел

Фотонные КГСЧ

КГСЧ на квантовом туннелировании

КГСЧ на флуктуациях вакуума



КГСЧ на спине или уровнях атома

Где используются квантовые генераторы случайных чисел сегодня

Генерация криптографических ключей

Научные и вычислительные симуляции

Защищённые коммуникации

Общественные маяки случайности

Отличия квантового генератора случайных чисел от классического генератора случайных чисел

ViPNet Quantum Random Number Generator

Последовательность получения случайных чисел с помощью ViPNet QRNG

1

Генерация квантового события

2

Измерение его результатов

3

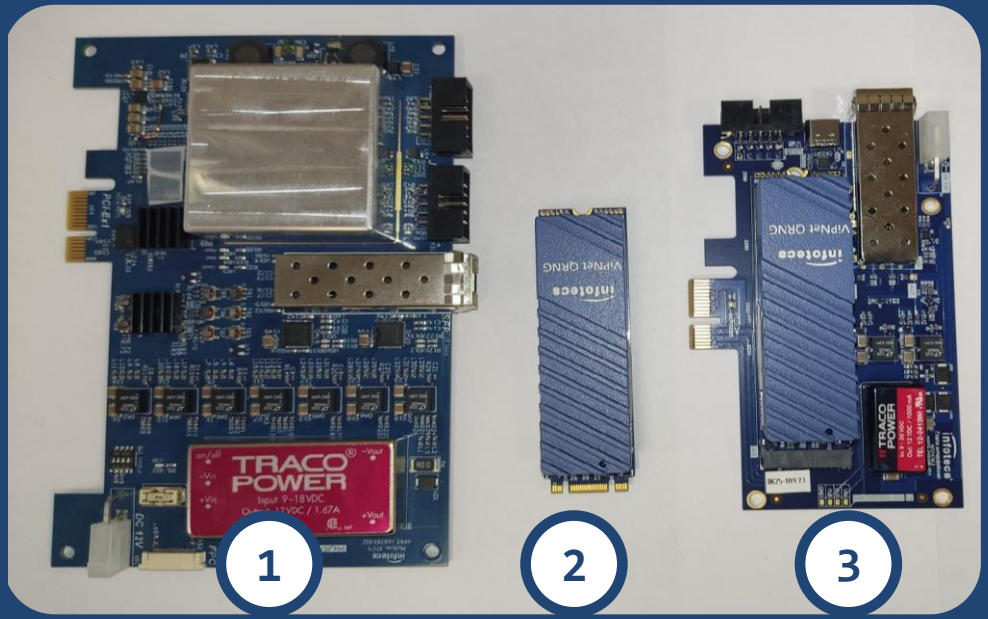
01
10

Преобразование его в цифровую форму

4

Полученная последовательность случайных чисел дополнительно защищена криптографическим способом

Модели ViPNet QRNG



1. **КГСЧ Ethernet/PCIe** (10x15 см). Сертифицирован в составе ViPNet РУКС по классу КС3

2. **КГСЧ M.2 (2x8 см).** Передаётся на сертификацию в составе HSM по классу КВ

3. **КГСЧ M.2 +** переходная плата Ethernet/PCIe (7x10 см). Внедрение с РУКС-Б в 2027 г.

Сравнение ФДСЧ и КГСЧ

Характеристики	ГСЧ Гроссмейстер	ViPNet QRNG
Габариты	15 x 13 x 4,5 мм	80 x 23 x 15.9 мм
Максимальное энергопотребление	–	До 3 Вт по цепи питания +3.3В
Интерфейс подключения	Встраивается через интерфейс SPI и I2C	1. Переходная плата PCI Express Gen1.0 x 1 (пропускная способность 2.5 Гбит/с) 2. M.2, разъем с ключами M+B, совместимость с разъёмами хоста высотой от 4 мм.
Источник энтропии	Шумящий диод	Квантовый (фотоэффект)
Номинальная скорость формирования случайных чисел	4096 бит/с	170 Мбит/с
Диапазон рабочих температур	+5...+50°C	+10...+35°C

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ИНФОТЕКС · TS Solution · AXOFT

Подписывайтесь на наши соцсети