конференция
РусКрипто

Ежегодная международная научно-практическая конференция

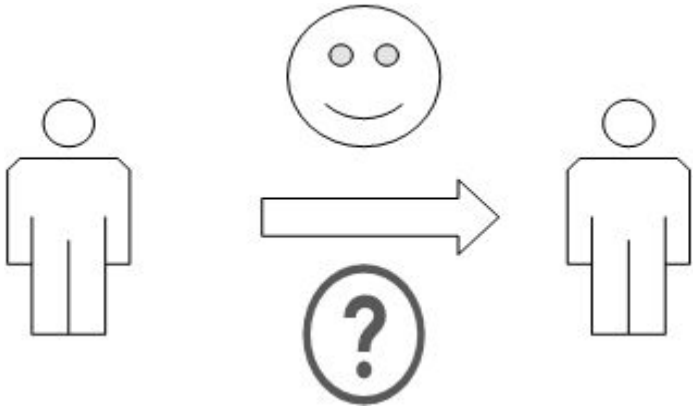
«РусКрипто'2023»

Классификация подходов квантовой аутентификации

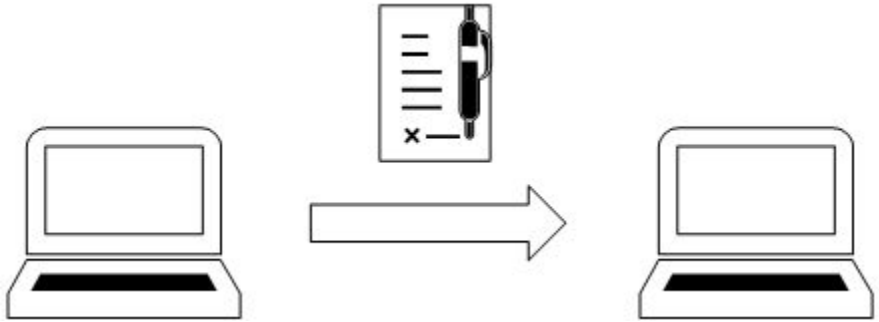
Лихтенберг А.М., системный аналитик, АО "ИнфоТеКС"; аспирант, Университет ИТМО
ankel.likhtenberg@infotecs.ru
Жиляев А.Е., к.т.н., исследователь, АО "ИнфоТеКС"
Беззатеев С.В., д.т.н., доцент, Государственный Университет Аэрокосмического

Что такое аутентификация?

Аутентификация стороны

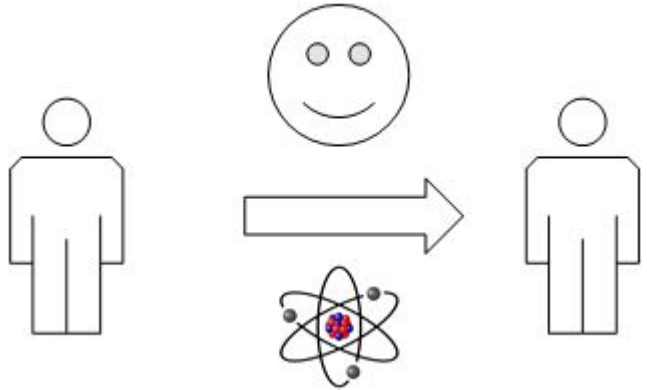


Аутентификация источника

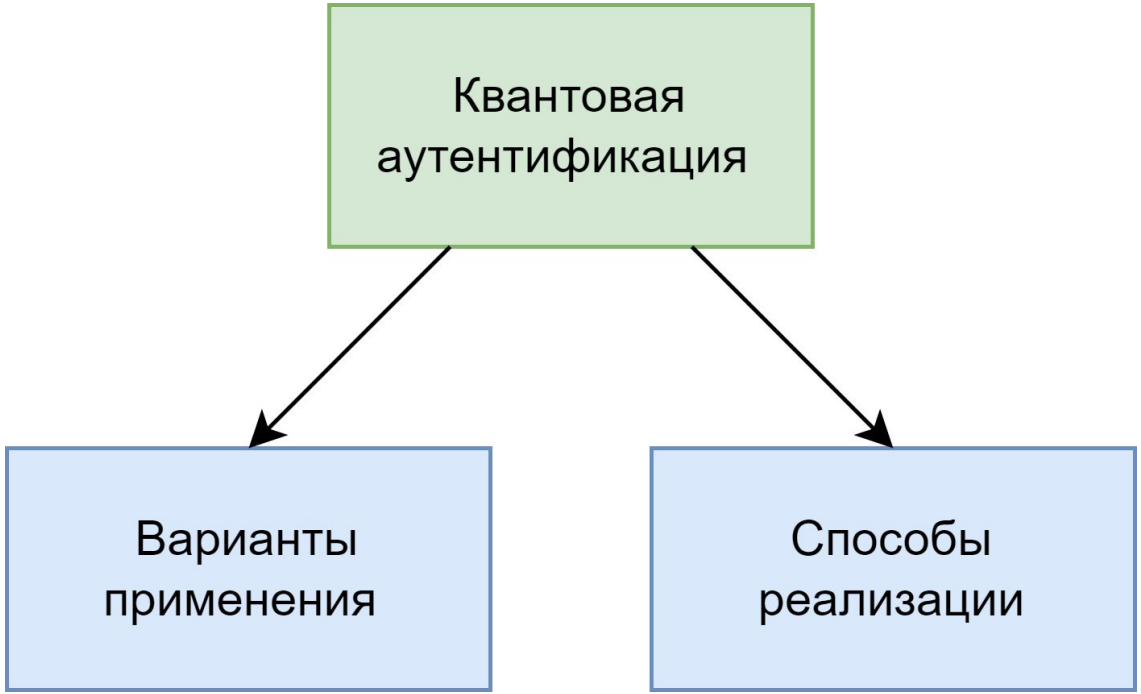


Что понимать под квантовой аутентификацией

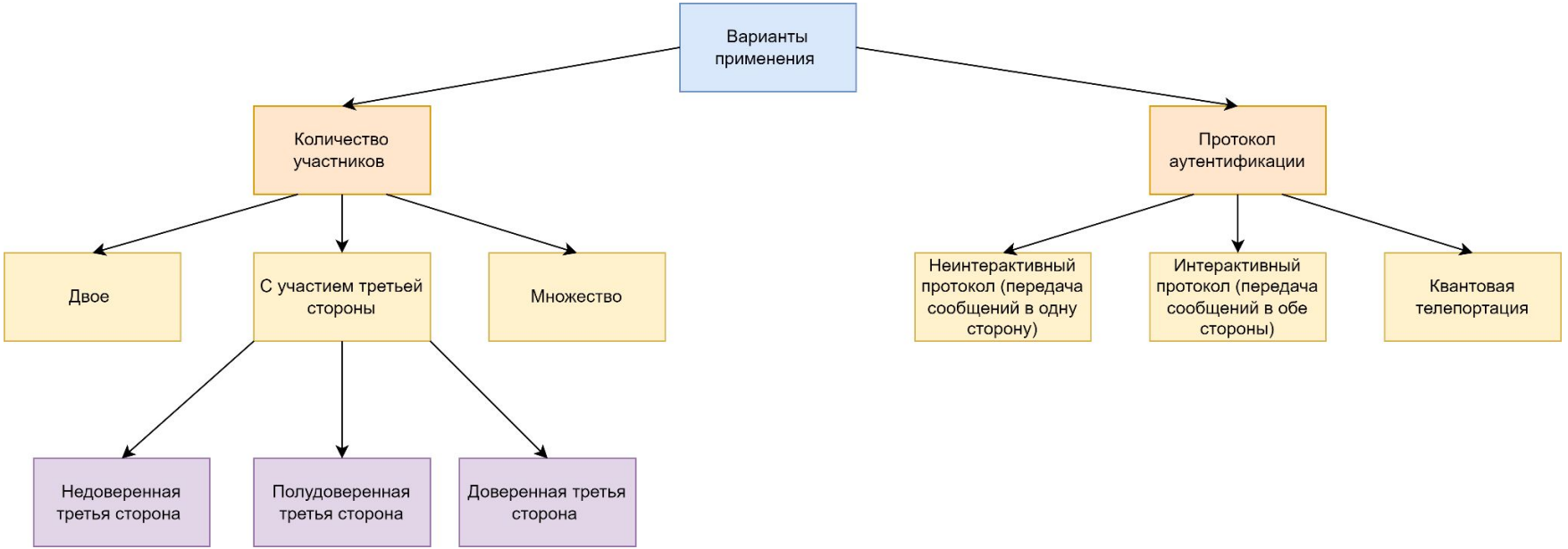
Обеспечение аутентичности *стороны* с применением свойств квантовых частиц и применением квантовых технологий



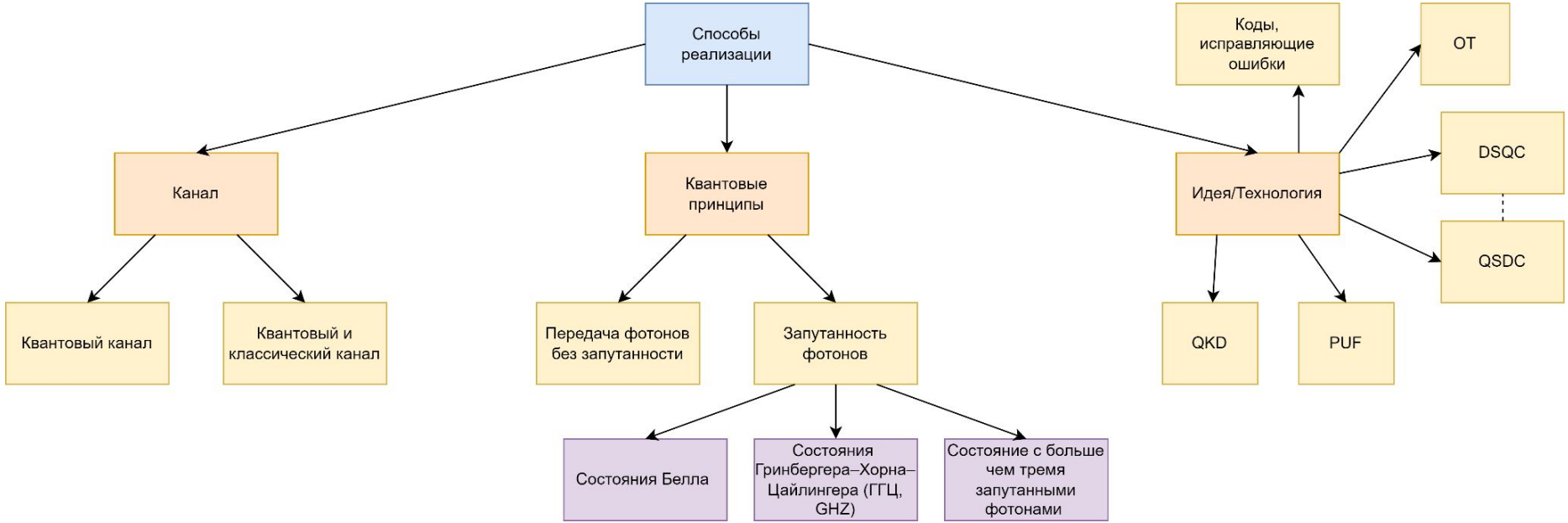
Классификация квантовой аутентификации



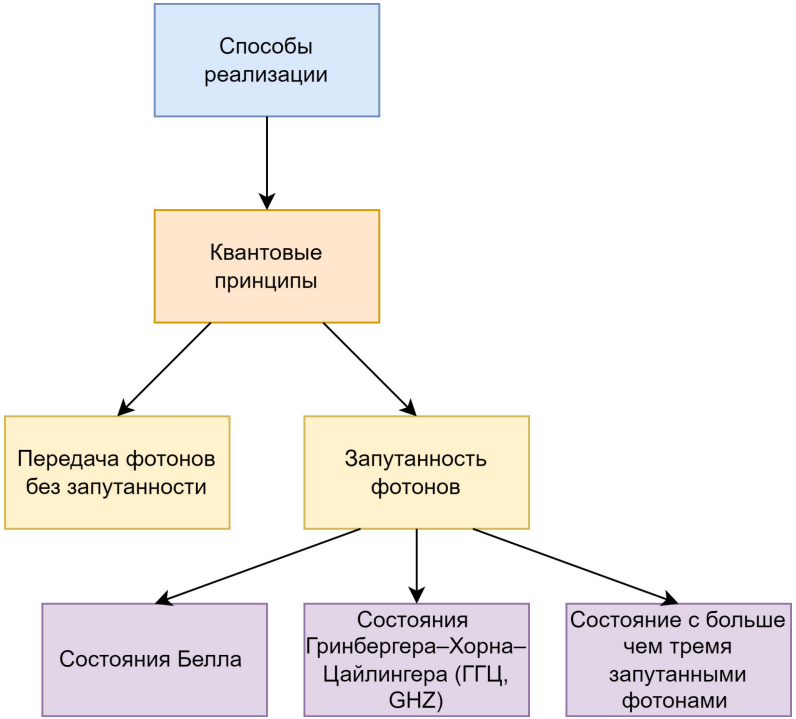
Варианты применения



Способы реализации



Способы реализации: квантовые принципы



Запутанность фотонов

Квантовая запутанность — квантовомеханическое явление, при котором квантовые состояния двух или большего числа объектов оказываются взаимозависимыми.

Запутанность фотонов: примеры

A Shared Secret Key Initiated by EPR Authentication and Qubit Transmission Channels [2]

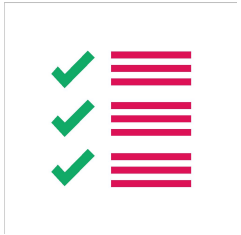
- два запутанных фотона
- без участия третьей стороны

Multi-party blind quantum computation protocol with mutual authentication in network [1]

- два запутанных фотона
- множество полудоверенных сторон-участников

Controlled mutual quantum entity authentication with an untrusted third party [3]

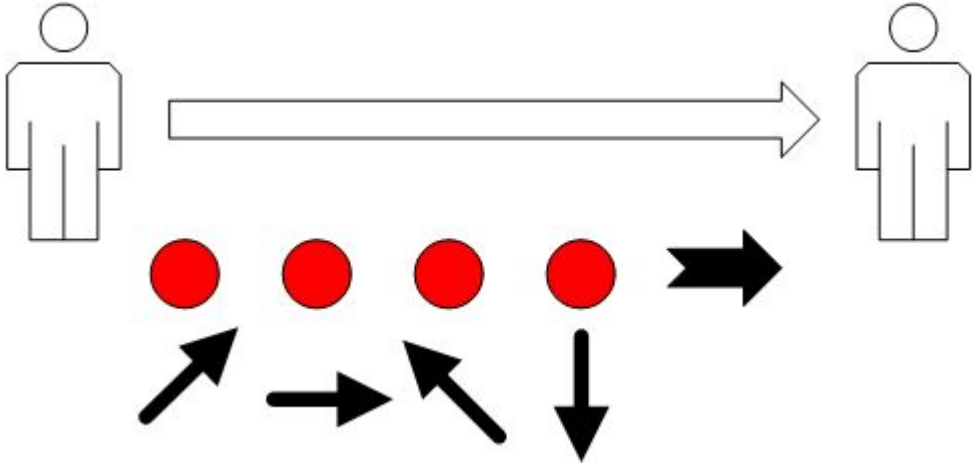
- три запутанных фотона
- участвует третья недоверенная сторона



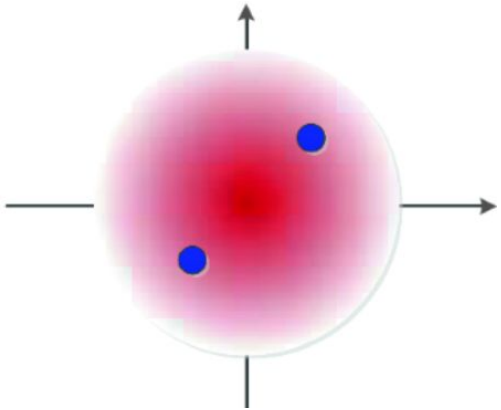
Controlled quantum secure direct communication with authentication protocol based on five-particle cluster state and classical xor operation [4]

- пять запутанных фотонов
- участвует третья доверенная сторона

Квантовые принципы: передача фотонов

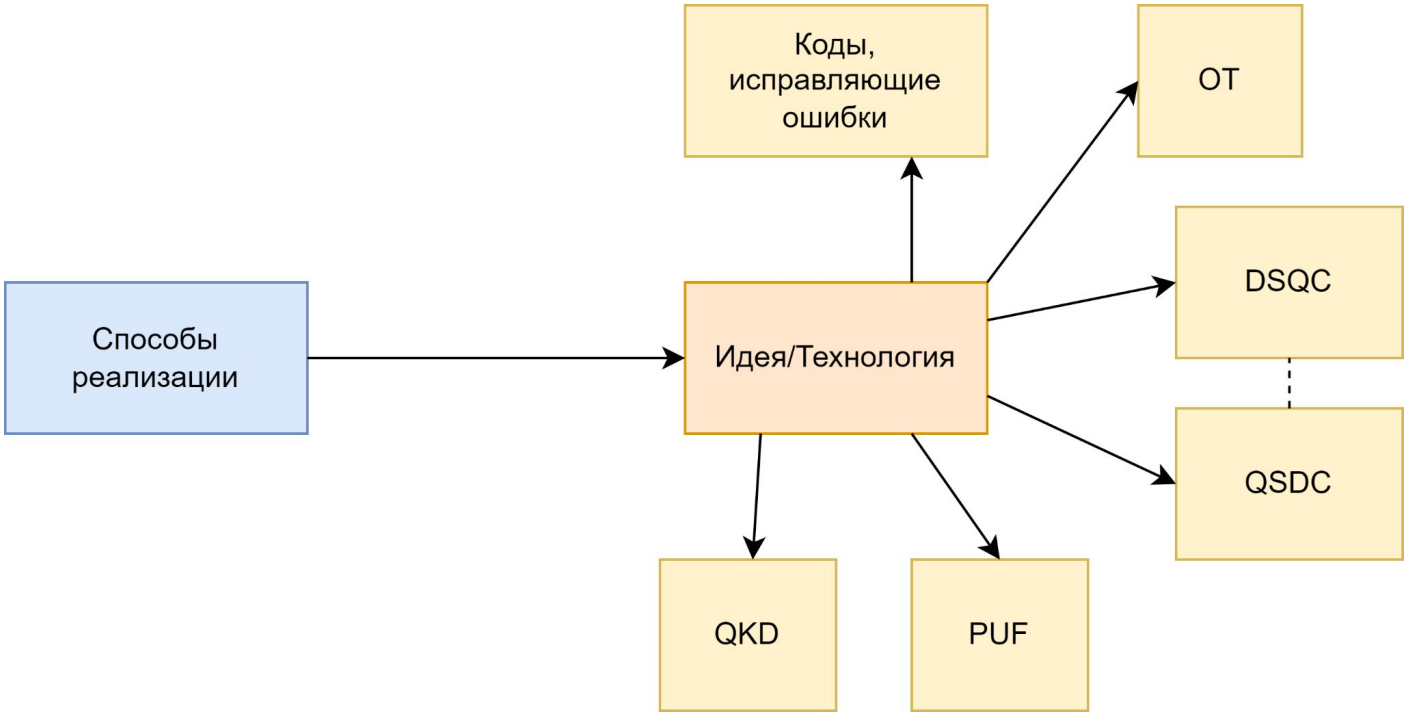


Кодирование в состояниях отдельных частиц (DV)



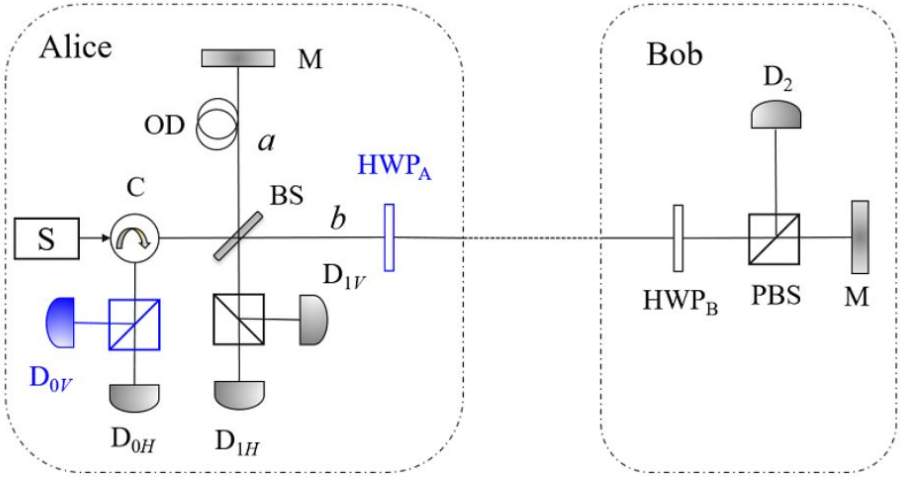
Кодирование в состояниях непрерывного излучения (CV)

Способы реализации: технологии



Технологии: QKD (Quantum Key Distribution)

С помощью протокола квантового распределения ключей генерируют общий предраспределённый секрет (ключ), который затем используют для аутентификации в квантовых или классических схемах.
Либо же на основе схемы КРК проверяется владение общим предраспределенным ключом



Пример: Quantum Identity Authentication in the Counterfactual Quantum Key Distribution Protocol [10]

Технологии: OT (Oblivious Transfer)

Предварительно распределенный секрет (классический)
Секрет используется для выбора базиса кодирования/детектирования
Алиса передает случайную строку
Боб должен предъявить полученную строку
Для защиты от ошибок в квантовом канале можно кодировать случайную строку некоторым кодом

Пример: Quantum oblivious mutual identification [8]

Технологии: QSDC и DSQC

Quantum Secure Direct Communication

На двух сторонах используют унитарный оператор, чтобы изменить некое квантовое состояние и потом обратить его обратно в исходное (в отличие от КРК, где передача исходит из классических данных). Классический канал может не использоваться.

Deterministic Secure Quantum Communication

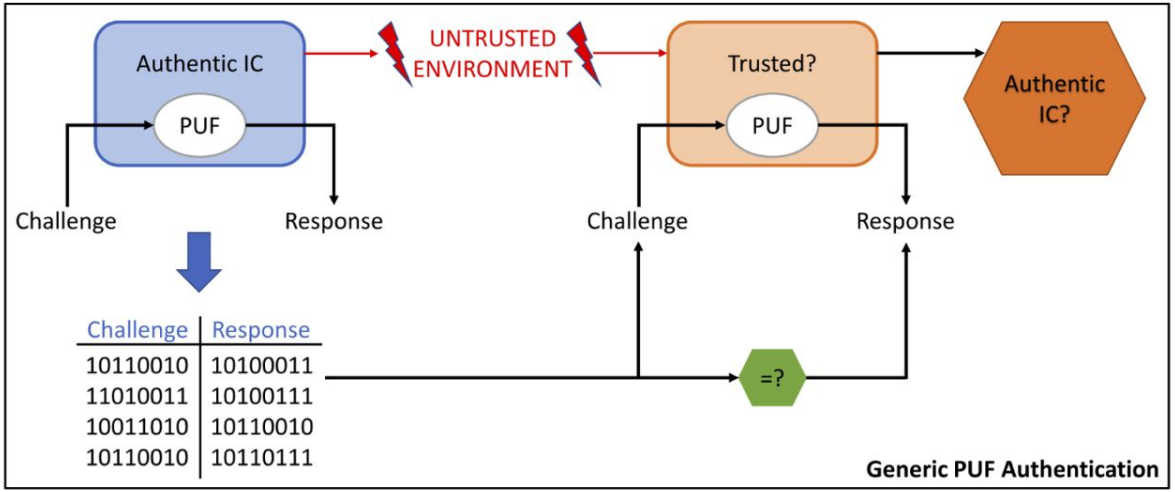
Использует квантовую плотную кодировку и протокол проверки ошибок, чтобы обеспечить безопасность передачи данных. Скорость передачи данных может быть повышена благодаря возможности передавать несколько бит информации за один квантовый бит.

Примеры:

- Controlled quantum secure direct communication with authentication protocol based on five-particle cluster state and classical xor operation [3] - QSDC
- Maximally efficient protocols for direct secure quantum communication [9] - DSQC трансформирован в QSDC

Технологии: PUF (Physical Unclonable Function)

В основе - квантовые принципы (каскад интерферометров Маха-Цандера, зеркало с уникальным напылением).
Предварительно записанная таблица запрос-ответ.
Запрос - закодирован в состоянии фотонов.
Ответ - регистрируется однофотонными детекторами.
Классический канал может не использоваться.



Пример: Quantum-secure authentication of a physical unclonable key [5]

Технологии: коды корректирующие ошибки

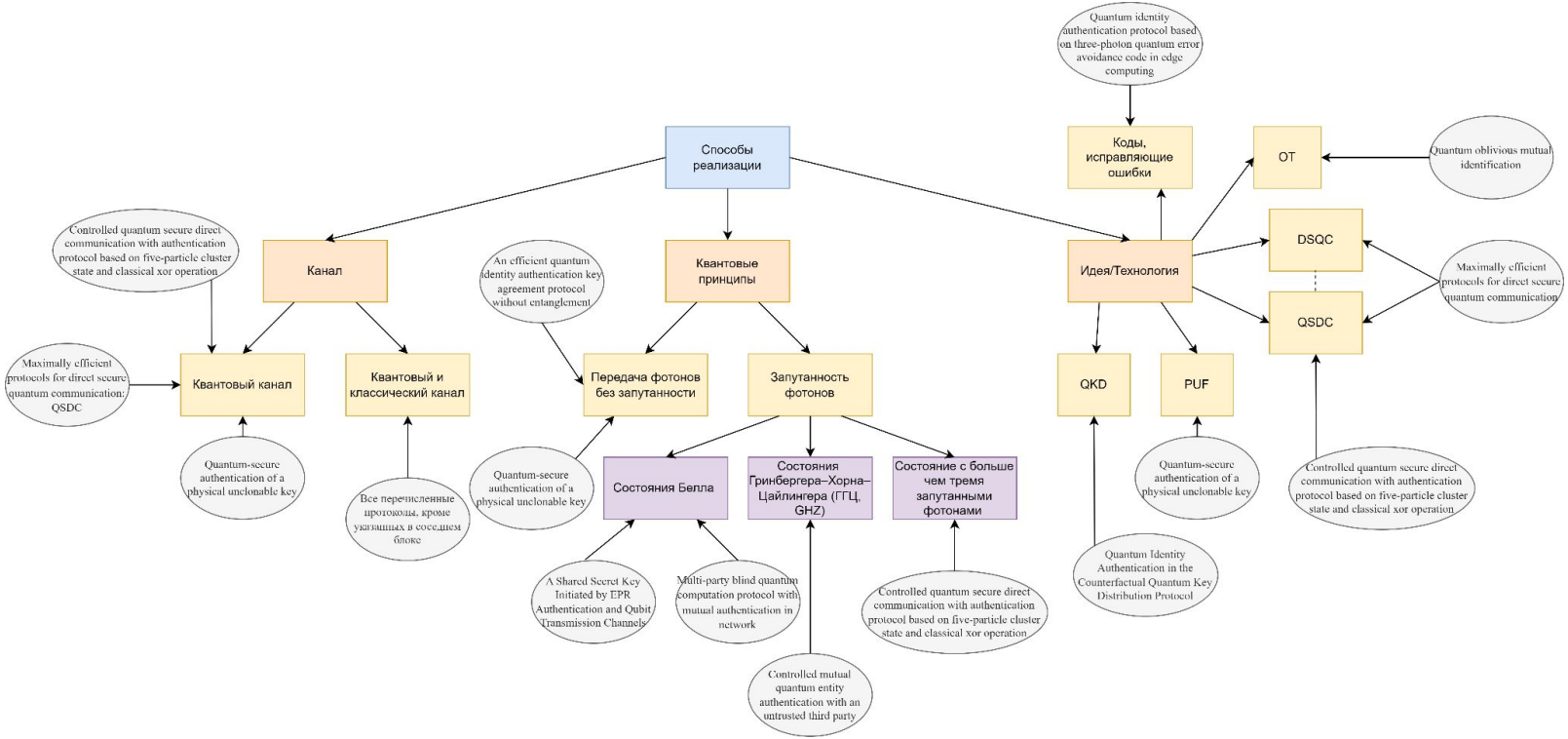
В основном используются как дополнение протоколов для противодействия ошибкам, возникающим из-за помех в канале

Самостоятельные схемы квантовой аутентификации используют общую известную обоим сторонам строку для корректного кодирования сообщения, которое Боб должен предъявить Алисе

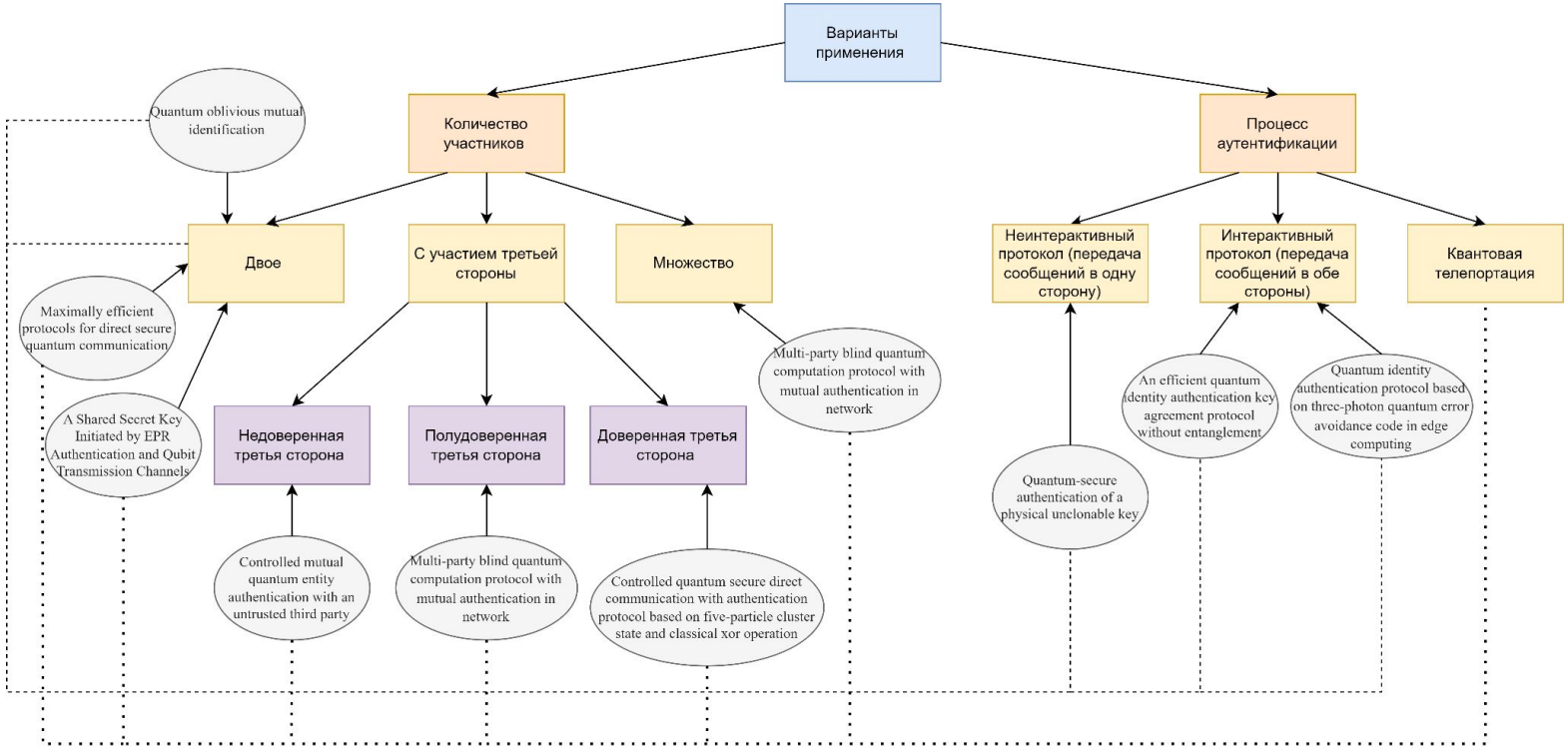
	X	
T	0	1
0	$\|\phi_1\rangle$	$\|\phi_2\rangle$
1	$\|\phi_2\rangle$	$\|\phi_3\rangle$
2	$\|\phi_3\rangle$	$\|\phi_1\rangle$

Пример: Quantum identity authentication protocol based on three-photon quantum error avoidance code in edge computing [7]

Способы реализации с примерами



Варианты применения с примерами



Вопросы

???

Контактная информация

- **Электронная почта:**

  ankel.likhtenberg@infotecs.ru
- **Телефон:**

  +7 981 143 41 45
- **Сайт:**

  infotecs.ru
  itmo.ru

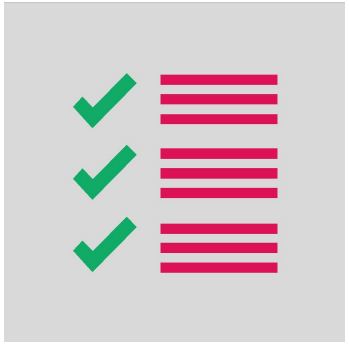
Литература

1. Shan R. T., Chen X., Yuan K. G. Multi-party blind quantum computation protocol with mutual authentication in network //Science China Information Sciences. – 2021. – Т. 64. – С. 1-14.
2. Abushgra A. A., Elleithy K. M. A shared secret key initiated By EPR authentication and Qubit transmission channels //IEEE Access. – 2017. – Т. 5. – С. 17753-17763.
3. Kang M. S. et al. Controlled mutual quantum entity authentication with an untrusted third party //Quantum Information Processing. – 2018. – Т. 17. – С. 1-15.
4. Zheng X., Long Y. Controlled quantum secure direct communication with authentication protocol based on five-particle cluster state and classical XOR operation //Quantum Information Processing. – 2019. – Т. 18. – №. 5. – С. 129.
5. Goorden S. A. et al. Quantum-secure authentication of a physical unclonable key //Optica. – 2014. – Т. 1. – №. 6. – С. 421-424.
6. Zhu H., Wang L., Zhang Y. An efficient quantum identity authentication key agreement protocol without entanglement //Quantum Information Processing. – 2020. – Т. 19. – С. 1-14.
7. Qu Z., Liu X., Wu S. Quantum identity authentication protocol based on three‐photon quantum error avoidance code in edge computing //Transactions on Emerging Telecommunications Technologies. – 2022. – Т. 33. – №. 6. – С. e3945.
8. Crépeau C., Salvail L. Quantum oblivious mutual identification //Advances in Cryptology—EUROCRYPT'95: International Conference on the Theory and Application of Cryptographic Techniques Saint-Malo, France, May 21–25, 1995 Proceedings 14. – Springer Berlin Heidelberg, 1995. – С. 133-146.
9. Banerjee A., Pathak A. Maximally efficient protocols for direct secure quantum communication //Physics Letters A. – 2012. – Т. 376. – №. 45. – С. 2944-2950.
10. Liu B. et al. Quantum identity authentication in the counterfactual quantum key distribution protocol //Entropy. – 2019. – Т. 21. – №. 5. – С. 518.

Возможно имеет смысл здесь привести некоторое сравнение рассмотренных подходов по способам и применениям и предложить наше мнение ЧТО может быть наиболее эффективным…

Название слайда

- Даем стабильный доход на годы
- Продолжаем развивать экосистему
- Интересы партнеров приоритетны
- Работаем открыто и честно
- Создаем вместе



Название слайда

Даем стабильный доход на годы

Даем стабильный доход на годы

Даем стабильный доход на годы

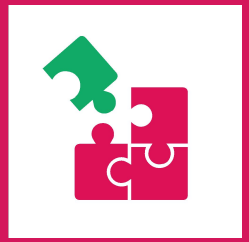
Название слайда

- Даем стабильный доход на годы
- Продолжаем развивать экосистему
- Интересы партнеров приоритетны

- Даем стабильный доход на годы
- Продолжаем развивать экосистему
- Интересы партнеров приоритетны

- Даем стабильный доход на годы
- Продолжаем развивать экосистему
- Интересы партнеров приоритетны

Название слайда



- Даем стабильный доход на годы
- Продолжаем развивать экосистему
- Интересы партнеров приоритетны

- Даем стабильный доход на годы
- Продолжаем развивать экосистему
- Интересы партнеров приоритетны

Набор основных пиктограмм