

Казанский физико-технический институт им. Е.К. Завойского  
ФИЦ Казанский научный центр РАН



Акатьев Дмитрий Олегович

**Разработка базовых устройств и протоколов квантовой связи  
на основе спонтанного параметрического рассеяния света**

Специальность 1.3.6. Оптика

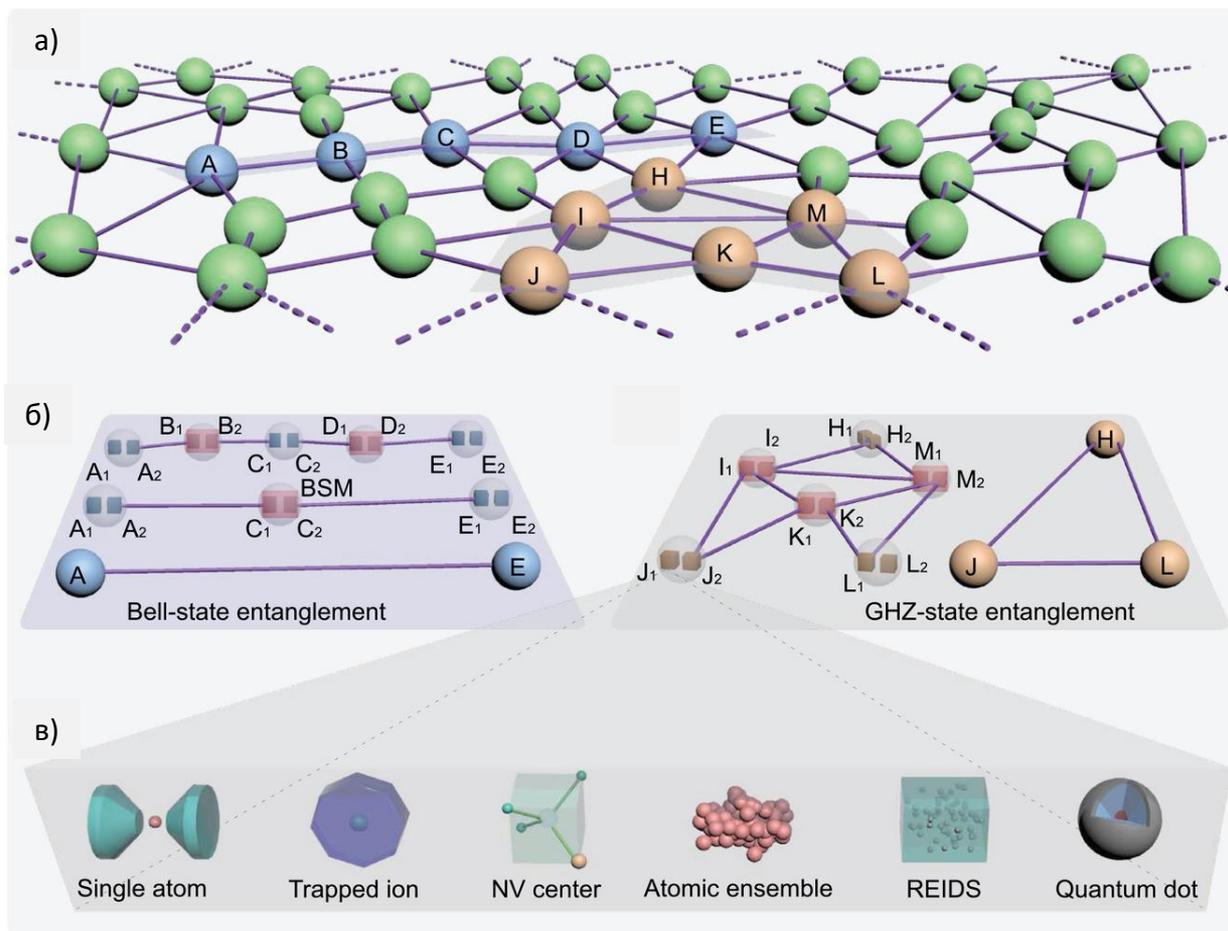
Научный руководитель:  
д. ф.-м. н., член-корр. РАН,  
Калачев Алексей Алексеевич

# План доклада

---

- Актуальность;
- Положения, выносимые на защиту;
- Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти;
- Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя;
- Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света;
- Основные результаты;
- Публикации автора по теме диссертации.

# Базовые устройства и протоколы квантовых коммуникационных сетей



Общая схема создания глобальной квантовой сети. а) Многоузловая квантовая сеть, б) схема создания перепутанности узлов, в) модели квантовой памяти .

# Базовые устройства и протоколы квантовых коммуникационных сетей

а)



## Основные устройства:

1. Источники одиночных фотонов
2. Источники перепутанных пар фотонов
3. Устройства квантовой памяти
4. Однофотонные детекторы
5. Квантовые частотные конверторы

## Базовые протоколы:

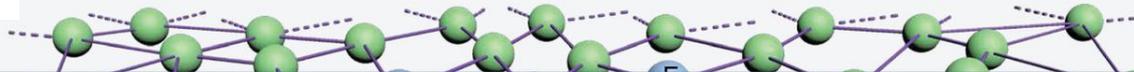
1. Протоколы квантового распределения ключа
2. Протоколы квантовой телепортации
3. Протоколы квантового повторителя
4. Протоколы квантового хеширования и т.д.

Single atom    Trapped ion    NV center    Atomic ensemble    REIDS    Quantum dot

Общая схема создания глобальной квантовой сети. а) Многоузловая квантовая сеть, б) схема создания перепутанности узлов, в) модели квантовой памяти .

# Базовые устройства и протоколы квантовых коммуникационных сетей

а)



Основные устройства:

1. **Источники одиночных фотонов**
2. Источники перепутанных пар фотонов
3. **Устройства квантовой памяти**
4. Однофотонные детекторы
5. Квантовые частотные конверторы

Базовые протоколы:

1. Протоколы квантового распределения ключа
2. Протоколы квантовой телепортации
3. Протоколы квантового повторителя
4. **Протоколы квантового хеширования и т.д.**

Single atom

Trapped ion

NV center

Atomic ensemble

REIDS

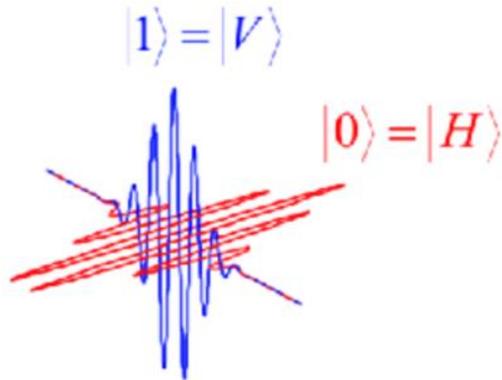
Quantum dot

Общая схема создания глобальной квантовой сети. а) Многоузловая квантовая сеть, б) схема создания перепутанности узлов, в) модели квантовой памяти .

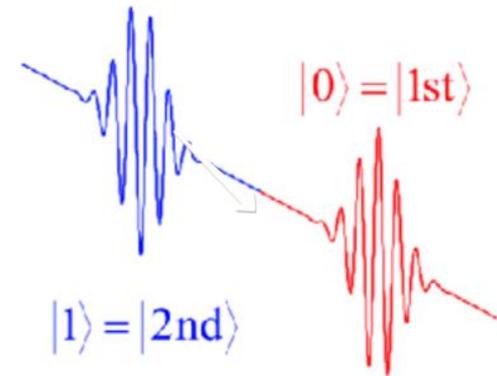
# Методы кодирования информации

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

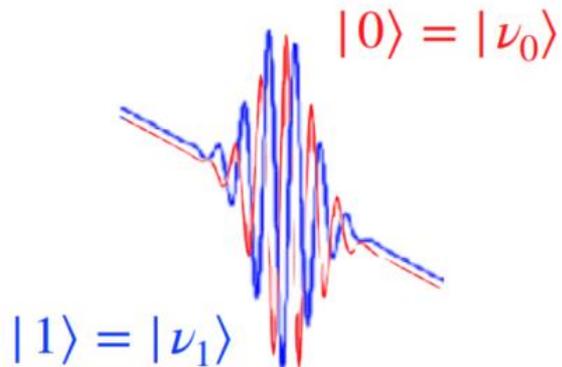
Поляризационное кодирование



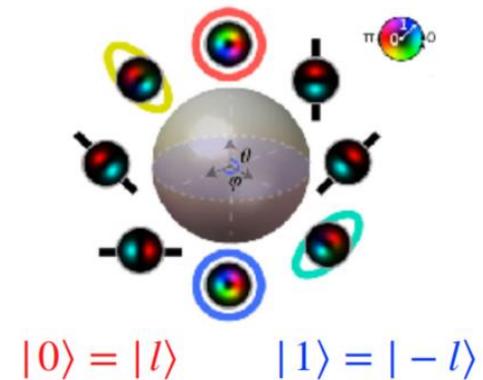
Временное кодирование



Частотное кодирование



Пространственное кодирование



# Цели и задачи

## Цели:

- Создание источников однофотонных состояний света на основе спонтанного параметрического рассеяния света, которые могут эффективно взаимодействовать с устройствами квантовой памяти и образовывать перепутанные состояния типа «квантовая память-фотон», а также разработка протоколов квантового хеширования на основе однофотонных состояний света, обладающих орбитальным угловым моментом.

## Задачи:

- Разработать экспериментальный образец источника одиночных фотонов на основе спонтанного параметрического рассеяния света в однорезонансном параметрическом генераторе света;
- Исследовать возможность объединения устройств квантовой памяти и узкополосных источников пар фотонов в общем резонаторе;
- Разработать источник многомерных однофотонных состояний света в базисе орбитального углового момента света на основе спонтанного параметрического рассеяния света.
- Разработать методику квантового хеширования на основе многомерных однофотонных состояний света.
- Исследовать свойство устойчивости к коллизиям квантовых многомерных функций хеширования на основе орбитального углового момента света.

# Положения, выносимые на защиту

---

- Спонтанное параметрическое рассеяние света позволяет создавать источники узкополосных однофотонных для квантовой памяти на основе ионов  $\text{Nd}^{3+}$ .
- Однорезонаторный параметрический генератор фотонов с квантовой памятью позволяет с высокой эффективностью формировать перепутанные состояния типа «квантовая память-фотон» в протоколах квантового повторителя.
- Использование многомерных однофотонных состояний уменьшает число квантовых носителей информации, необходимых для реализации оптимальных параметров протокола квантового хеширования.

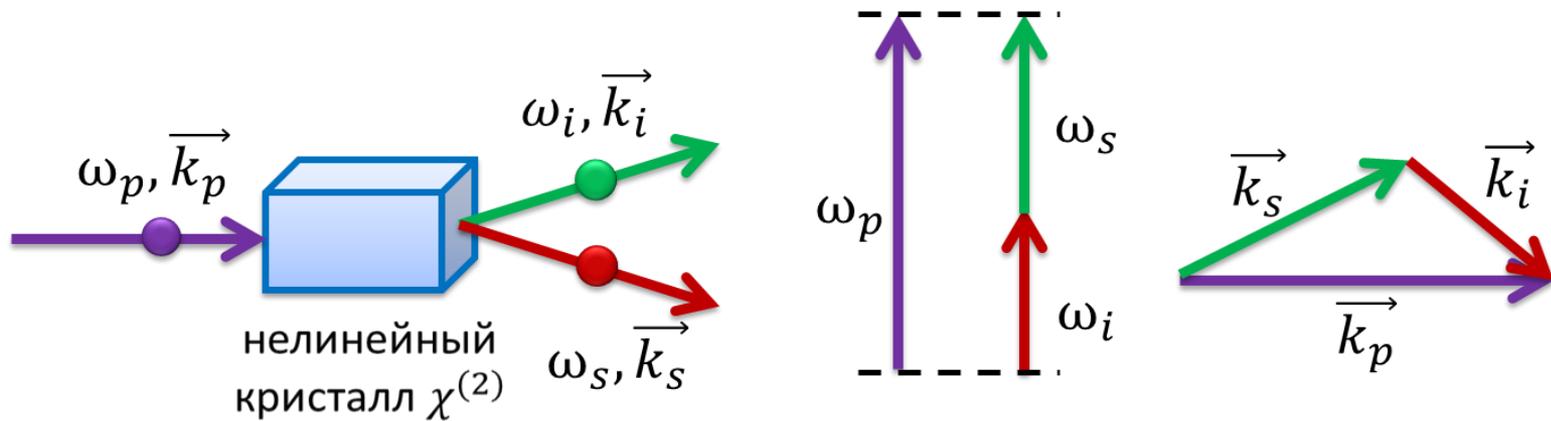
# Положения, выносимые на защиту

---

- Спонтанное параметрическое рассеяние света позволяет создавать источники узкополосных однофотонных для квантовой памяти на основе ионов  $\text{Nd}^{3+}$ .
- Однорезонаторный параметрический генератор фотонов с квантовой памятью позволяет с высокой эффективностью формировать перепутанные состояния типа «квантовая память-фотон» в протоколах квантового повторителя.
- Использование многомерных однофотонных состояний уменьшает число квантовых носителей информации, необходимых для реализации оптимальных параметров протокола квантового хеширования.

# Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти

## Спонтанное параметрическое рассеяния света



Условия фазового синхронизма

$$\omega_p = \omega_s + \omega_i,$$

$$\vec{k}_p = \vec{k}_s + \vec{k}_i.$$

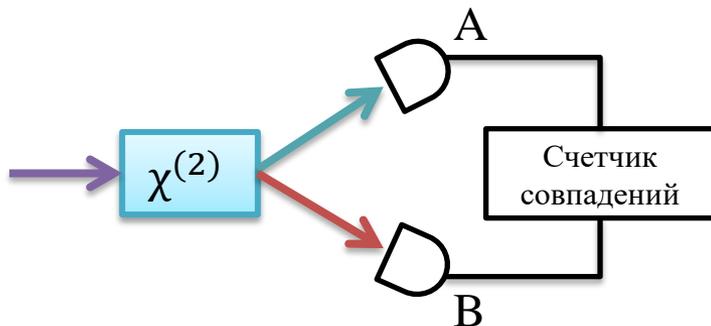
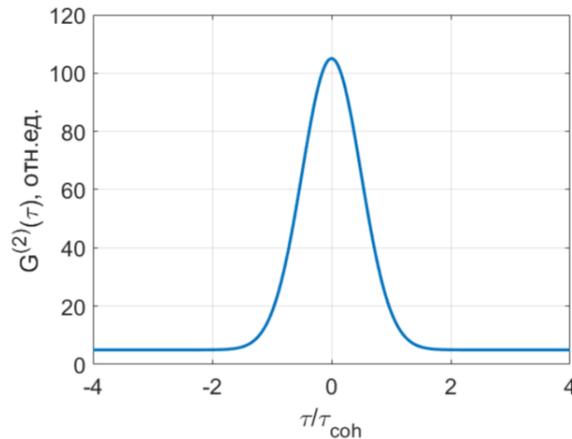
$\delta\nu_{spdc} \sim 10$  ГГц – несколько ТГц

# Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти

Кросс-корреляционная функция:

$$G^{(2)}(\tau) = \langle \Psi | E_I^{(-)}(x,t) E_S^{(-)}(x,t+\tau) E_S^{(+)}(x,t+\tau) E_I^{(+)}(x,t) | \Psi \rangle$$

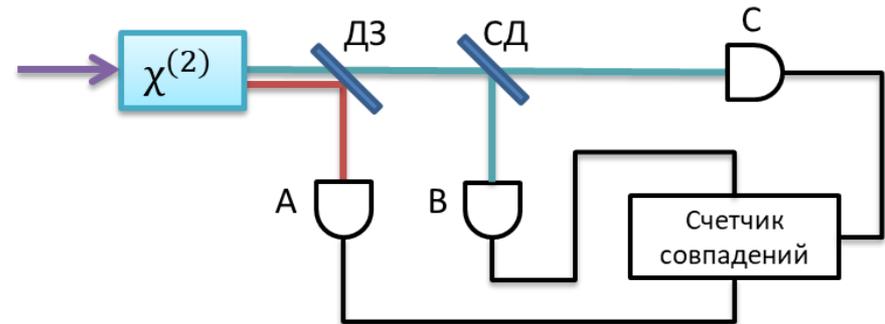
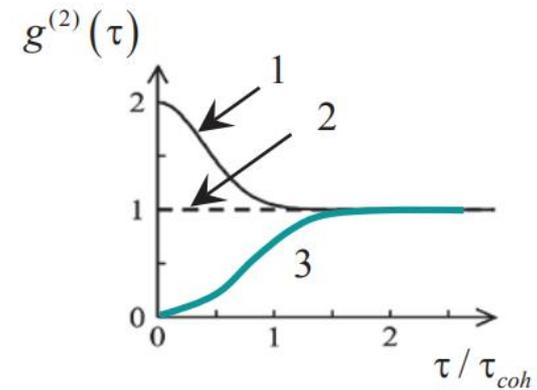
- Сигнал-шум
- Спектр бифотонного поля



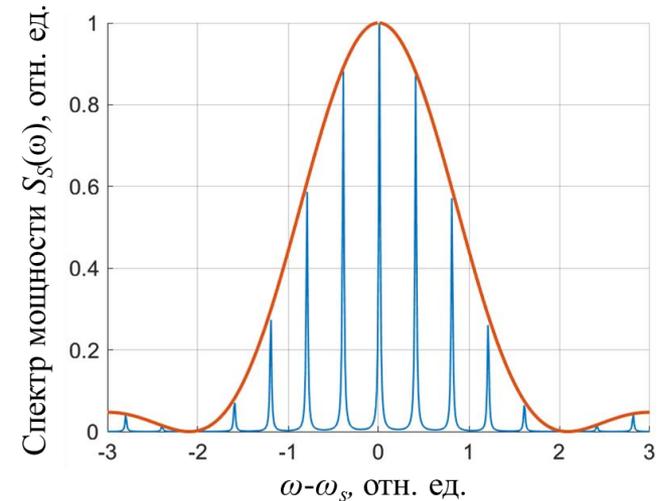
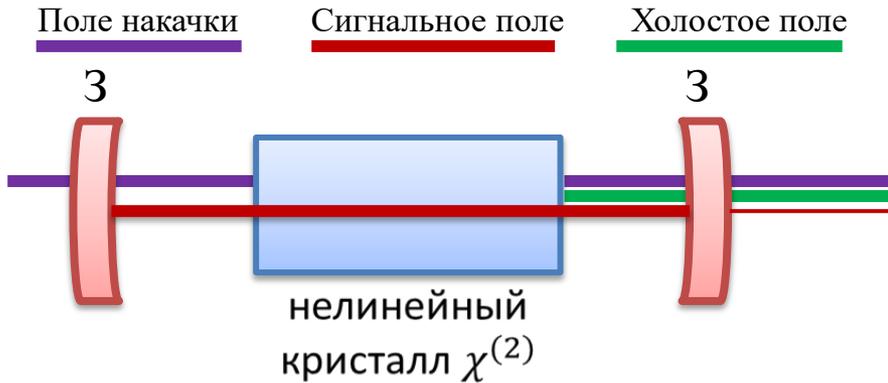
Автокорреляционная функция:

$$g^2(0) = \frac{\langle n(t)(n(t) - 1) \rangle}{\langle n(t) \rangle^2} = 1 - \frac{1}{n}$$

- Степень однофотонности



# Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти

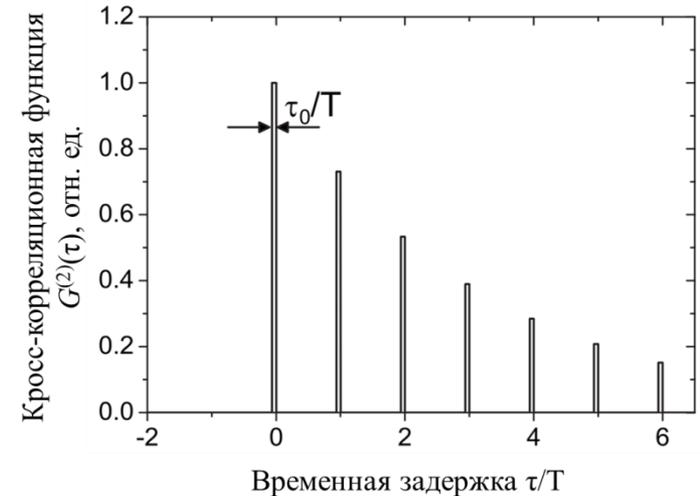


Условие частотного синхронизма:

$$\omega_p = \omega_{i,m} + \omega_{s,m}$$

$$\omega_{s,m} = \frac{(m_{s,0} + m_s)\pi c}{n_s(\omega_{s,m})L}, \text{ где } m_{s,0} = \frac{\omega_{s,0}n_s(\omega_{s,0})L}{\pi c}$$

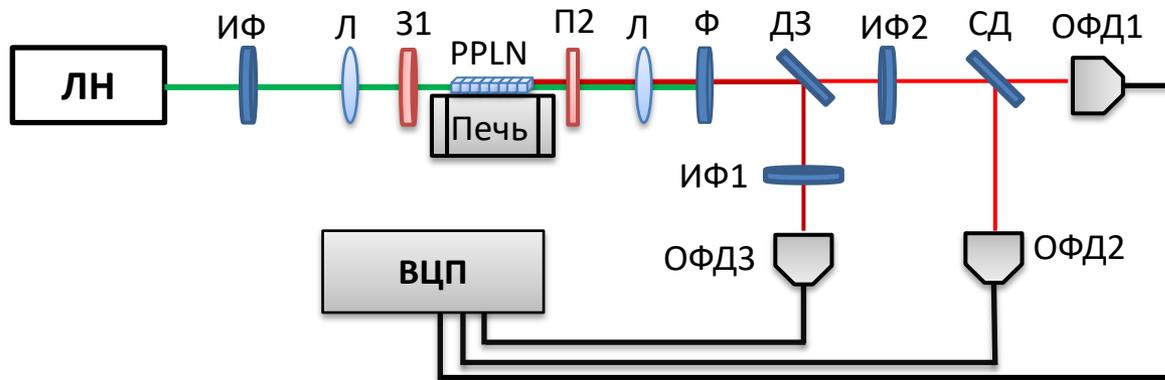
$$G^{(2)}(\tau) \sim e^{-\Gamma\tau} \left\| \sum_{-\infty}^{\infty} \text{sinc}\left(\frac{\omega_{s,m}\tau_0}{2}\right) e^{i\omega_{s,m}(\tau + \tau_0/2)} \right\|^2$$



Herzog U., Scholz M., Benson O. Theory of biphoton generation in a singleresonant optical parametric oscillator far below threshold // Physical Review A. – 2008. – Vol. 77, no. 2. – с. 023826.

Jeronimo-Moreno Y., Rodriguez-Benavides S., U'Ren A. B. Theory of cavity-enhanced spontaneous parametric downconversion // Laser physics. – 2010. – Vol. 20, no. 5. – с. 1221–1233.

# Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти

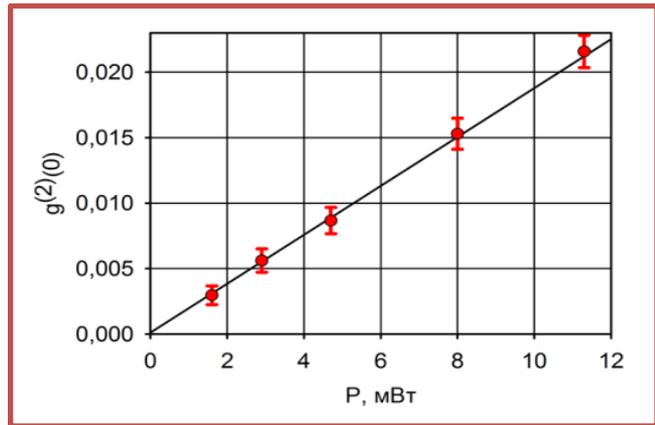
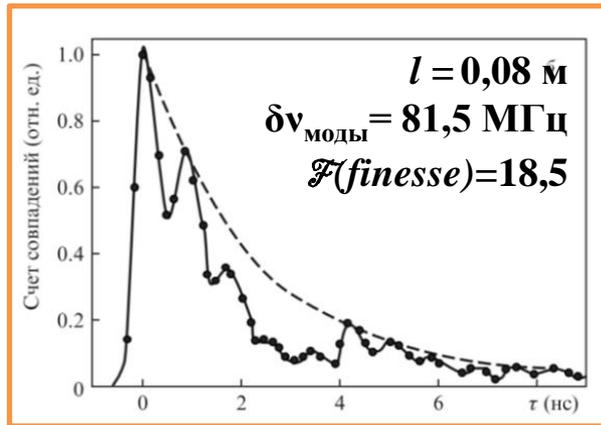
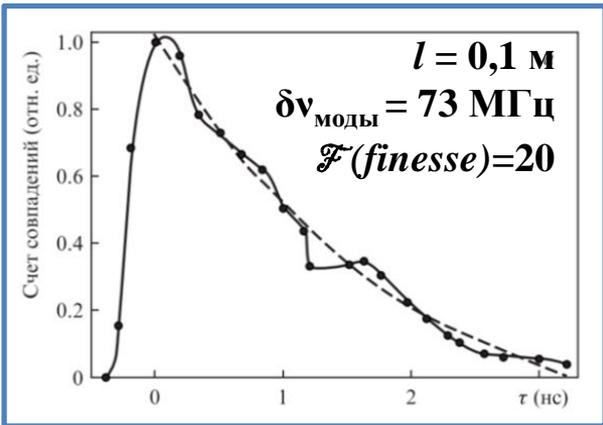


Источник узкополосных однофотонных состояний на основе однорезонаторного параметрического генератора.

$$g^{(2)}(0) = 0,004 \pm 0,001$$

Однофотонная чистота:

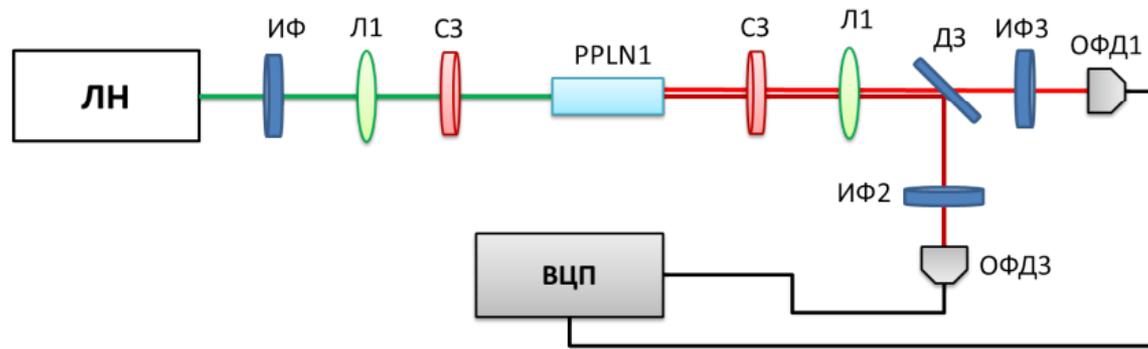
$$F = 1 - \frac{g^{(2)}(0)}{2} = 0,998 \pm 0,0005$$



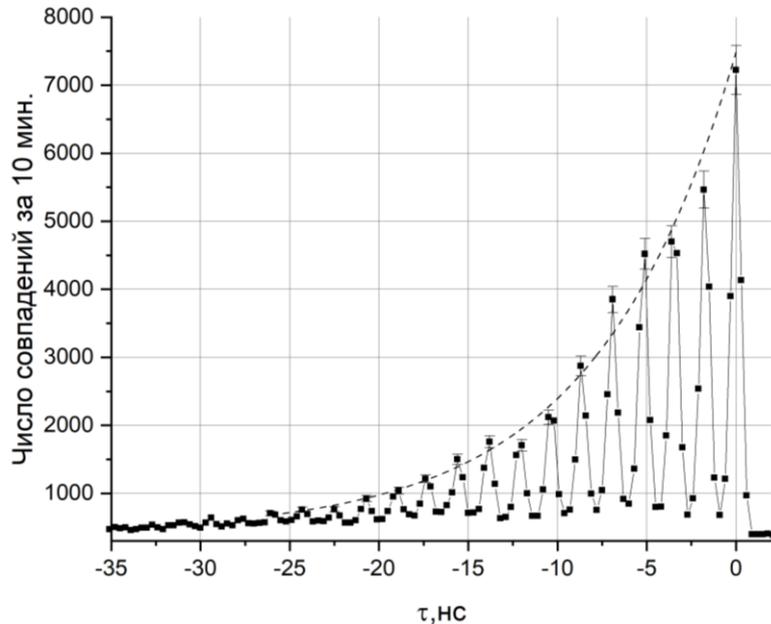
Кросс-корреляционная функция второго порядка  $G^{(2)}(\tau)$ .

Автокорреляционная функция второго порядка  $g^{(2)}(\tau)$  в зависимости от мощности накачки  $P$ .

# Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти



Модернизированный источник узкополосных однофотонных состояний



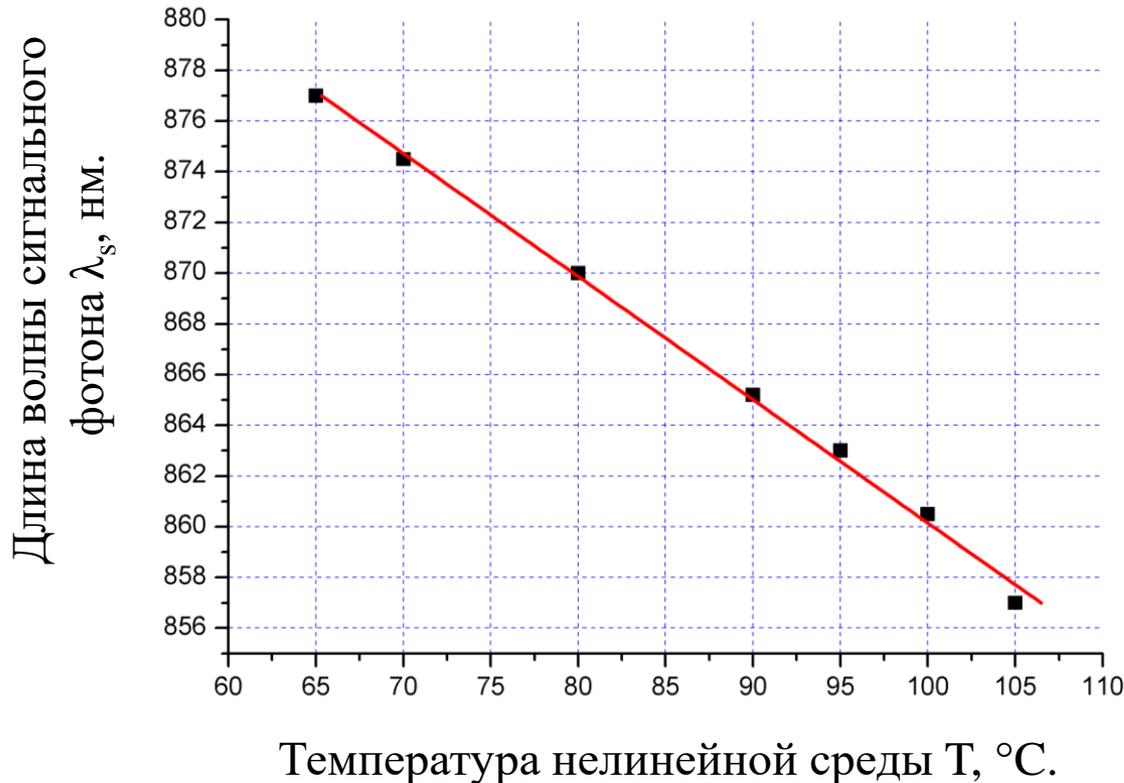
$$l = 0,232 \text{ м}$$

$$\Delta\nu_{\text{моды}} = 19 \pm 1,5 \text{ МГц}$$

$$\mathcal{F} = 30,8$$

Кросс-корреляционная функция второго порядка  $G^{(2)}(\tau)$ .

# Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти



$$\frac{d\lambda_s}{dT} \approx -0,5 \text{ нм/град}$$

YLiF<sub>4</sub>:Nd<sup>3+</sup> – 867 нм

Y<sub>2</sub>SiO<sub>5</sub>:Nd<sup>3+</sup> – 883 нм

CaWO<sub>4</sub>:Nd<sup>3+</sup> – 876 нм

Красная линия – теоретическая длина волны сигнального фотона  $\lambda_s$ ,  
 квадраты – экспериментально измеренные значения длины волны  $\lambda_s$ .

$$k_p(\lambda_p, n_p(\lambda_p, T)) = k_s(\lambda_s, n_s(\lambda_s, T)) + k_i(\lambda_i, n_i(\lambda_i, T)) + \frac{2\pi}{\Lambda(T)}$$

# Узкополосные источники света на основе спонтанного параметрического рассеяния света для устройств квантовой памяти

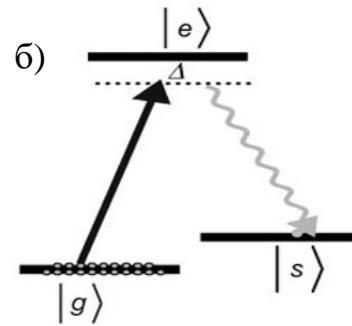
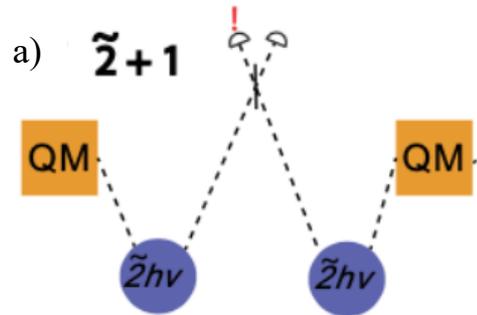
- На основе спонтанного параметрического рассеяния света в параметрическом генераторе света реализован перестраиваемый источник узкополосных однофотонных состояний света, которые совместимы с устройствами квантовой памяти на основе  $\text{Nd}^{3+}$  в различных диэлектрических матрицах;
- Ширина спектральной линии  $\delta\nu_{\text{моды}} = 19 \pm 1,5$  МГц ;
- Автокорреляционная функция второго порядка  $g^{(2)}(0) = 0,004 \pm 0,001$  при  $P = 2$  мВт;
- Температурный перестроечный коэффициент  $\frac{d\lambda_s}{dT} \approx -0,5$  нм/град.

# Положения, выносимые на защиту

---

- Спонтанное параметрическое рассеяние света позволяет создавать источники узкополосных однофотонных для квантовой памяти на основе ионов  $\text{Nd}^{3+}$ .
- Однорезонаторный параметрический генератор фотонов с квантовой памятью позволяет с высокой эффективностью формировать перепутанные состояния типа «квантовая память-фотон» в протоколах квантового повторителя.
- Использование многомерных однофотонных состояний уменьшает число квантовых носителей информации, необходимых для реализации оптимальных параметров протокола квантового хеширования.

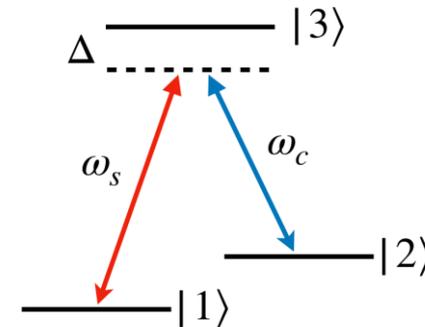
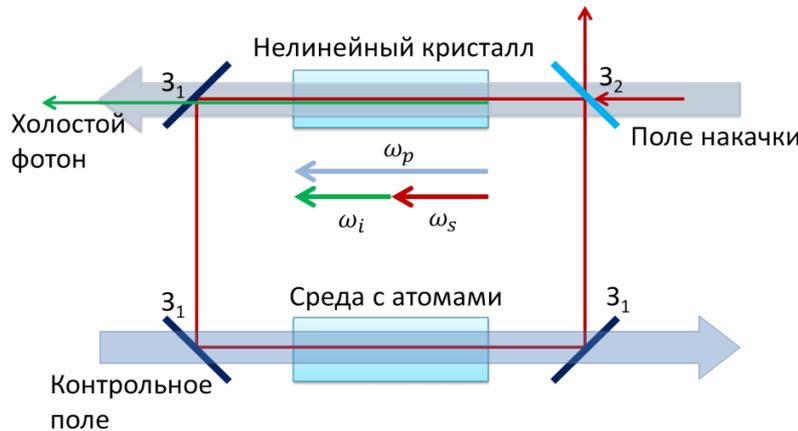
# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



$$\frac{1}{\sqrt{2}}(|g\rangle|s\rangle + |s\rangle|g\rangle)$$

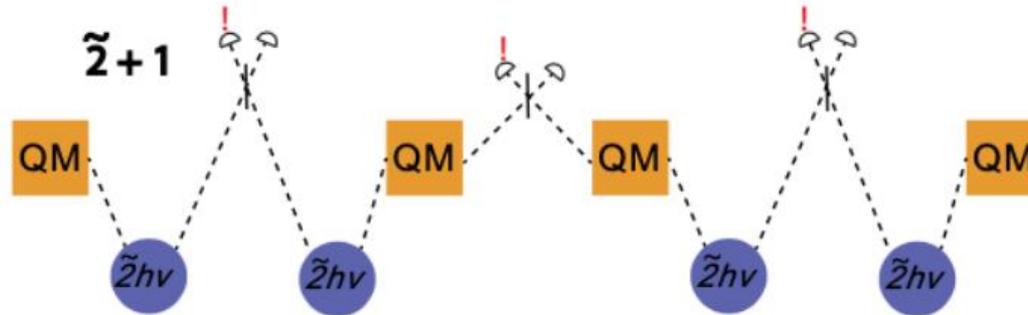
а) Схема создания перепутанного состояния между двумя устройствами квантовой памяти. б) Рамановская схема уровней атомных ансамблей. QM – устройство квантовой памяти на атомных ансамблях,  $\tilde{2}h\nu$  – двухфотонный источник.

Quantum Repeaters with Photon Pair Sources and Multimode Memories / C. Simon [et al.] // Phys. Rev. Lett. – 2007. – Vol. 98, No 19. – P. 190503.



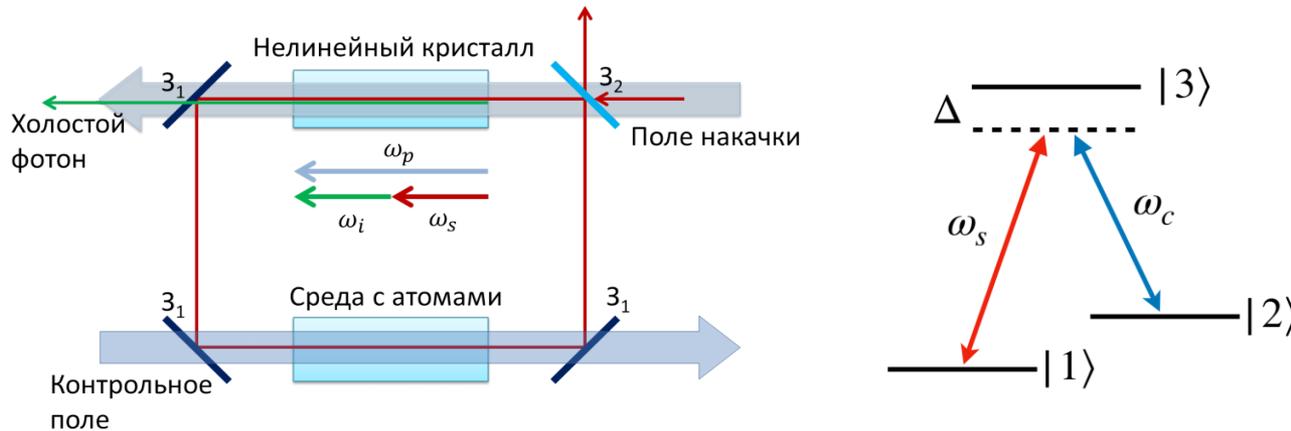
Модель источника перепутанных состояний «квантовая память-фотон», реализуемого с помощью объединения однорезонансного ПГС и УКП (среда с атомами) в общем кольцевом резонаторе.

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



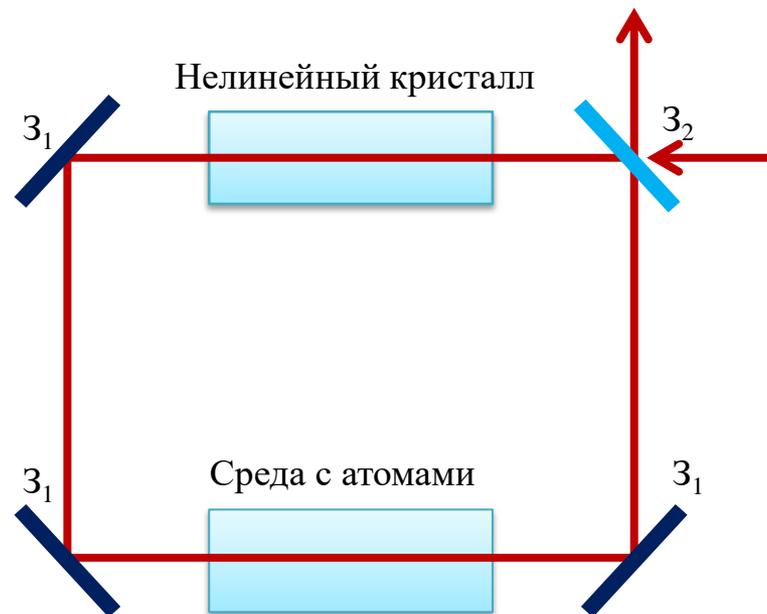
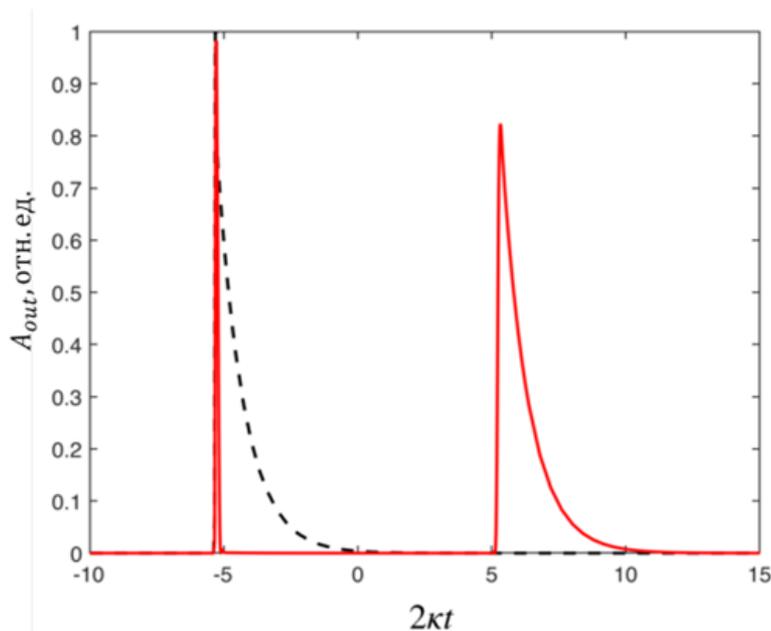
а) Схема создания перепутанного состояния между двумя устройствами квантовой памяти. б) Рамановская схема уровней атомных ансамблей. QM – устройство квантовой памяти на атомных ансамблях,  $\tilde{2}h\nu$  – двухфотонный источник.

Quantum Repeaters with Photon Pair Sources and Multimode Memories / C. Simon [et al.] // Phys. Rev. Lett. – 2007. – Vol. 98, No 19. – P. 190503.



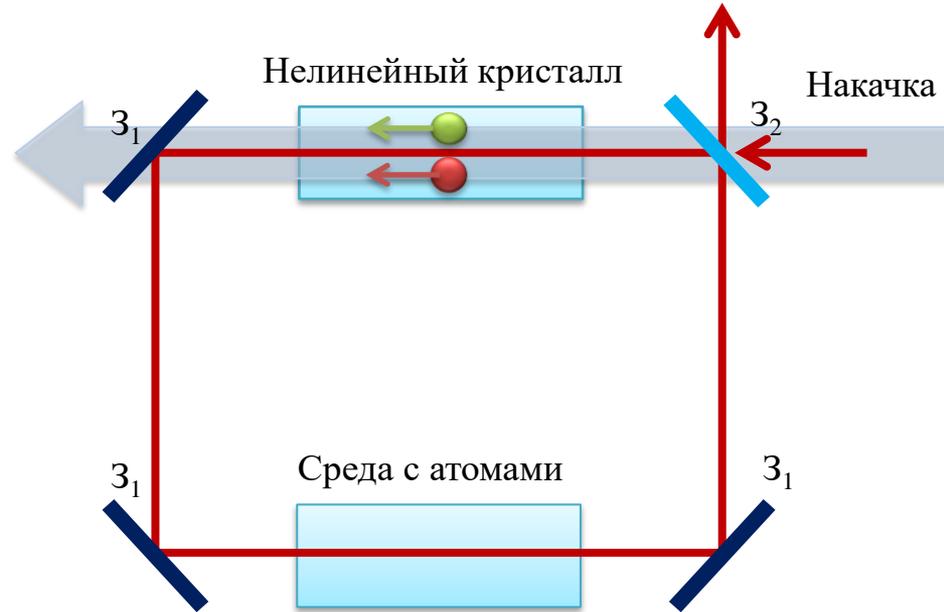
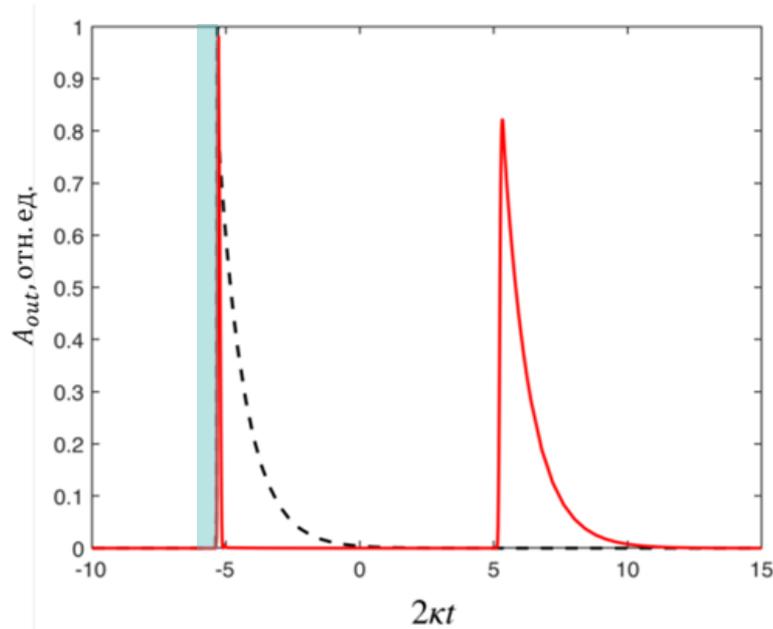
Модель источника перепутанных состояний «квантовая память-фотон», реализуемого с помощью объединения однорезонансного ПГС и УКП (среда с атомами) в общем кольцевом резонаторе.

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



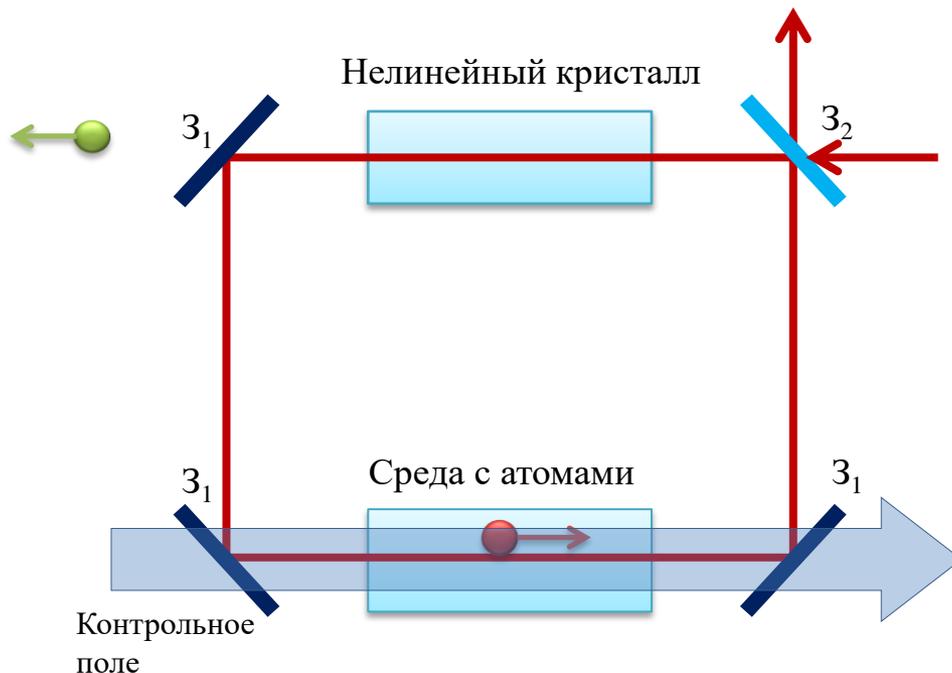
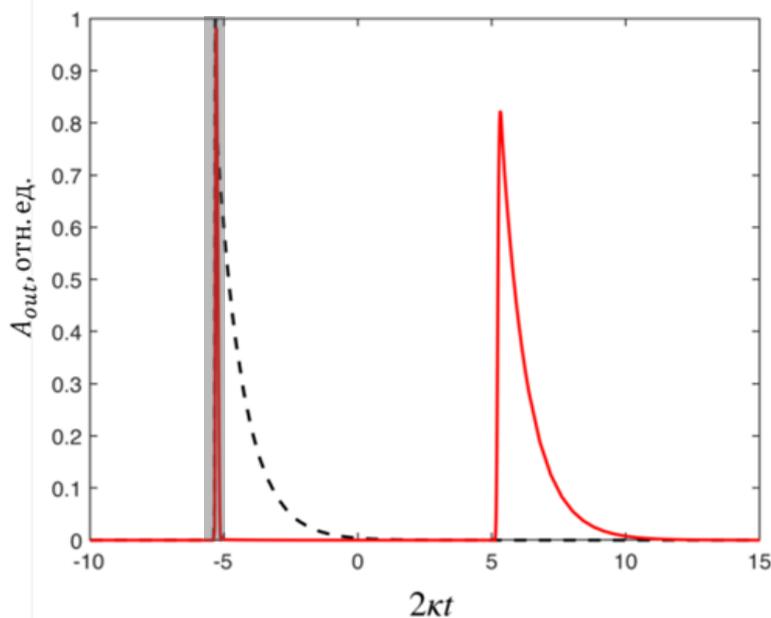
Красная кривая – поле на выходе резонатора в процессе записи и считывания слабого (однофотонного) сигнального поля под действием контрольного поля, пунктирная кривая – поле на выходе резонатора в отсутствие контрольного поля. Контрольное поле (серые прямоугольники) действует в момент  $-T$  и  $T$ .

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



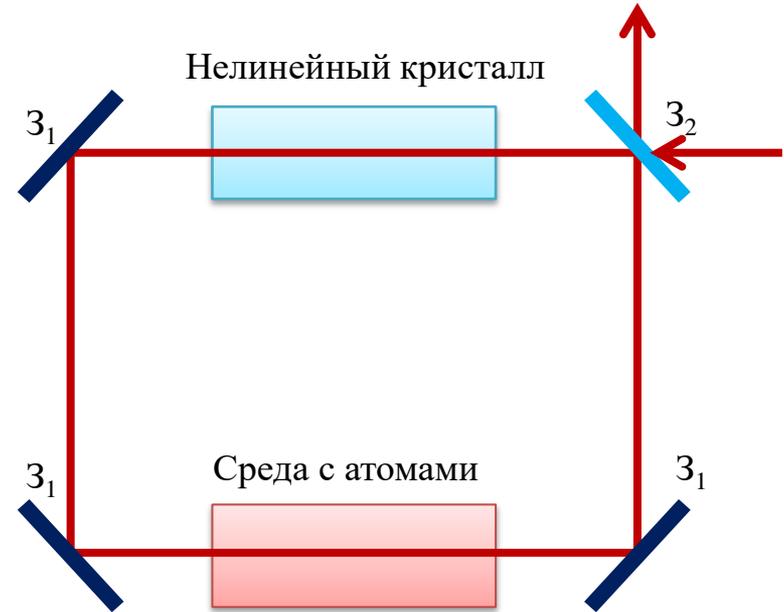
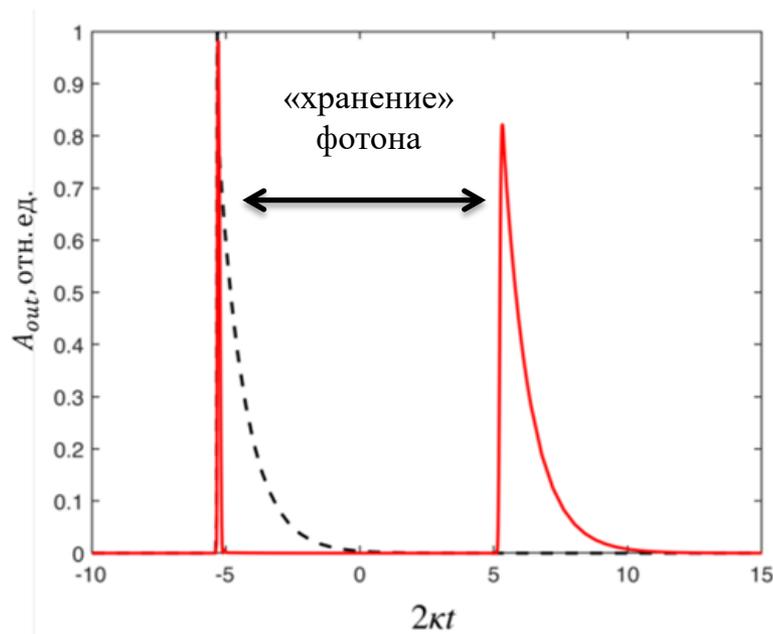
Красная кривая – поле на выходе резонатора в процессе записи и считывания слабого (однофотонного) сигнального поля под действием контрольного поля, пунктирная кривая – поле на выходе резонатора в отсутствие контрольного поля. Контрольное поле (серые прямоугольники) действует в момент  $-T$  и  $T$ .

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



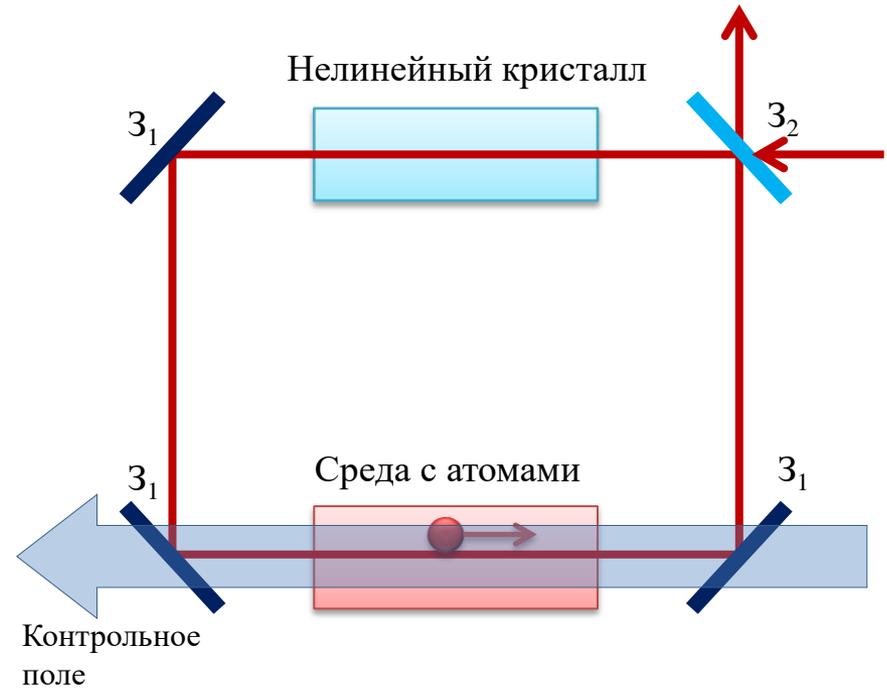
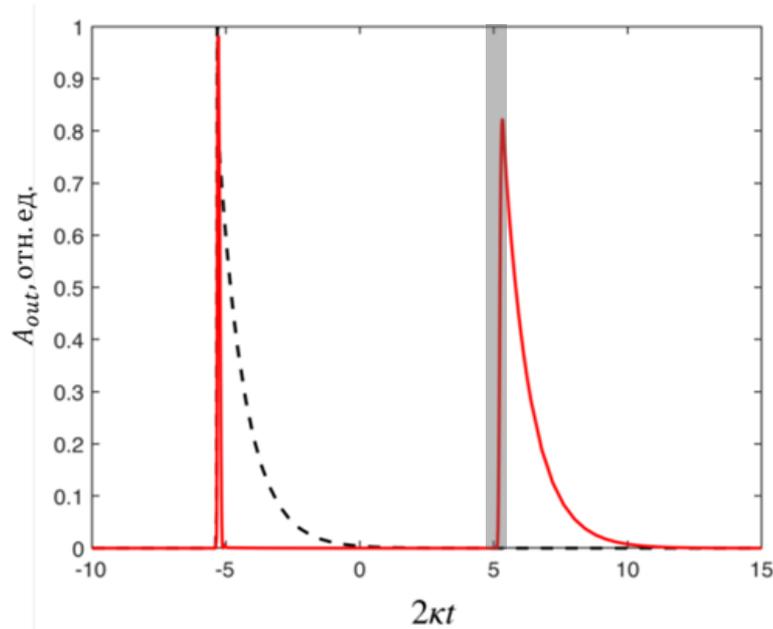
Красная кривая – поле на выходе резонатора в процессе записи и считывания слабого (однофотонного) сигнального поля под действием контрольного поля, пунктирная кривая – поле на выходе резонатора в отсутствие контрольного поля. Контрольное поле (серые прямоугольники) действует в момент  $-T$  и  $T$ .

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



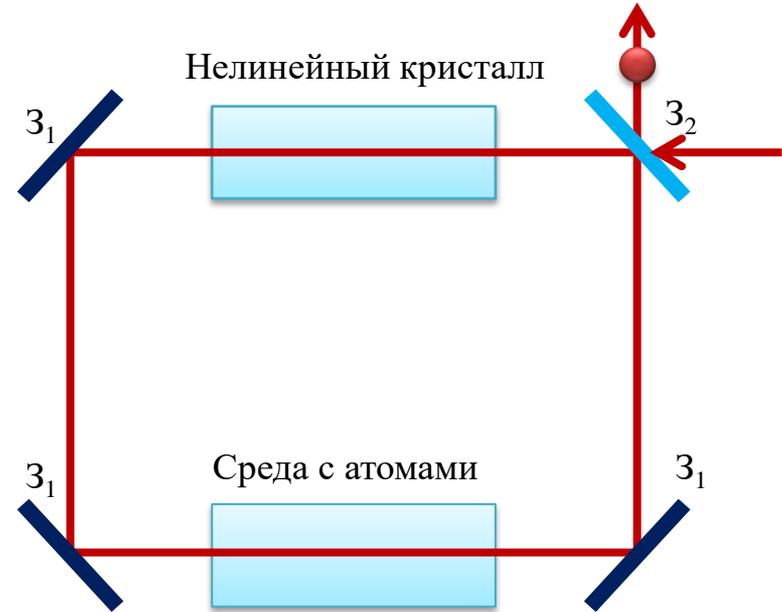
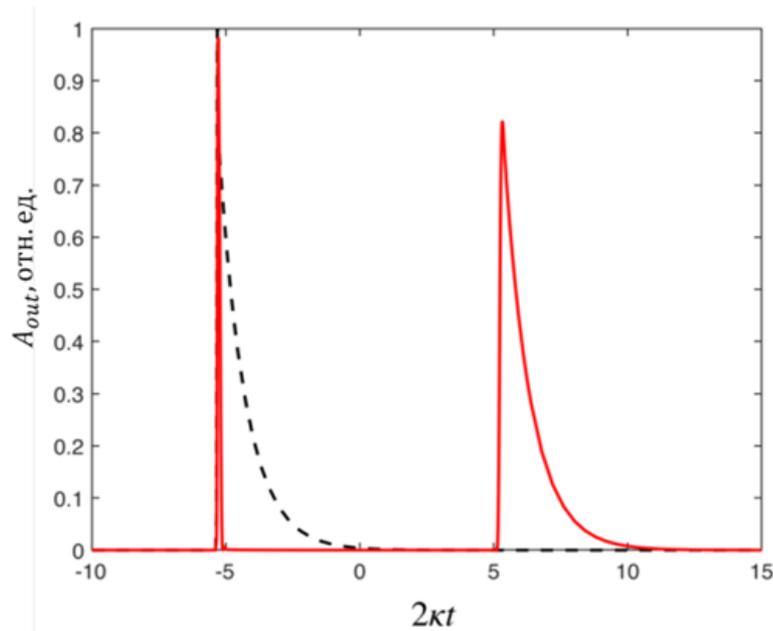
Красная кривая – поле на выходе резонатора в процессе записи и считывания слабого (однофотонного) сигнального поля под действием контрольного поля, пунктирная кривая – поле на выходе резонатора в отсутствие контрольного поля. Контрольное поле (серые прямоугольники) действует в момент  $-T$  и  $T$ .

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



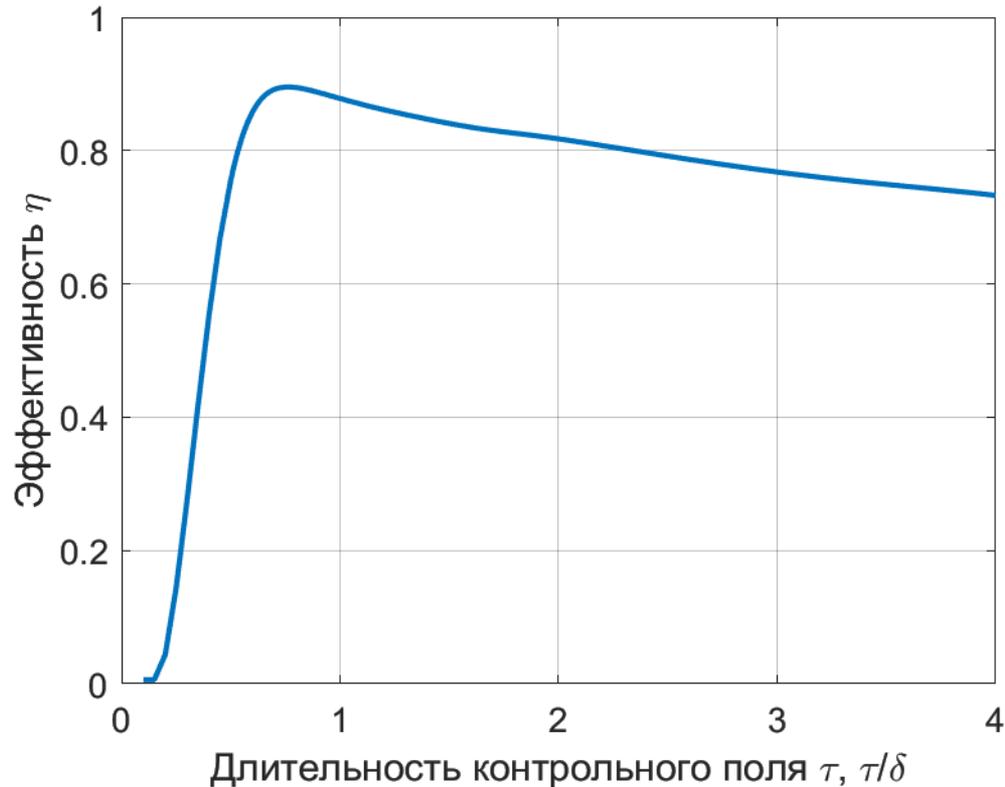
Красная кривая – поле на выходе резонатора в процессе записи и считывания слабого (однофотонного) сигнального поля под действием контрольного поля, пунктирная кривая – поле на выходе резонатора в отсутствие контрольного поля. Контрольное поле (серые прямоугольники) действует в момент  $-T$  и  $T$ .

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



Красная кривая – поле на выходе резонатора в процессе записи и считывания слабого (однофотонного) сигнального поля под действием контрольного поля, пунктирная кривая – поле на выходе резонатора в отсутствие контрольного поля. Контрольное поле (серые прямоугольники) действует в момент  $-T$  и  $T$ .

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя



Эффективность процесса записи и считывания слабого сигнального поля в зависимости от длительности контрольного поля  $\tau$ .  $1/\delta$  – эффективное неоднородное уширение рамановского перехода.

$$C = \kappa_{at}/\kappa=25 \rightarrow \eta_{max} = \left(\frac{C}{1+C}\right)^2 \approx 0.92$$

# Источник узкополосных однофотонных состояний и квантовая память для устройства квантового повторителя

---

- Исследована возможность генерации перепутанных состояний типа «квантовая память-фотон» на основе совмещения узкополосного источника одиночных состояний света и квантовой памяти в общем резонаторе;
- Получено, что максимальная эффективность цикла записи и считывания сигнального импульса  $\eta = 0,88$  достигается при длительности гауссова импульса контрольного поля  $\tau = 0,77\delta$ , где  $\delta$  – неоднородное время жизни рамановского перехода.

# Положения, выносимые на защиту

---

- Спонтанное параметрическое рассеяние света позволяет создавать источники узкополосных однофотонных для квантовой памяти на основе ионов  $\text{Nd}^{3+}$ .
- Однорезонаторный параметрический генератор фотонов с квантовой памятью позволяет с высокой эффективностью формировать перепутанные состояния типа «квантовая память-фотон» в протоколах квантового повторителя.
- Использование многомерных однофотонных состояний уменьшает число квантовых носителей информации, необходимых для реализации оптимальных параметров протокола квантового хеширования.

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$$x = \underbrace{101011101 \dots}_{S \text{ бит}}$$



$$|\Psi(x)\rangle = \underbrace{|\psi_1(x)\rangle \otimes \dots \otimes |\psi_m(x)\rangle}_{m \text{ кудитов размерности } d}$$

$m$  кудитов размерности  $d$

- Однонаправленность:  $P_{\text{extraction}} = \frac{d^m}{2^S} \ll 1, \quad m < S$
- Устойчивость к коллизиям:  $P_{\text{collision}} = \max |\langle \Psi(x_1) | \Psi(x_2) \rangle|^2 \ll 1, \quad x_1 \neq x_2$

• Ablayev F., Vasiliev A. Cryptographic quantum hashing // Laser Physics Letters. – 2014. – т. 11, № 2. – с. 025202.

• Quantum hashing via single-photon states with orbital angular momentum / D. A. Turaykhanov [и др.] // Phys. Rev. A. – 2021. – т. 104, вып. 5. – с. 052606.

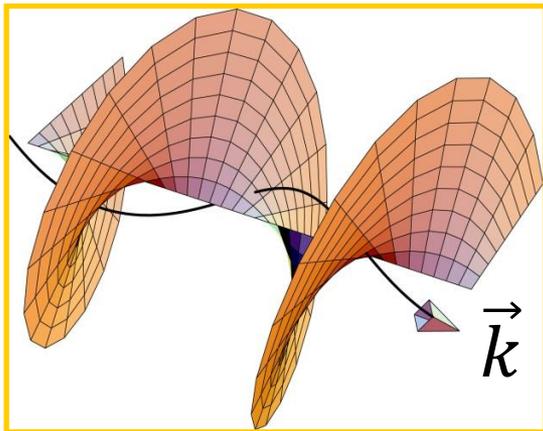
# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$$x = \underbrace{101011101 \dots}_{S \text{ бит}}$$

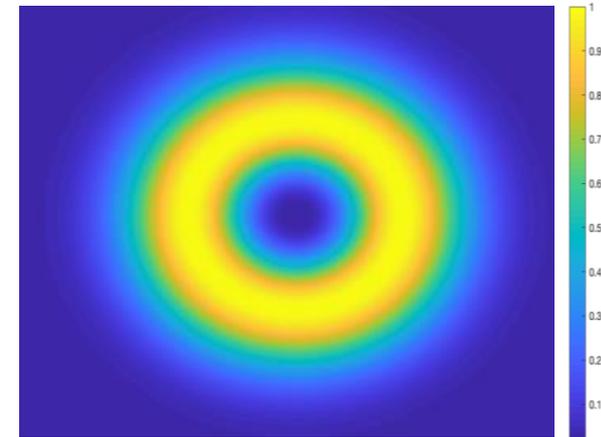
↓  
S бит

$$|\Psi(x)\rangle = |\psi_1(x)\rangle \otimes \dots \otimes |\psi_m(x)\rangle$$

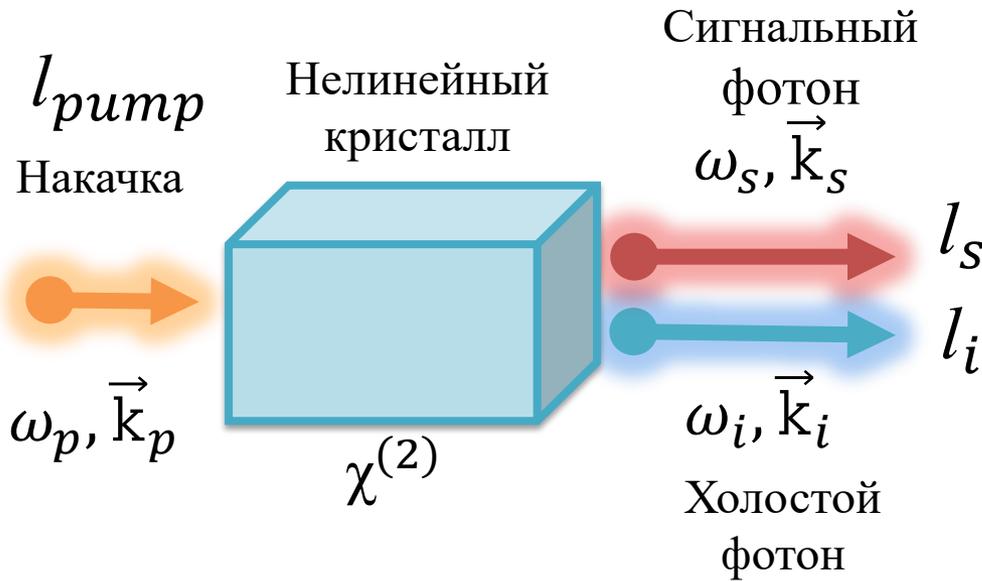
$$|\psi_m(x)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i2\pi s_{m,2}x/q}|\ell_2\rangle + \dots + e^{i2\pi s_{m,d}x/q}|\ell_d\rangle);$$



$\exp(il\varphi)$   
где  $l$  – ОУМ,  
 $\varphi$  – азимутальный угол  
 $0 \leq \varphi \leq 2\pi$



# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света



Условия фазового синхронизма:

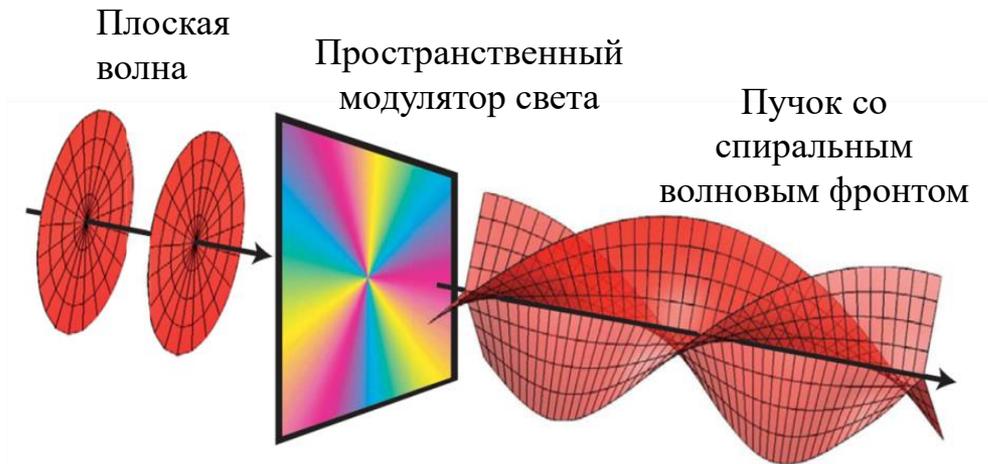
$$\omega_p = \omega_i + \omega_s$$

$$\vec{k}_p = \vec{k}_i + \vec{k}_s$$

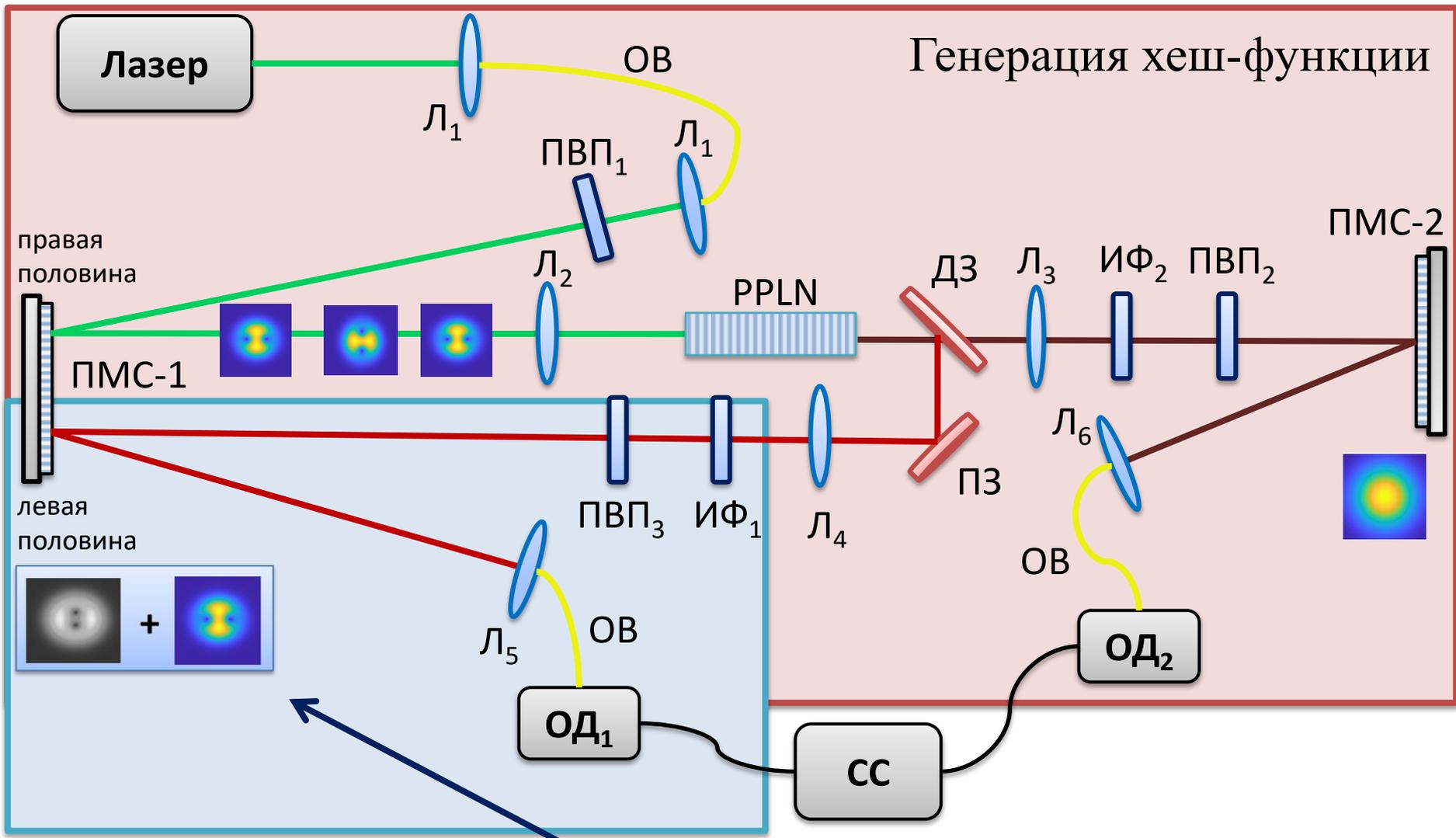
$$l_{pump} = l_s + l_i$$



$$l_i = 0 \rightarrow l_{pump} = l_s$$



# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света



Детектирование/верификация хеш-функции

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$$|\Psi(x)\rangle = |\psi_1(x)\rangle \otimes \dots \otimes |\psi_m(x)\rangle$$

$S = 8$  бит классической информации кодируется в  $m$  кудитов

$$|\psi_m(x)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i2\pi s_{m,2}x/q}|\ell_2\rangle + \dots + e^{i2\pi s_{m,d}x/q}|\ell_d\rangle),$$

$$\min_{\{s_{j,d}\}} \max_{x \neq 0} \frac{1}{d^m} \prod_{j=1}^m \left| 1 + e^{i\frac{2\pi s_{j,2}x}{q}} + \dots + e^{i\frac{2\pi s_{j,d}x}{q}} \right|^2$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$$|\Psi(x)\rangle = |\psi_1(x)\rangle \otimes \dots \otimes |\psi_m(x)\rangle$$

$S = 8$  бит классической информации кодируется в  $m$  кудитов

$$|\psi_m(x)\rangle = \frac{1}{\sqrt{d}} (|\ell_1\rangle + e^{i2\pi s_{m,2}x/q} |\ell_2\rangle + \dots + e^{i2\pi s_{m,d}x/q} |\ell_d\rangle),$$

$$|\psi_j^{d=2}(\phi_1)\rangle = \frac{1}{\sqrt{2}} (|2\rangle + e^{i\phi_1} |-2\rangle)$$

$$|\psi_j^{d=3}(\phi_2, \phi_3)\rangle = \frac{1}{\sqrt{3}} (|2\rangle + e^{i\phi_2} |-2\rangle + e^{i\phi_3} |0\rangle)$$

$$|\psi_j^{d=4}(\phi_4, \phi_5, \phi_6)\rangle = \frac{1}{\sqrt{4}} (|3\rangle + e^{i\phi_4} |-3\rangle + e^{i\phi_5} |1\rangle + e^{i\phi_6} |-1\rangle)$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$$|\psi_j^{d=2}(\phi_1)\rangle = \frac{1}{\sqrt{2}} (|2\rangle + e^{i\phi_1}|-2\rangle)$$

$$|\psi_j^{d=3}(\phi_2, \phi_3)\rangle = \frac{1}{\sqrt{3}} (|2\rangle + e^{i\phi_2}|-2\rangle + e^{i\phi_3}|0\rangle)$$

$$|\psi_j^{d=4}(\phi_4, \phi_5, \phi_5)\rangle = \frac{1}{\sqrt{4}} (|3\rangle + e^{i\phi_4}|-3\rangle + e^{i\phi_5}|1\rangle + e^{i\phi_6}|-1\rangle)$$

$$\rho_j^{exp} |\psi_j^{d=2}(\frac{2\pi}{3})\rangle = \begin{pmatrix} 0.500 \pm 0.004 & -0.251 \pm 0.001 + (0.432 \pm 0.001)i \\ -0.251 \pm 0.001 - (0.432 \pm 0.001)i & 0.499 \pm 0.004 \end{pmatrix}$$

$$F = [Tr(\sqrt{\sqrt{\rho_{target}}\rho^{exp}\sqrt{\rho_{target}}})]^2$$

$$F_{d=2} = 0.99 \pm 0.01$$

$$\lambda_{d=2} = 0.999$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$$|\psi_j^{d=2}(\phi_1)\rangle = \frac{1}{\sqrt{2}} (|2\rangle + e^{i\phi_1}|-2\rangle)$$

$$|\psi_j^{d=3}(\phi_2, \phi_3)\rangle = \frac{1}{\sqrt{3}} (|2\rangle + e^{i\phi_2}|-2\rangle + e^{i\phi_3}|0\rangle)$$

$$|\psi_j^{d=4}(\phi_4, \phi_5, \phi_5)\rangle = \frac{1}{\sqrt{4}} (|3\rangle + e^{i\phi_4}|-3\rangle + e^{i\phi_5}|1\rangle + e^{i\phi_6}|-1\rangle)$$

$$\rho_{|\psi_j^{d=3}(0,0)\rangle}^{exp} = \rho_{real}^{exp} + \rho_{imag}^{exp}$$

$$\rho_{real}^{exp} = \begin{pmatrix} 0.332 \pm 0.002 & 0.328 \pm 0.005 & 0.33 \pm 0.005 \\ 0.328 \pm 0.005 & 0.344 \pm 0.01 & 0.332 \pm 0.002 \\ 0.33 \pm 0.005 & 0.332 \pm 0.002 & 0.344 \pm 0.009 \end{pmatrix}$$

$$\rho_{imag}^{exp} = \begin{pmatrix} 0 & (0.002 \pm 0.003)i & (0.002 \pm 0.003)i \\ (-0.002 \mp 0.003)i & 0 & -(0.002 \pm 0.001)i \\ (-0.002 \mp 0.003)i & (0.002 \pm 0.001)i & 0 \end{pmatrix}$$

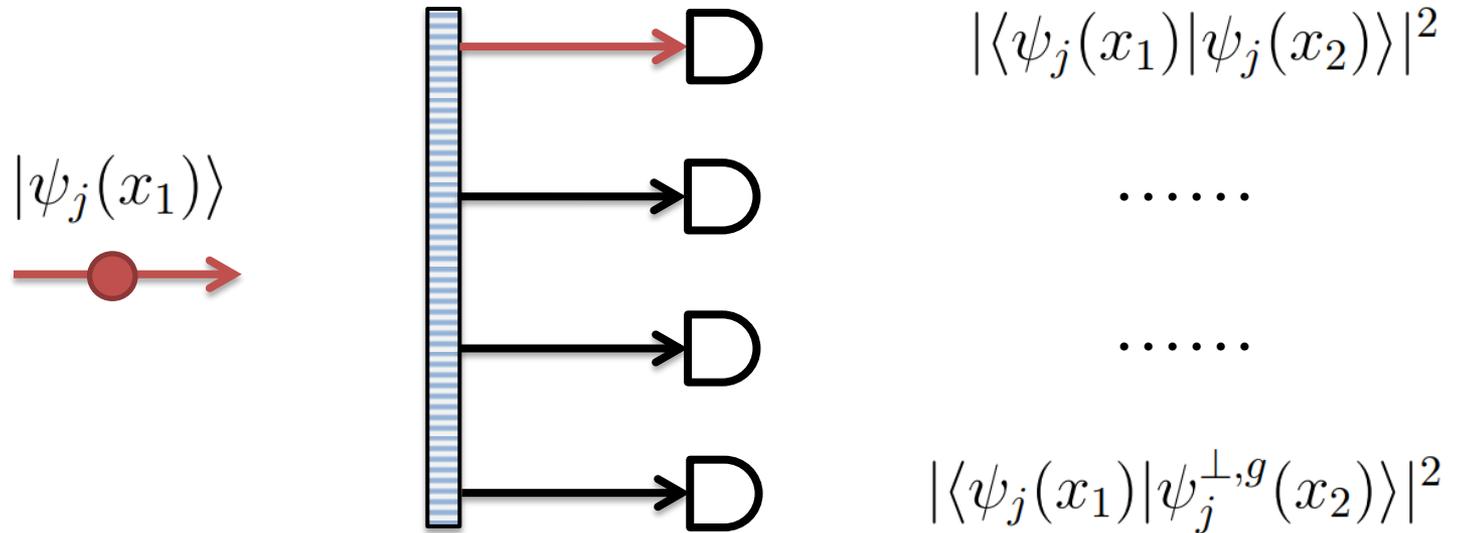
$$F_{d=3} = 0.987 \pm 0.012$$

$$\lambda_{d=3} = 0.993$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$x_1 = x_2$  или  $x_1 \neq x_2$  ?

$$|\psi_m(x)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i2\pi s_{m,2}x/q}|\ell_2\rangle + \dots + e^{i2\pi s_{m,d}x/q}|\ell_d\rangle),$$



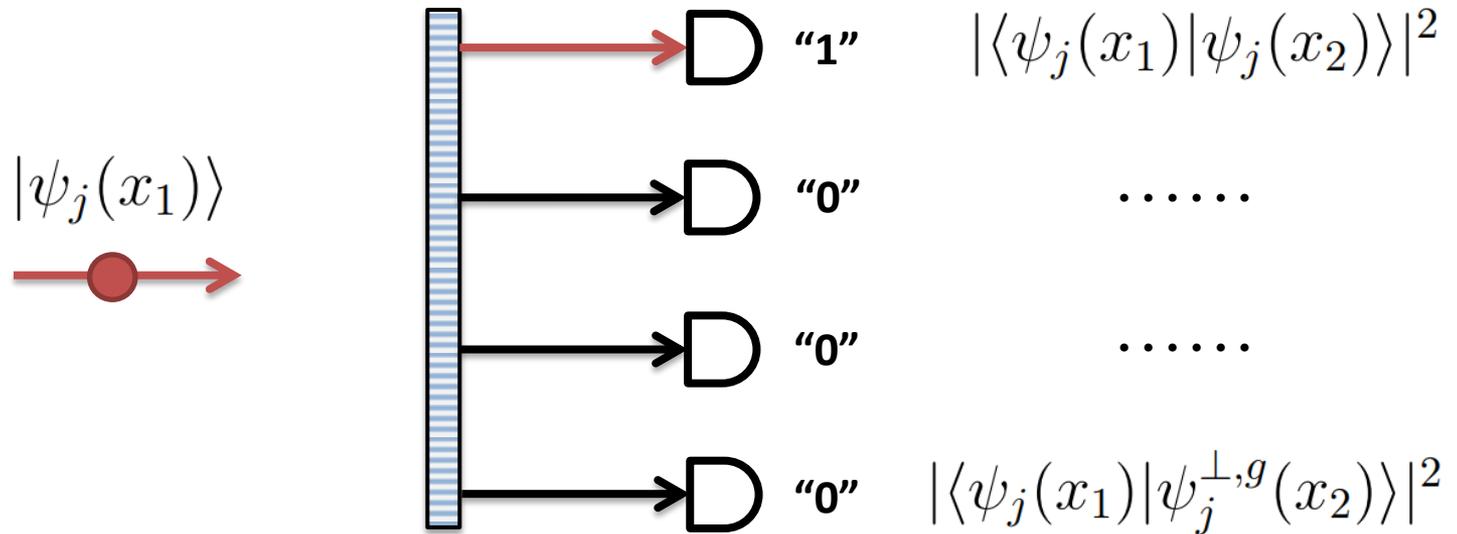
$$|\psi_j^{\perp,g}(x_2)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i\frac{2\pi s_{j,2}x_2}{q} + i\varphi_{g,2}}|\ell_2\rangle + \dots + e^{i\frac{2\pi s_{j,d}x_2}{q} + i\varphi_{g,d}}|\ell_d\rangle)$$

$$|\langle \psi_j(x_2) | \psi_j^{\perp,g}(x_2) \rangle|^2 = 0, \quad g = 1, 2, \dots, d - 1$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$x_1 = x_2$  или  $x_1 \neq x_2$  ?

$$|\psi_m(x)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i2\pi s_{m,2}x/q}|\ell_2\rangle + \dots + e^{i2\pi s_{m,d}x/q}|\ell_d\rangle),$$



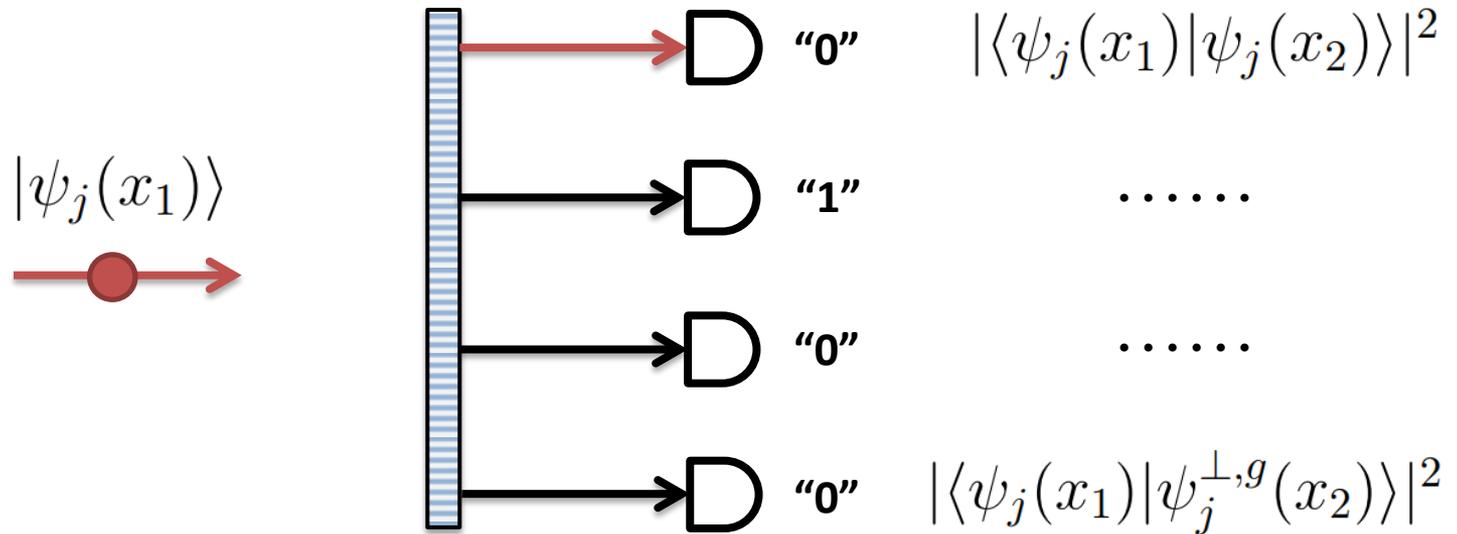
$$|\psi_j^{\perp,g}(x_2)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i\frac{2\pi s_{j,2}x_2}{q} + i\varphi_{g,2}}|\ell_2\rangle + \dots + e^{i\frac{2\pi s_{j,d}x_2}{q} + i\varphi_{g,d}}|\ell_d\rangle)$$

$$|\langle \psi_j(x_2) | \psi_j^{\perp,g}(x_2) \rangle|^2 = 0, \quad g = 1, 2, \dots, d - 1$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

$x_1 = x_2$  или  $x_1 \neq x_2$  ?

$$|\psi_m(x)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i2\pi s_{m,2}x/q}|\ell_2\rangle + \dots + e^{i2\pi s_{m,d}x/q}|\ell_d\rangle),$$



$$|\psi_j^{\perp,g}(x_2)\rangle = \frac{1}{\sqrt{d}}(|\ell_1\rangle + e^{i\frac{2\pi s_{j,2}x_2}{q} + i\varphi_{g,2}}|\ell_2\rangle + \dots + e^{i\frac{2\pi s_{j,d}x_2}{q} + i\varphi_{g,d}}|\ell_d\rangle)$$

$$|\langle \psi_j(x_2) | \psi_j^{\perp,g}(x_2) \rangle|^2 = 0, \quad g = 1, 2, \dots, d - 1$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

Наихудший случай для  $x_2 = 0$

$$x_1 = \operatorname{argmax}_{x_1 \neq 0} \frac{1}{d^{2m}} \prod_{j=1}^m \left| 1 + e^{i \frac{2\pi s_j 2x_1}{q}} + \dots + e^{i \frac{2\pi s_j d x_1}{q}} \right|^2$$

$s = 8$  – число битов,  $m$  – число кудитов

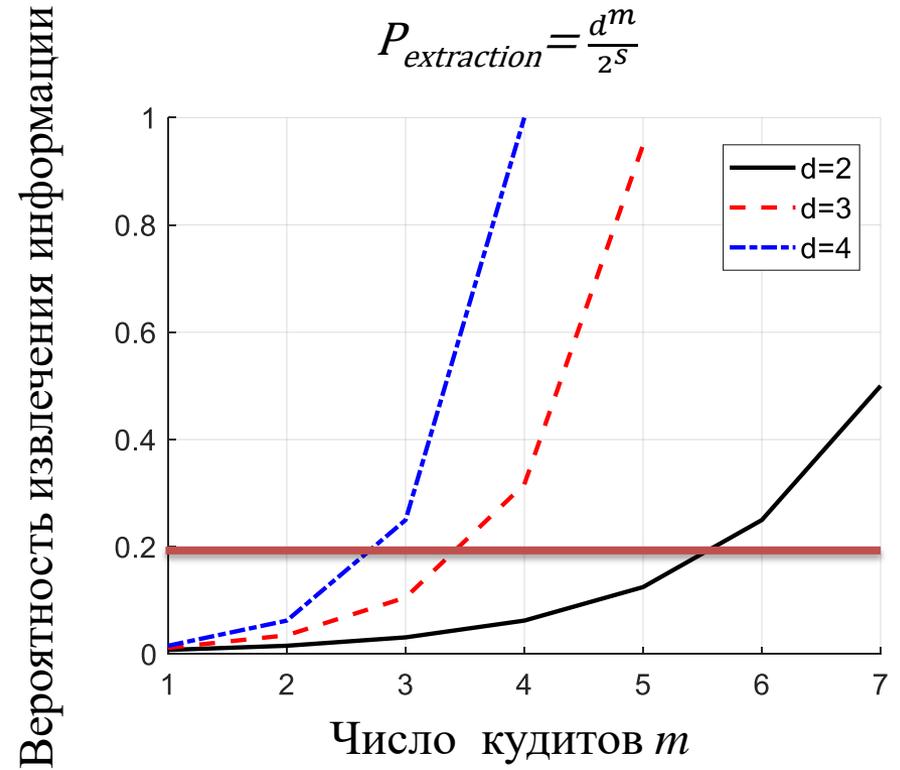
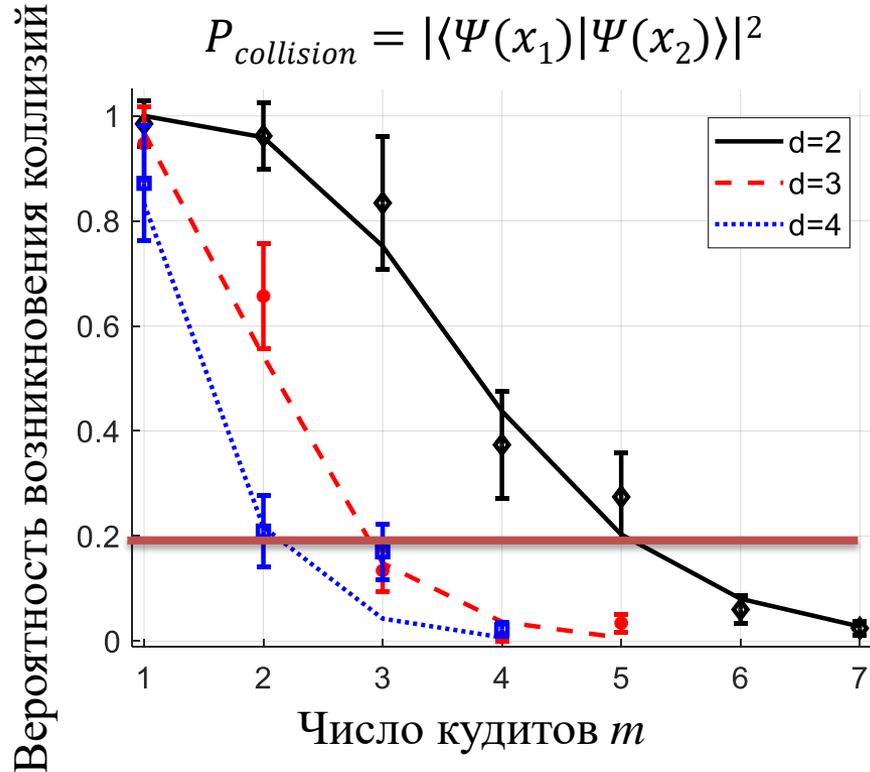
$d = 2$	
m	$x_1 (\varepsilon^*)$
1	1 (0,9998)
2	9 (0,9590)
3	24 (0,7519)
4	114 (0,4378)
5	97 (0,2031)
6	76 (0,0806)
7	69 (0,0279)

$d = 3$	
m	$x_1 (\varepsilon^*)$
1	97 (0,9681)
2	69 (0,5422)
3	93 (0,1483)
4	95 (0,0368)
5	123 (0,0063)

$d = 4$	
m	$x_1 (\varepsilon^*)$
1	37 (0,8329)
2	44 (0,2174)
3	49 (0,0429)
4	123 (0,0072)

\*  $\varepsilon = P_{\text{collision}}$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света



Оптимальные соотношения для ( $\delta = 0,2; \epsilon = 0,2$ )

$d = 2 (m = 5)$

$d = 3 (m = 3)$

$d = 4 (m = 2)$

При одинаковом размере квантового пространства ( $16 = \dim |\Psi(x)\rangle\rangle$ )

$$\epsilon_{d=4,m=2} \approx \epsilon_{d=2,m=4}/2$$

# Классически-квантовые функции хеширования на основе многомерных однофотонных состояний света

- Получены однофотонные многомерные состояния в базисе мод орбитального углового момента света с размерность  $d = 2, 3, 4$ .
- Реализована процедура квантовой томографии генерируемых многомерных однофотонных состояний. Продемонстрировано, что генерируемые состояния воспроизводятся с высокой степенью точности и чистоты. (  $F_{d=2} = 0.99 \pm 0.01$   
 $\lambda_{d=2} = 0.999$        $F_{d=3} = 0.987 \pm 0.012$        $\lambda_{d=3} = 0.993$  )
- Предложен протокол квантового хеширования на основе многомерных однофотонных состояний света и исследованы свойства устойчивости к коллизиям многомерных квантовых хеш-функций. Продемонстрировано, что однофотонные состояния высокой размерности позволяют достичь оптимальных параметров хеширования (вероятности коллизий и вероятности «декодирования») с меньшим количеством носителей информации, используемых в реализации протокола.

# Основные результаты

- Создан источник узкополосных однофотонных состояний света на основе однопараметрического генератора света, который согласован с устройствами квантовой памяти на основе  $\text{Nd}^{3+}$  в различных диэлектрических матрицах и генерирует оповещающий фотон, совместимый с оптоволоконными линиями связи.
- Предложена модель генерации перепутанных состояний «квантовая память-фотон» на основе совмещения устройств квантовой памяти и узкополосного источника света в общем кольцевом резонаторе.
- Получен источник многомерных однофотонных состояний света на основе спонтанного параметрического рассеяния света в базисе орбитального углового момента света, который позволяет увеличить скорость работы различных квантовых протоколов.
- Предложен протокол квантового хеширования на основе многомерных однофотонных состояний света и исследованы свойства устойчивости к коллизиям многомерных квантовых хеш-функций. Кроме того, предложен обобщенный процесс верификации результатов квантового хеширования (хеш-суммы) на основе многомерных однофотонных состояний света.

# Публикации по теме диссертации

## Публикации в индексируемых журналах:

1. PPLN-based photon-pair source compatible with solid state quantum memories and telecom optical fibers / I. Z. Latypov, A. V. Shkalikov, **D. O. Akat'ev** [et al.] // Journal of Physics: Conference Series. – 2017. – V. 859. – 2017. – P. 012011.
2. Генерация узкополосных однофотонных состояний при спонтанном параметрическом рассеянии для квантовой памяти в примесных кристаллах / **Д. О. Акатьев** [и др.] // Квантовая электроника. – 2018. – Т. 48, № 10. – С. 902–905.
3. Multiqudit quantum hashing and its implementation based on orbital angular momentum encoding / **D. O. Akat'ev** [et al.] // Laser Physics Letters. – 2022. – V. 19, № 12. – P. 125205.
4. **Akat'ev D. O.**, Kalachev A. A. Optical parametric oscillator with quantum memory for quantum repeaters // Laser Physics. – 2023. – V. 33, № 1. – P. 015202.
5. Однорезонаторный параметрический источник фотонов, совместимый с твердотельной квантовой памятью / Д. А. Турайханов, **Д. О. Акатьев** [и др.] // Известия вузов. Радиофизика. – 2023. – Т. 66, № 2. – (принята к печати)

# Публикации по теме диссертации

## В сборниках трудов конференций:

1. Multiqudit quantum hashing via orbital angular momentum of light / D. Akat'ev [et al.] // Proceedings of the 5th international school on quantum technologies. – 2022. – P. 51-52.
2. Функции хеширования на основе многомерных однофотонных состояний / Д. Акатьев [и др.] // XX сероссийский молодежный Самарский конкурс-конференция научных работ по оптике и лазерной физике, посвященный 100-летию со дня рождения Н.Г. Басова: сборник трудов конференции. – 2022. – С. 34-39. – ISBN 978-5-89513-516-7.
3. Функции хеширования на основе многомерных однофотонных состояний / Д. Акатьев [и др.] // Научный семинар «Нанооптика, фотоника и когерентная спектроскопия. Яльчик – 2021»: Сборник тезисов. – 2021. – С. 58-61. – ISBN 978-5-89513-504-4.
4. Функция хеширования на основе орбитального углового момента света / Д. Акатьев [и др.] // XVIII Всероссийский молодежный Самарский конкурс-конференция научных работ по оптике и лазерной физике: сборник трудов конференции. – 2020. – С. 28-34. – ISBN 978-5-902622-44-4.
5. Generation of time-bin qudit based on spontaneous parametric down-conversion / A. D.O. [et al.] // Proceedings of the ninth german-russian week of the young researcher “quantum science: light-matter interaction”. – 2019. – P. 11.
6. Генерация "time-bin"кудитов на основе спонтанного параметрического рассеяния света / Д. Акатьев [и др.] // XIII международные чтения по квантовой оптике (IWQO – 2019): Сборник тезисов. – 2019. – С. 258-259. – ISBN 978-5-89513-451-1.
7. Preparation of narrow-band single photon states via cavity-assisted spontaneous parametric down-conversion / D. Akat'ev [et al.] // VIII Russian-Chinese Symposium on Laser Physics and Photonics. PROGRAM&ABSTRACTS. – 2018. – P. 27.
8. Developing narrowband heralded single-photon sources based on spontaneous parametric down-conversion / D. Turaykhanov [et al.] // 4th Russian-German-French Laser Symposium. PROGRAM & ABSTRACTS. – 2018. – P. 16.

# Публикации по теме диссертации

## В сборниках трудов конференций:

9. Приготовление однофотонных состояний в процессе спонтанного параметрического рассеяния света в кристалле PPLN в резонаторе для квантовой памяти на основе  $\text{YLiF}_4$  / А. Шкаликов [и др.] // XI международный симпозиум по фотонному эхо и когерентной спектроскопии (ФЭКС – 2017): Сборник тезисов. – 2017. – С. 144-145. – ISBN 978-5-89513-421-4.
10. Preparation of single-photon states via cavity-assisted spontaneous parametric down-conversion for quantum memory based on  $\text{Y}_7\text{LiF}_4:\text{Nd}^{3+}$  crystal / D. Akatiev [и др.] // EPJ Web of Conferences. Vol. 161. – EDP Sciences. 2017. – P. 02026.

# Апробация работы

1. 5-ая Международная школа по квантовым технологиям, Хоста, г. Сочи, 2-8 октября 2022 г.;
2. XX Всероссийский молодежный Самарский конкурс-конференция научных работ по оптике и лазерной физике, посвященный 100-летию со дня рождения Н.Г. Басова, г. Самара, 8-12 ноября 2022 г.;
3. Семинар Нанооптика, фотоника и когерентная спектроскопия. Яльчик – 2021, г. Йошкар-Ола, 1-4 июля 2021 г.;
4. XVIII Всероссийский молодежный Самарский конкурс-конференция научных работ по оптике и лазерной физике, г. Самара, 9-12 ноября 2020 г.;
5. IX Российско-германская неделя молодого учёного, г. Москва, 23-26 сентября 2019 г.;
6. XIII Международные чтения по квантовой оптике (IWQO-2019), г. Владимир, 9-14 сентября 2019 г.;
7. VIII Российско-китайский симпозиум по лазерной физике и фотонике, г. Казань, 11-16 октября 2018 г.;
8. IV Германо-французско-российский симпозиум по лазерной физике, г. Казань, 23-27 апреля 2018 г.;
9. XI Международный симпозиум по фотонному эхо и когерентной спектроскопии (ФЭКС-2017), г. Светлогорск, 16-21 сентября 2017 г..

Доклады 1, 2, 6 были отмечены дипломами.

**Спасибо за внимание!**

# Квантовая томография состояний с ОУМ

$$\hat{\rho} = \frac{1}{d} \hat{\tau}_0 + \sum_{n=1}^{d^2-1} b_n \hat{\tau}_n$$

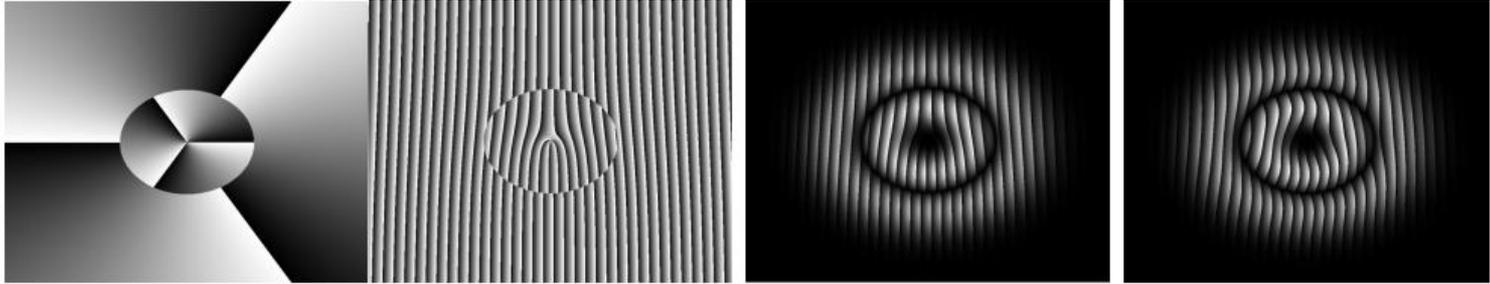
$$|\Psi_j(\varphi)\rangle = (|j\rangle + e^{i\varphi} | -j\rangle) / \sqrt{2}$$

$$\hat{\rho} = \frac{1}{2} \sum_{i=0}^3 S_i \hat{\sigma}_i$$

где  $\hat{\sigma}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $\hat{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ,  $\hat{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ ,  $\hat{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ .

$$S_0 = P_{|0\rangle} + P_{|1\rangle}, S_1 = P_{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)} - P_{\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)}, S_2 = P_{\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle)} - P_{\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)},$$

$$S_3 = P_{|0\rangle} - P_{|1\rangle}.$$



$$\Phi(x, y) = A_{ratio}(x, y) \bmod (\varphi_{des}(x, y) - \pi A_{ratio}(x, y), 2\pi)$$

$$\varphi_{des} = \varphi_{out}(x, y) - \varphi_{in}(x, y) + \varphi_{gr}, \quad \varphi_{gr} = \bmod\left(\frac{2\pi x}{\Lambda}, 2\pi\right)$$