ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Передатчик для городской сети КРК с пассивным приготовлением состояний

Игорь Павлов
Технический директор QRate

Система КРК QRate QKD312

Протокол функционирования	BB84 Decoy-State	
Рабочая длина волны	1550±10	нм
Частота приготовления	312,5	МГц
Поддержка протоколов	ETSI, ПЛИВ, ProtoQA* в разработке	
Требования к сети	наличие одномодового “темного” волокна	
Мощность	800	Вт
Габаритные размеры	450 x 600 x 177	мм

Возможные атаки:
Superlinear detector control
Detector mismatch
Detector dead-time
Trojan-horse attack
Light injection in calibration photodetector
Backflash
Pattern effect in the IM
QRNG attack

ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Пилотные проекты QRate

Пилотная сеть м10 – Сколково

2018

Интеграция в действующие линии связи

2019

Прохождение ПМИ

2020

Сопряжение с инфраструктурой

2020

Защищённая ВКС

2021

Атмосферное распределение ключей

2022

Партнёры:

МИСИС УНИВЕРСИТЕТ

РЖД

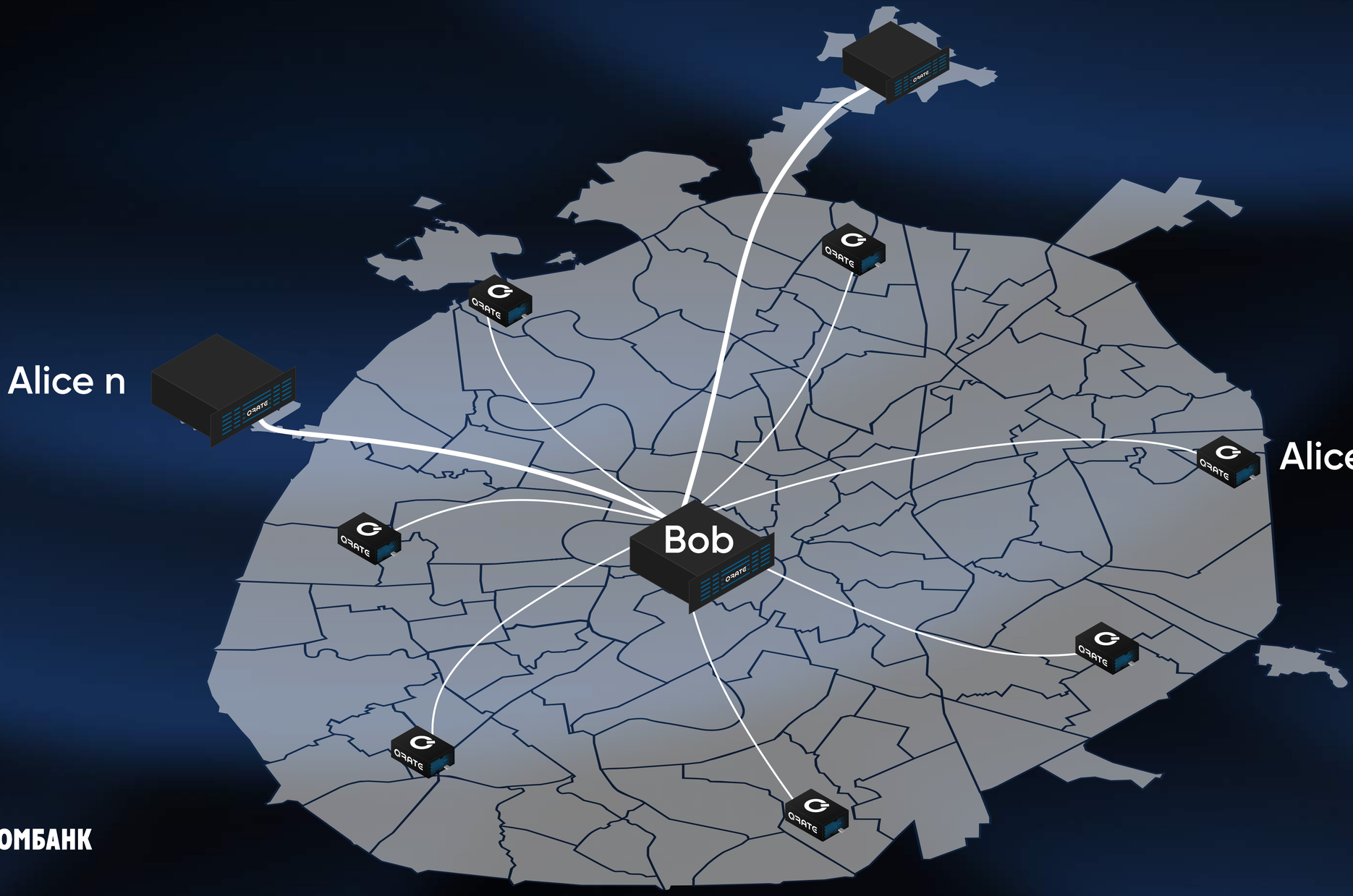
ТТК

МТУСИ

ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Внутригородская квантовая сеть



ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Скорость генерации ключа

$\mu = 0.3$

$\eta = 20\%$

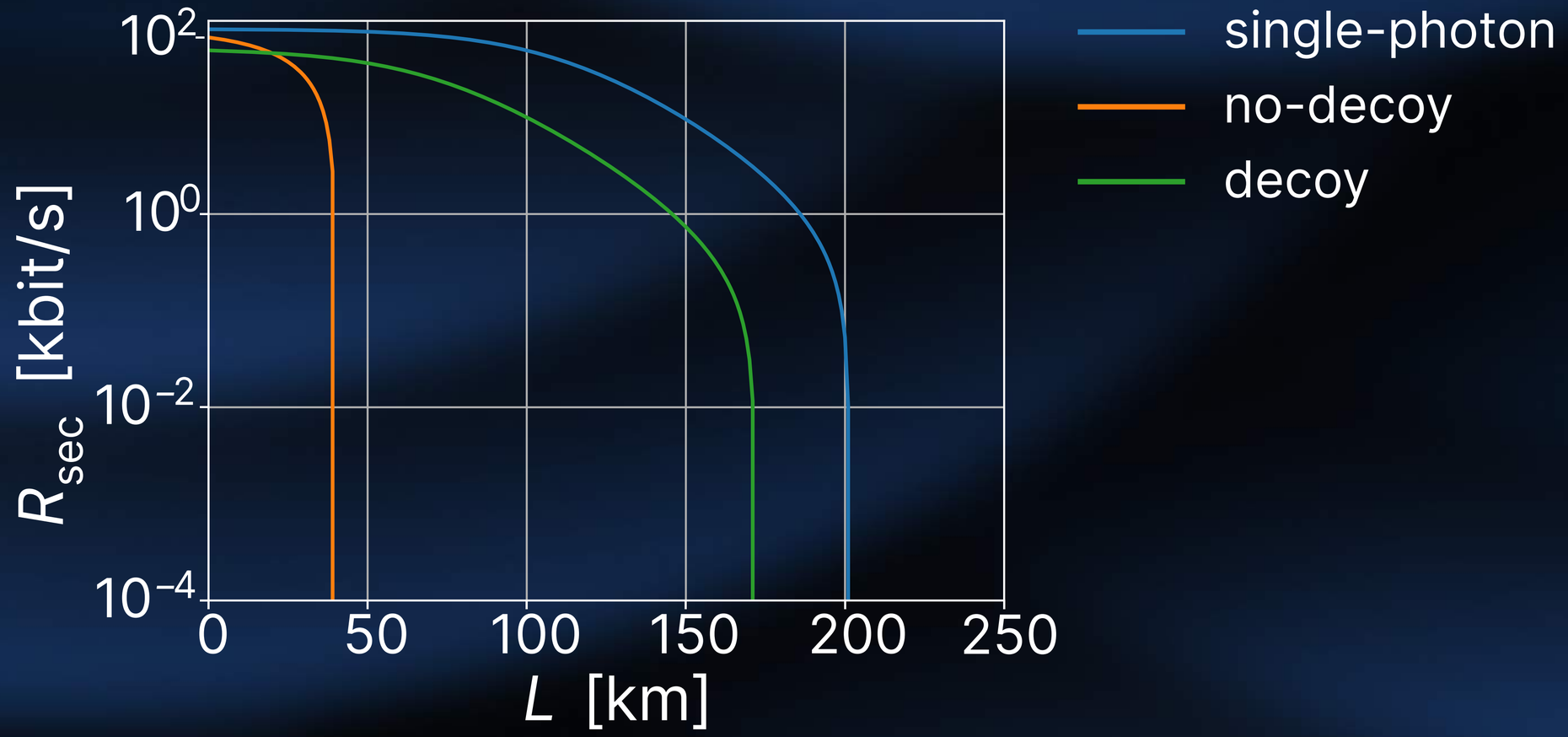
$p_{dc} = 10^{-6}$

$p_{opt} = 1\%$

$\tau_d = 5\ \mu s$

$\delta_B = 3 dB$

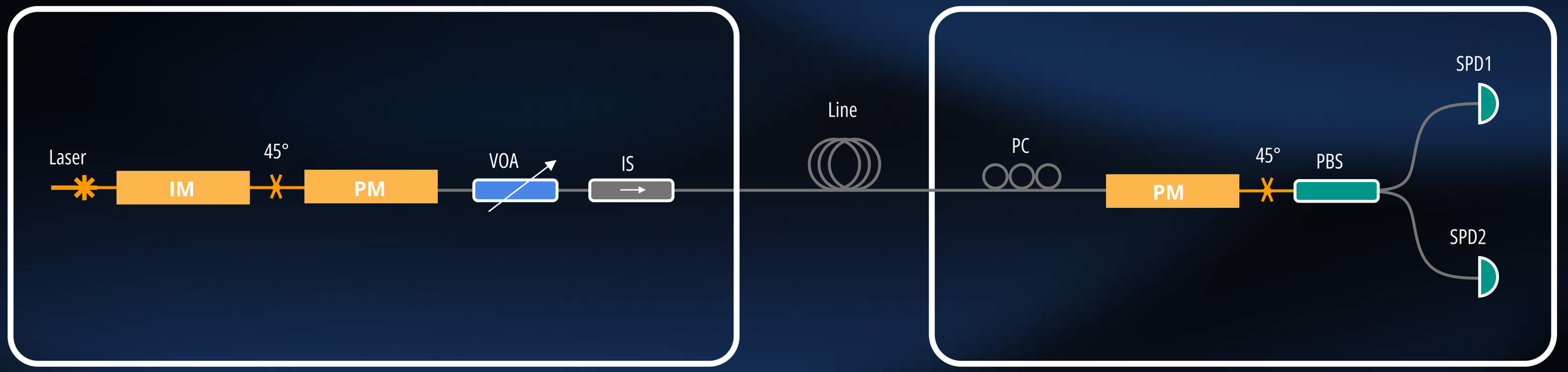
$f = 312 MHz$



ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Оптическая схема QKD312



Кодируемые состояния
на сфере Пуанкаре

1) A. Duplinsky, V. Ustimchik, A. Kanapin, V. Kurochkin and Y. Kurochkin, “Low loss QKD optical scheme for fast polarization encoding”, Opt. Express 25(23), 28886-18897 (2017).

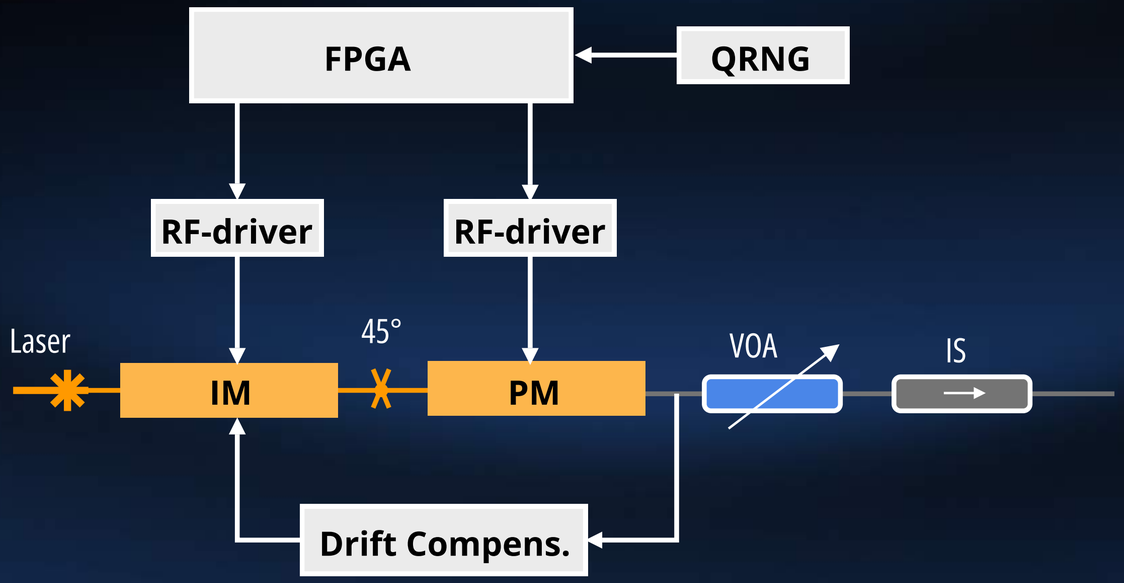
2) A. Duplinskiy et al., "Quantum-Secured Data Transmission in Urban Fiber-Optics Communication Lines ", Journal of Russian Laser Research, 2018, Vol. 39, no. 2, P. 113-119.

ГАЗПРОМБАНК
Банк ГПБ (АО)

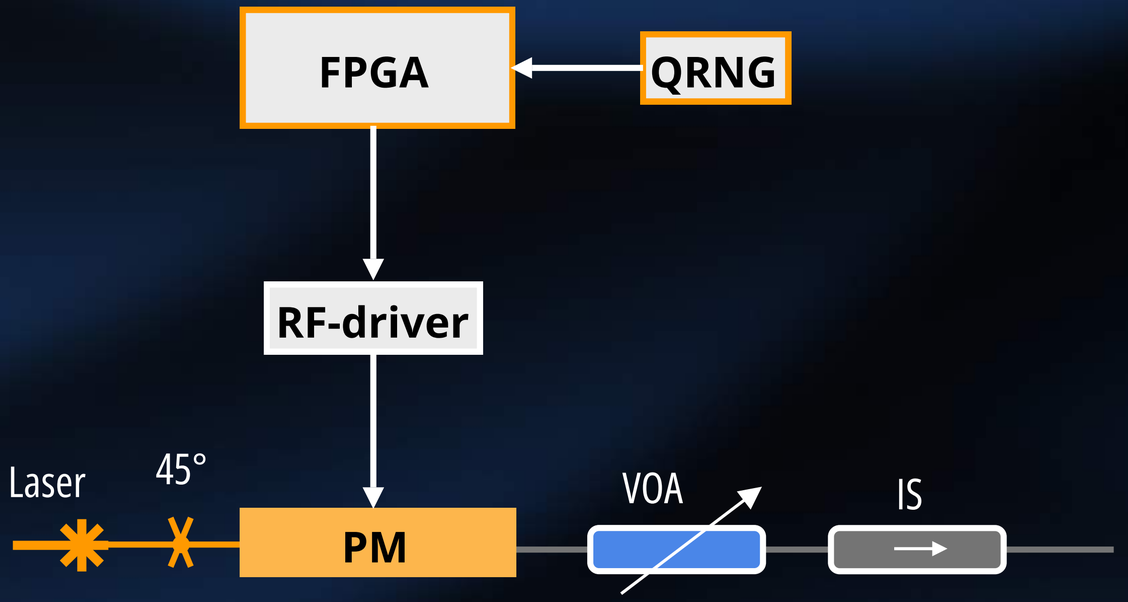
QRATE

Отказ от состояний-ловушек позволяет существенно упростить систему

Было



Стало



Защита от атак:
Trojan-horse attack
Pattern effect in the IM
QRNG attack

ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Идея пассивного приготовления поляризационных состояний

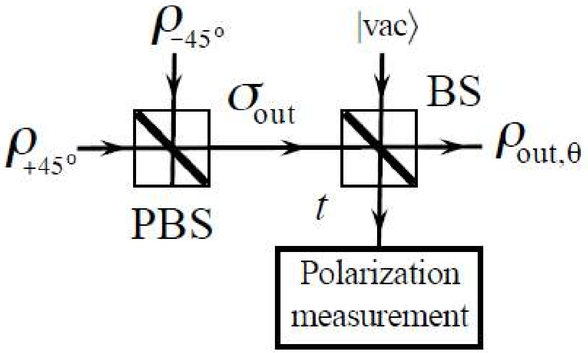


FIG. 2: Basic setup of a passive BB84 QKD source with strong coherent light. The mean photon number of the signal states $\rho_{+45°}$ and $\rho_{-45°}$ can be chosen very high; for instance, $\approx 10^8$ photons. The parameter t represents the transmittance of the BS; it satisfies $t \ll 1$.

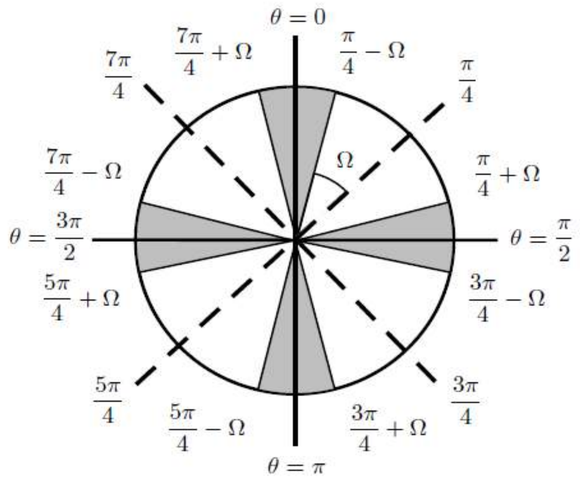
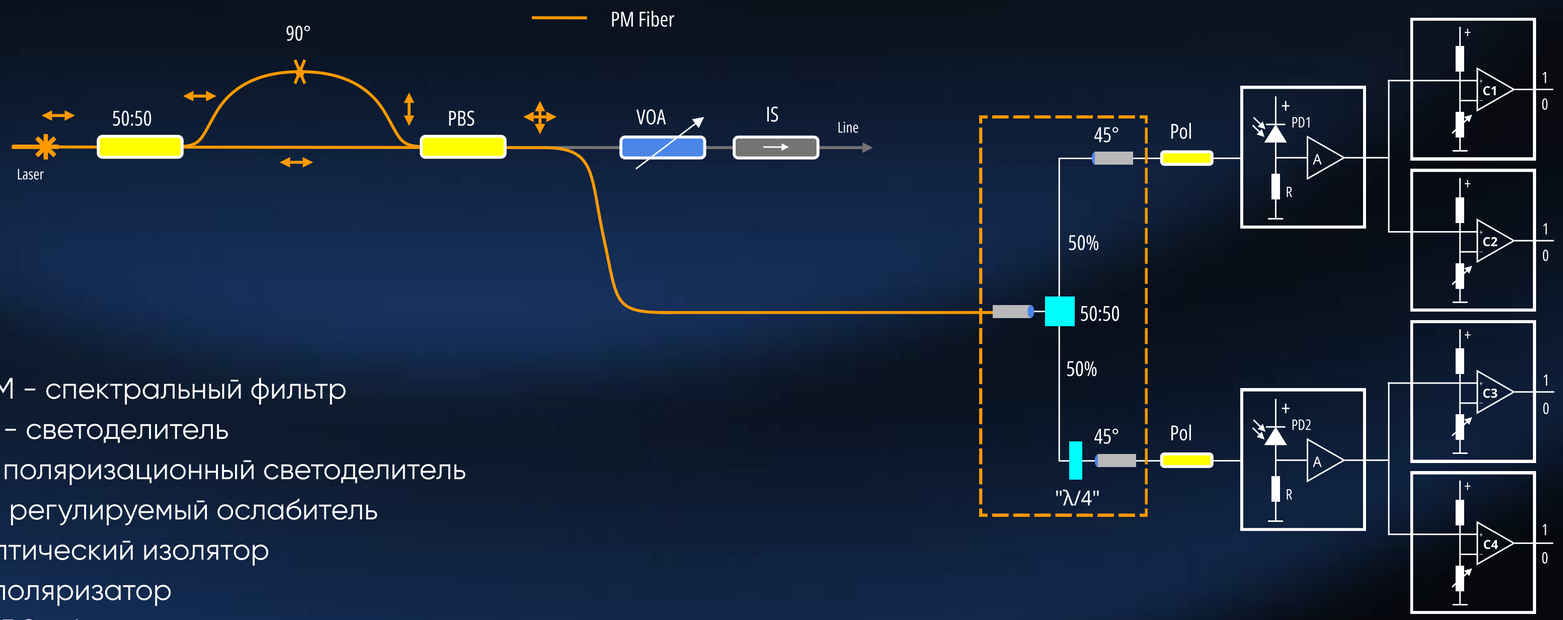


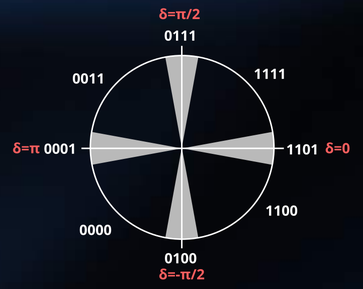
FIG. 3: Graphical representation of the valid regions for the angle θ. These regions are marked in grey. They depend on an acceptance parameter $\Omega \in [0, \pi/4]$.

M Curty, et al. "Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals." Physical Review A 82.5 (2010): 052325.

Схема пассивного приготовления с одним лазером



DWDM - спектральный фильтр
50:50 - светоделитель
PBS - поляризационный светоделитель
VOA - регулируемый ослабитель
IS - оптический изолятор
Pol - поляризатор
PD1, PD2 - фотодиод
C1..C4 - компаратор



Срабатывание компараторов

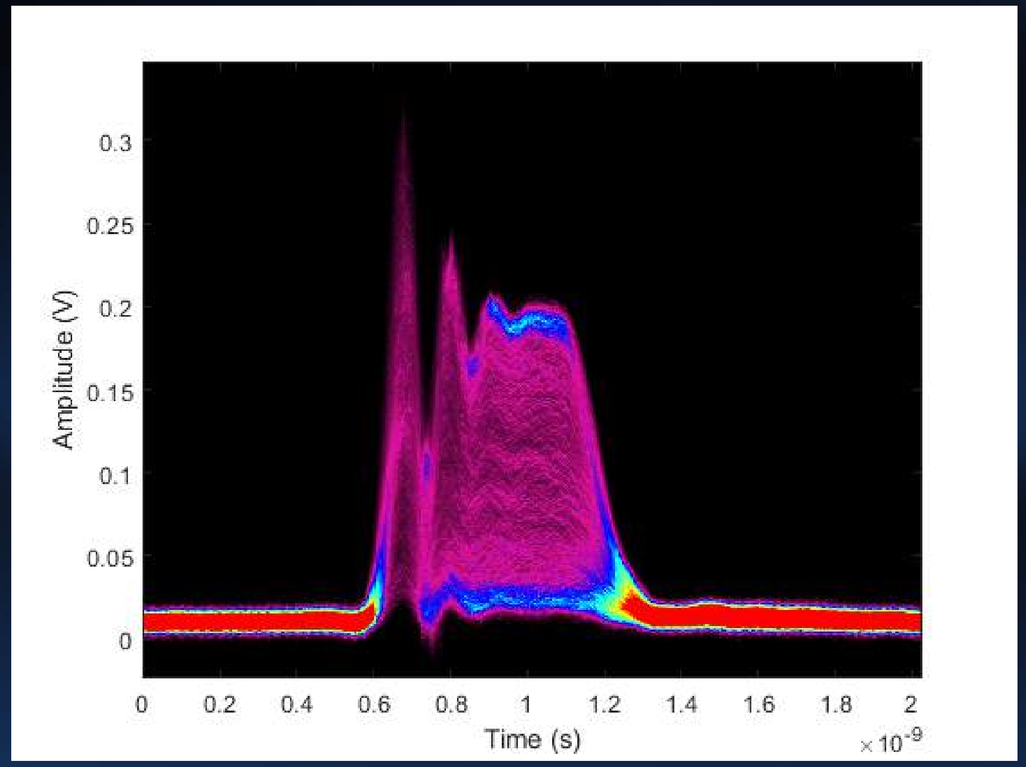
	C1	C2	C3	C4
↕	1	1	0	1
↔	0	0	0	1
↺	0	1	1	1
↻	0	1	0	0

Таблица селекции состояний

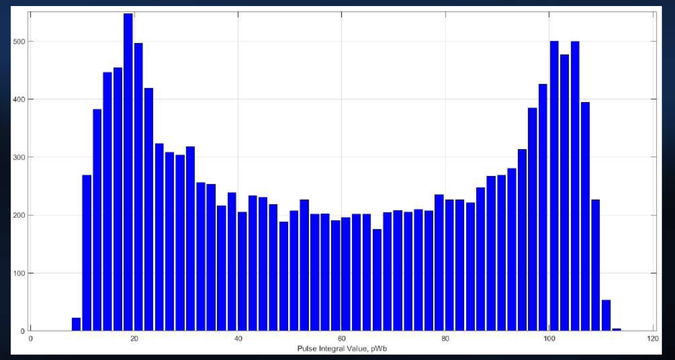
ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

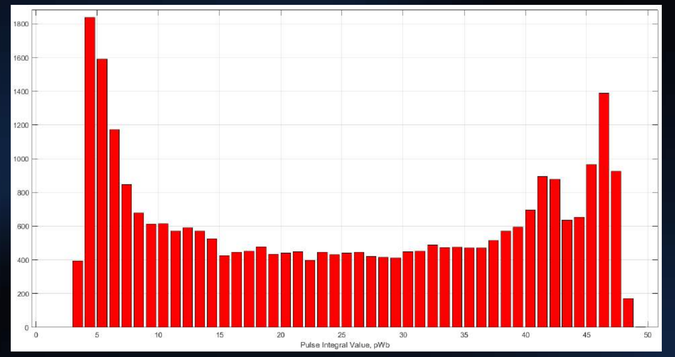
Предварительные экспериментальные результаты



Осциллограмма с наложением сигнала. Длительность импульсов 600 пс, частота следования 312 МГц.



Гистограмма по полному импульсу

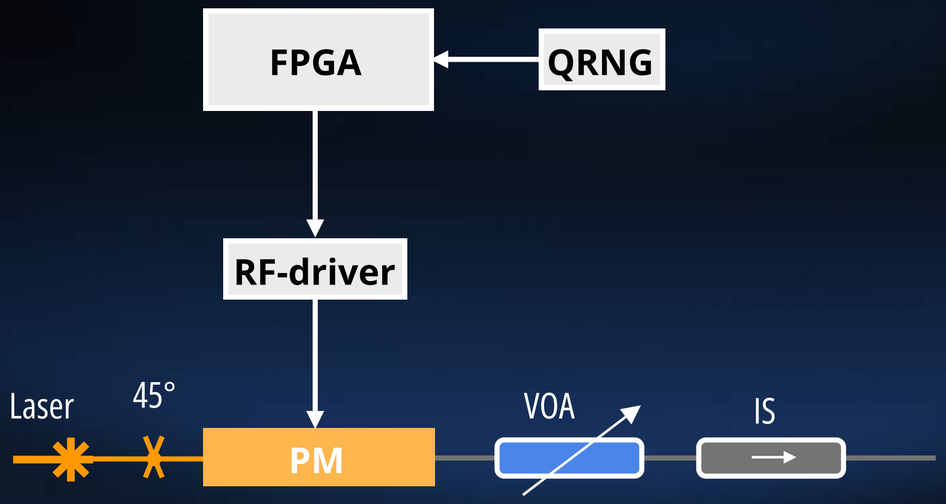


Гистограмма по задней части импульса

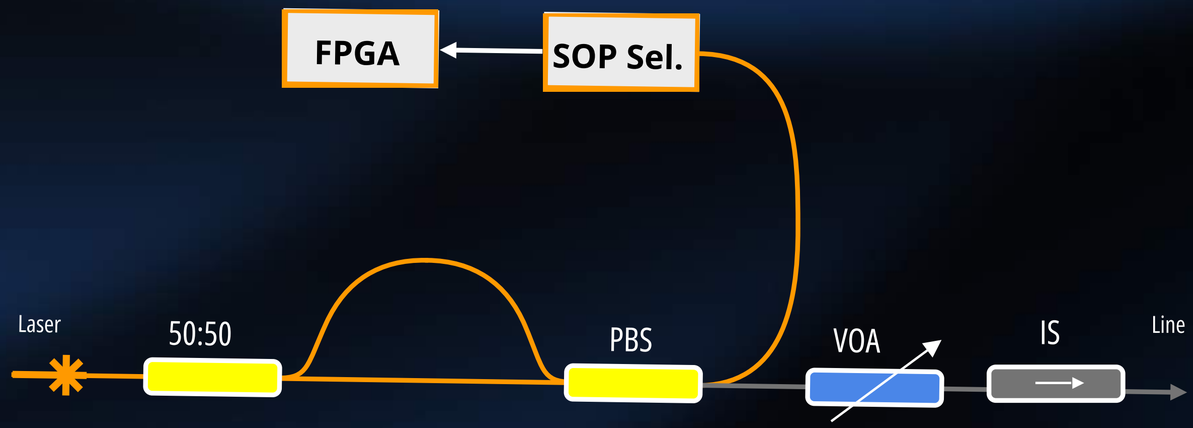
ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Более простая и секретная

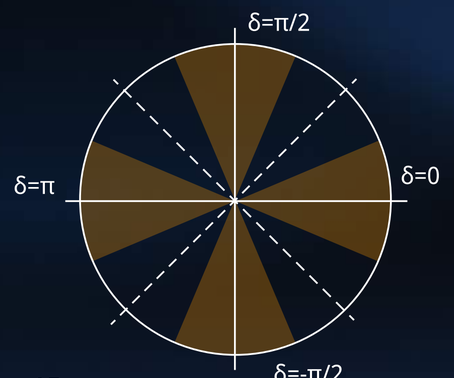


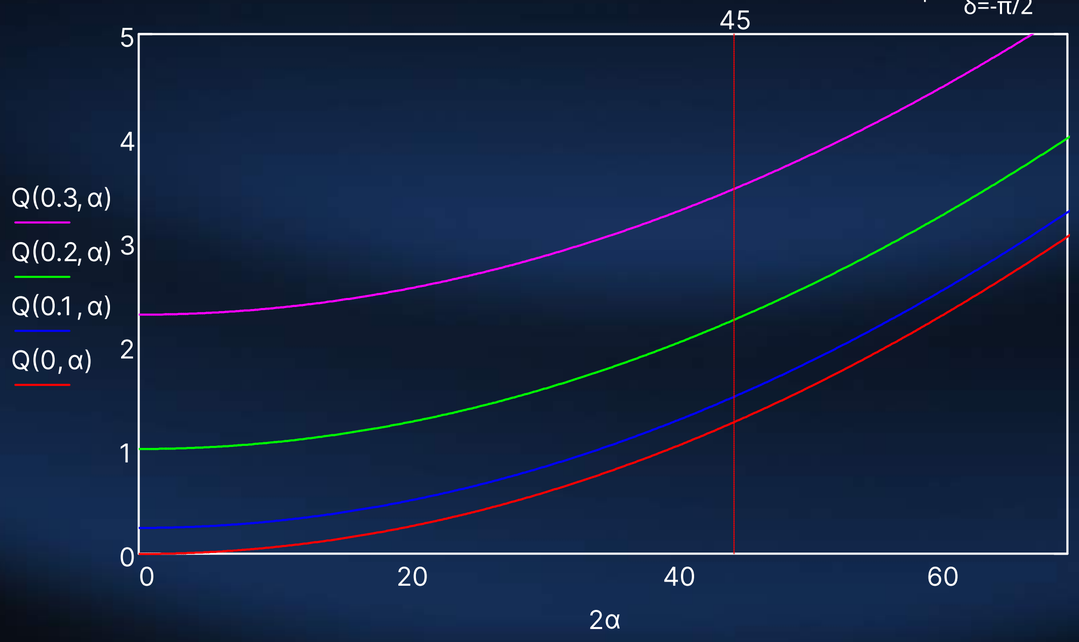
Было



Стало

Улучшение секретности





Протокол с 4-мя базисами

Недоверенный центральный узел

Защита от атак:
Superlinear detector control
Detector mismatch
Detector dead-time
Light injection in calibration photodetector
Backflash

ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE

Резюме

Ограничение дальности работы передатчика позволяет не использовать в протоколе состояния-ловушки и отказаться от применения модулятора интенсивности и обслуживающих его систем. Снижаются требования к ПЛИС и КвГСЧ.

Переход к пассивному приготовлению состояний позволяет полностью отказаться в передатчике от применения электрооптических модуляторов, ВЧ драйверов, скоростных ЦАП-ов, КвГСЧ.

Отсутствие в составе передатчика электрооптических модуляторов делает бессмысленной на них атаку типа «троянский конь». Риск атаки на лазер остается только в узком спектральном диапазоне. Секретность системы становится выше.

Передатчик с пассивным приготовлением состояний может без усложнения поддерживать протокол с 4-мя базисами и работать в системах КРК с недоверенным центральным узлом

Спасибо за внимание!

ГАЗПРОМБАНК
Банк ГПБ (АО)

QRATE