

Ежегодная международная научно-практическая конференция

«РусКрипто'2024»

Высокоскоростная система квантового распределения ключей

Павлов Игорь Денисович
Технический директор QRate

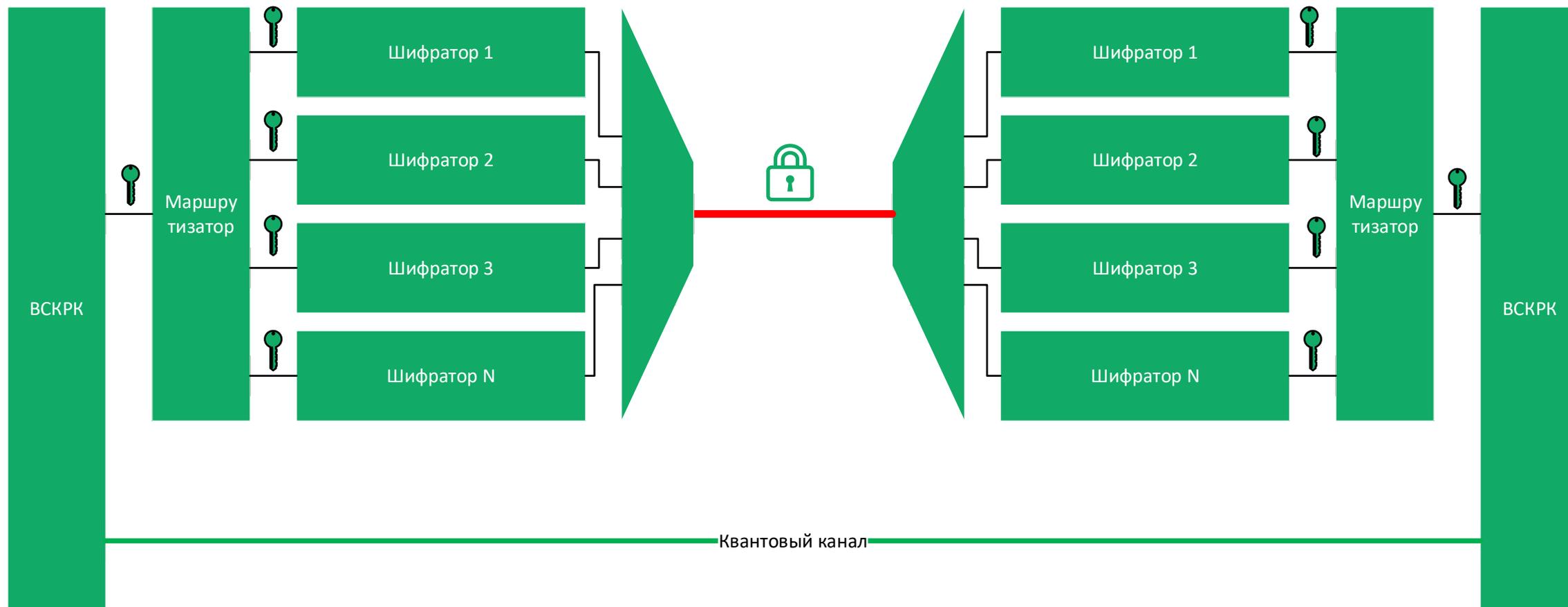
Зачем нужна высокоскоростная система КРК?

- ключ генерируется для каждого сообщения (каждый ключ используется только один раз)
- ключ статистически надёжен (то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны)
- длина ключа равна или больше длины сообщения
- исходный (открытый) текст обладает некоторой избыточностью (что является критерием оценки правильности расшифровки)

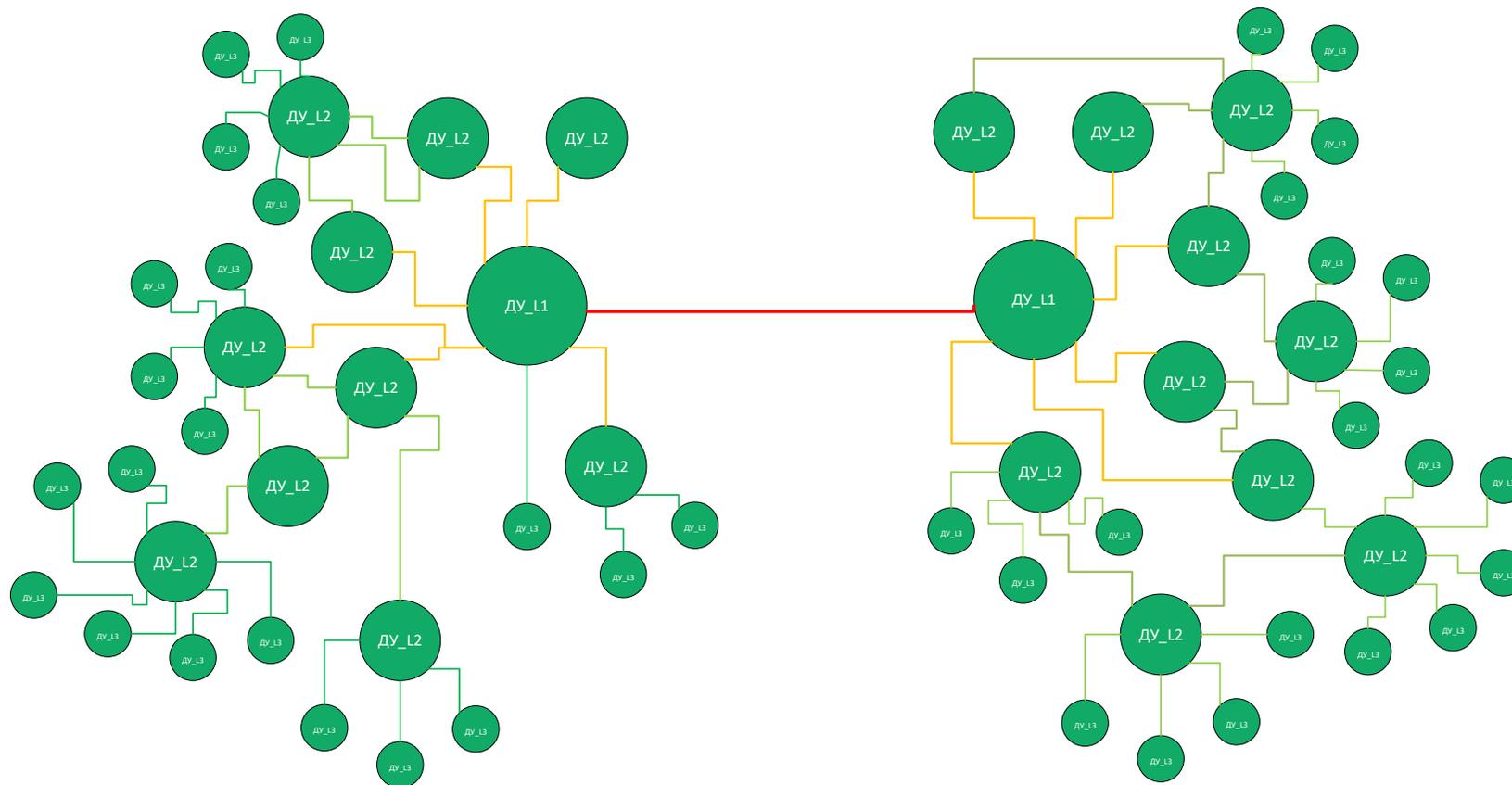


Клод Шеннон

Применение ВСКРК для защиты каналов с несколькими шифраторами



Требования к скорости ККС ВРК на основании топологии квантовой сети



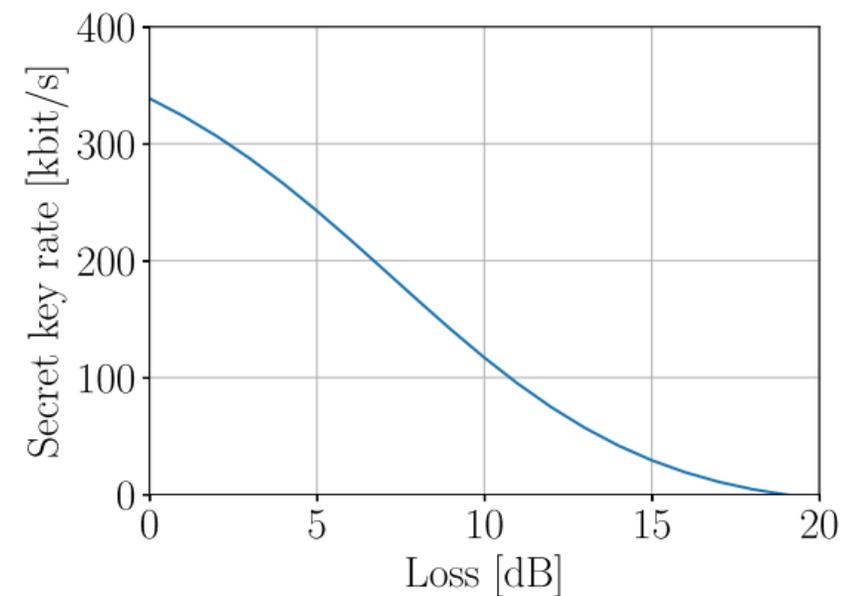
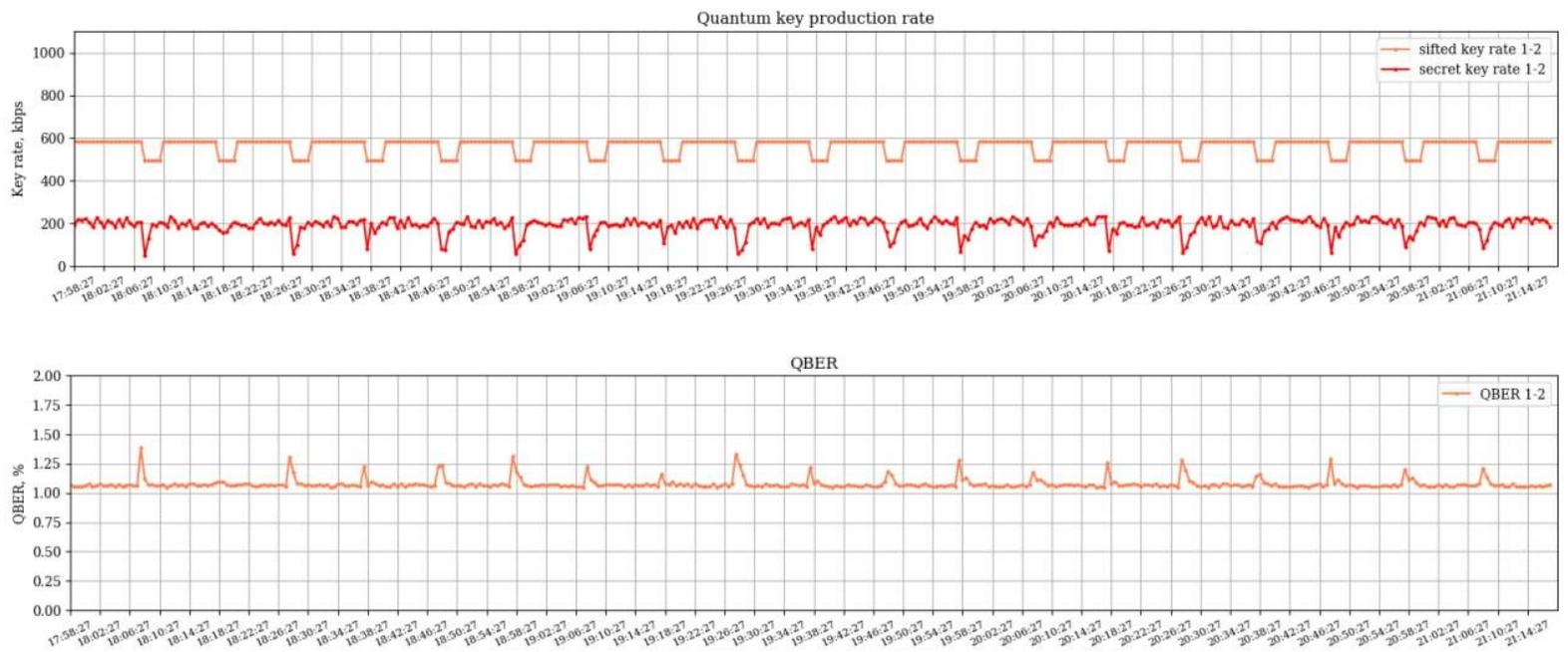
Ограничивающие факторы повышения скорости генерации ключей

- Частота приготовления состояний
- Мертвое время детекторов
- Эффективность детекторов
- Неоптимальность протокола

Примененные методы для повышения скорости

- Повышение тактовой частоты приготовления квантовых состояний до 1.25 ГГц
- Разработка стробируемого детектора одиночных фотонов с частотой строба 1.25 ГГц и мертвым временем ~ 500 нс
- Внедрен протокол в котором базисы выбираются с соотношением вероятностей 90:10

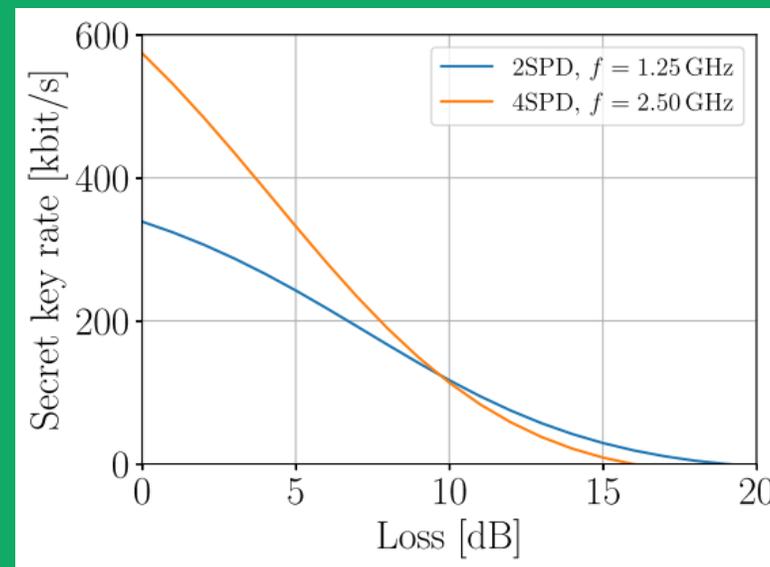
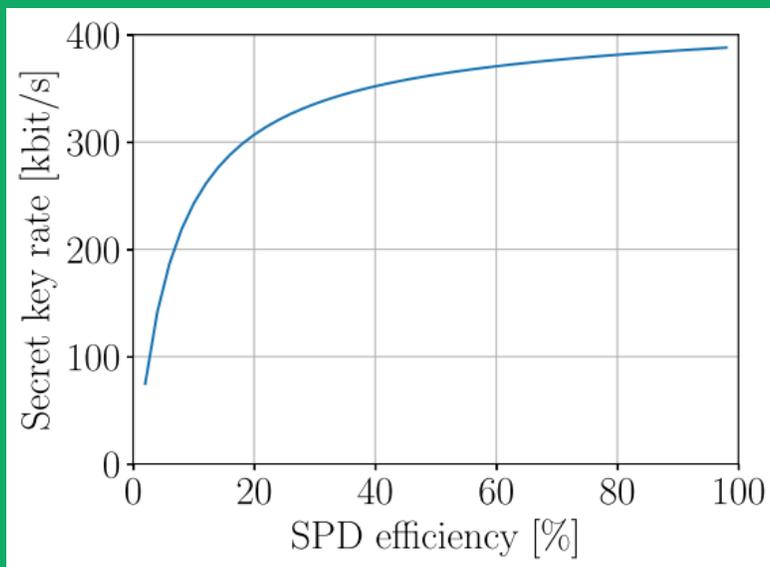
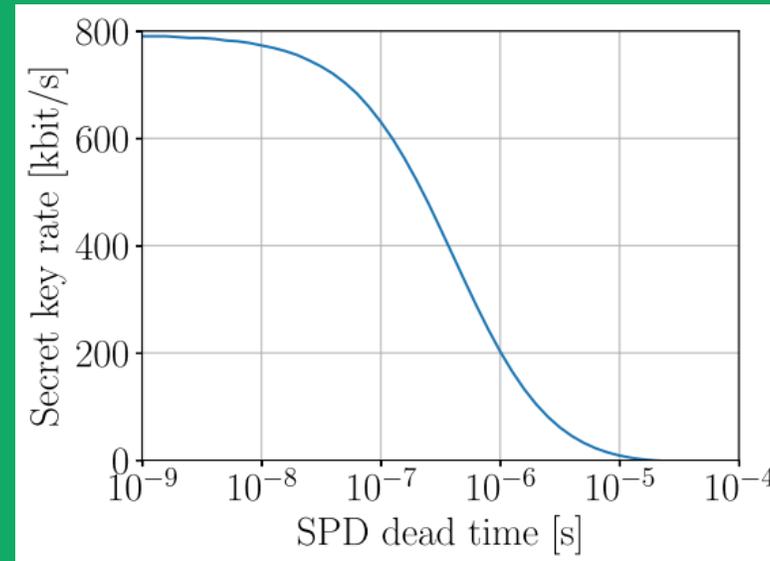
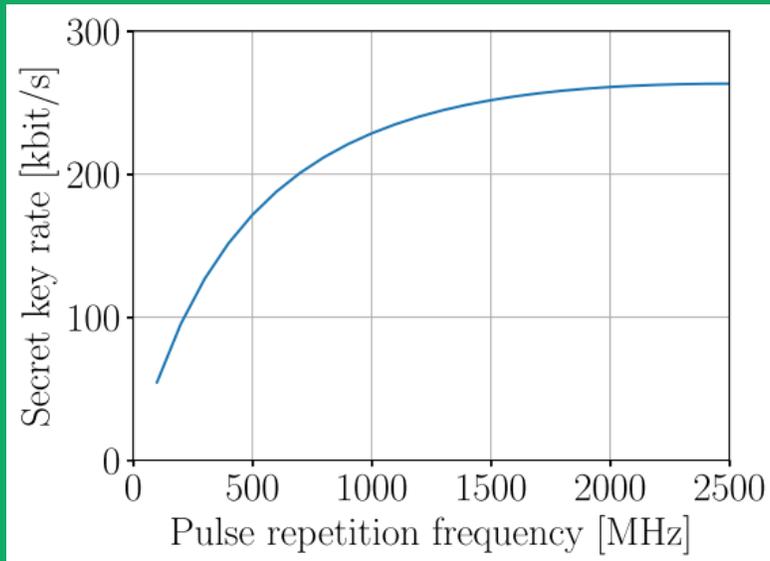
Испытания макетов ВСКРК



Методы дальнейшего увеличения скорости

- Внедрение детекторов с мертвым временем ~ 200 нс
- Повышение частоты приготовления до 2.5ГГц
- Применение 4-х детекторов одиночных фотонов (?)

$\mu = 0.3$
 $\nu_1 = 0.1$
 $\nu_2 = 0.001$
 $\rho_\mu = 0.7$
 $\rho_{\nu_1} = 0.2$
 $\rho_Z = 0.9$
 $f = 1.25 \cdot 10^9 \text{ Hz}$
 $QE = 0.1$
 $P_{dc} = 10^{-6}$
опт. ошибка = 0.01
 $DT = 800 \cdot 10^{-9}$



Контактная информация

- **Электронная почта:**
ip@goqrate.com
- **Телефон:**
+7 (967) 172-80-87
- **VK:** <https://vk.com/goqrate>
- **Сайт:**
goqrate.com



Вопросы

???