



THE FUTURE OF secure
communication IS quantum

ТЕКУЩО СЪСТОЯНИЕ И БЪДЕЩИ ПЕРСПЕКТИВИ НА КВАНТОВИТЕ КОМУНИКАЦИИ

Обучителни материали за административен
персонал



НАСТОЯЩО СЪСТОЯНИЕ И ПЕРСПЕКТИВИ НА КВАНТОВИТЕ КОМУНИКАЦИИ

Обучителни материали за административен състав

Лъчезар Георгиев
Редактор

Проект 101091399 “BG National QCI Plan”

www.euroqci.bg

Проект 101091399 “BG National QCI Plan” е съфинансиран от Европейския съюз. Изразените позиции са на автора/ите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия. Нито Европейският съюз, нито съфинансиращият орган носят отговорност за тях

София, 2024

Заглавие: Настоящо състояние и перспективи на квантовите комуникации, учебни материали за административен състав

Научен редактор: Лъчезар Георгиев

Автори: Лъчезар Георгиев^(1,2), Димитар Недановски⁽²⁾, Антон Младенов^(1,2), Светослав Христов^(1,2), Николай Николов⁽²⁾, Петко Николов^(1,2), Григори Матеин⁽¹⁾, Людмил Хаджииванов⁽²⁾, Михаил Стоилов⁽²⁾, Лилианна Пантелеев-Симеонова⁽²⁾, Бойко Вачев^(1,2), Константин Иванов⁽⁴⁾, Мирослав Димитров⁽³⁾, Чавдар Руменин^(1,2), Август Иванов^(1,2), Сия Лозанова^(1,2), Любомир Куртев⁽¹⁾, Николай Георгиев^(1,2), Климент Найденов⁽¹⁾, Мартин Ралчев^(1,2), Георги Илиев⁽¹⁾, Красимир Модев⁽¹⁾, Андрей Бояджиев⁽¹⁾, Кирил Кирилов⁽¹⁾

(1) Център за компетентност КВАЗАР

(2) Институт по роботика – Българска академия на науките

(3) Електрон прогрес

(4) Ентерпрайз Комуникейшън груп

Дизайн на корицата: Корект консултинг груп

Съдържание

Списък на съкращенията	2
Списък на фигурите	3
1 Въведение	4
2 На кратко за няколко известни криptosистеми и уязвимостта им от квантовите компютри	5
2.1 Симетрично и асиметрично криптиране	5
2.2 AES 256	6
2.3 RSA и ECC	7
3 QKD протоколи	7
3.1 Протокол BB84	9
3.2 Кохерентен еднопосочен протокол	11
3.3 Квантово предаване на секретен ключ с непрекъсната променлива	12
4 Изисквания към инфраструктурата	14
4.1 Параметри на оптичните кабели	14
4.2 Комуникация в свободното пространство	16
4.2.1 Основни инфраструктурни елементи (по важност)	16
4.2.2 QKD в свободно пространство въздух/космос близо до земята	18
4.2.3 Земно атмосферна FSQC/сателитна квантова комуникация	19
4.2.4 Проблеми със сигурността и надеждността	21
4.2.5 Сигурни възли (Trusted nodes)	23
5 Оборудване за QKD	24
6 Интегриране на платформите за QKD с класически криптори AES 256	25
7 Литература	27

Списък на съкращенията

- AES 256** Advanced Encryption System 6
- BB84** DV protocol proposed by Charles Bennett and Gilles Brassard in 1984 9
- COW** Coherent One-Way protocol 11
- CV** Continuous Variable 8
- CV-QKD** Continuous Variable (use coherent detectors and sources) QKD 12
- DEP** Digital Europe Programme 5
- DV** Discrete Variable 8
- DV-QKD** Discrete Variable (use single-photon detectors and sources) QKD 8
- DWDM** Dense-Wavelength-Division-Multiplexing 13
- ECC** Elliptic Curve Cryptography 7
- EuroQCI** European Quantum Communication Infrastructure 4
- FSQC** Free Space Quantum Communication 19
- PKI** Public Key Infrastructure 24
- QBER** Quantum Bit Error Rate 11
- QKD** Quantum Key Distribution 7
- RSA** Rivest–Shamir–Adleman 7
- TN** Trusted Node 24

Списък на фигурите

1	Симетрично криптиране.	6
2	Асиметрично криптиране.	6
3	Протокол BB84 с фотонна поляризация.	9
4	Загуби в оптичните влакна.	15
5	Twin-field QKD.	16
6	Европейска сателитна QKD система Eagle-1.	20
7	QKD с един междинен сигурен възел.	23
8	QKD мрежа с три възли и интегрирани AES 256 криптиори.	26

1 Въведение

Квантовите технологии, като квантовите изчисления, квантовите комуникации и квантовата симулация, преминават през втора квантова революция след първата, която триумфира със създаването на квантовата механика в началото на двадесети век. Квантовите изчисления обещават да решават трудни математически проблеми експоненциално по-бързо от класическите суперкомпютри и това представлява сериозна заплаха за класическата криптография, чиято сигурност се основава на детерминирани трудни за решаване математически проблеми.

Бързото развитие на квантовите компютри заплашва значително класическата криптография, която се използва за защита на чувствителни данни по време на комуникация чрез публични мрежи. За щастие, квантовата криптография или квантовата комуникация използват стохастични процеси, базирани на свойствата на квантовите системи, като фотони, квантите на електромагнитното поле, което ги прави безопасни срещу заплахата от квантовите компютри. Дори сега класически криптираната информация, изпратена през обществени мрежи, не е безопасна поради атаките от тип *harvest-now-decrypt-later*.

Квантовото разпределение на ключове (или квантовата комуникация) е революционна технология за разпространение на симетричен таен ключ с помощта на фотони или много къси лазерни импулси, предавани през оптични влакна или свободно пространство. Този ключ не може да бъде копиран, тъй като всеки опит за получаване на информация променя състоянията на квантовите системи, използвани за кодиране на битовете, и създава значителни грешки в предадените ключове, които са видими за комуникиращите страни.

Необходимостта от внедряване на квантово разпределение на ключове (QKD) за защита на комуникациите между публичните органи беше оценена от държавите-членки на Европейския съюз, които стартираха инициативата “Европейска инфраструктура за квантова комуникация” (EuroQCI) през 2019 г. и през 2022 г. всички 27 държави-членки на ЕС подписаха декларация за участие в тази инициатива. България е подписала декларацията през 2020 г. Тази инициатива изисква внедряването на нов квантов слой и интегрирането му в съществуващите телекомуникационни оптични мрежи (наземен сегмент), съчетавайки най-добрите решения в класическата и квантовата криптография, напр. комбиниране на класическия Advanced Encryption Standard (AES-256) с QKD, за да се получи безпрецедентна сигурност на публичните комуникации. Планът за действие EuroQCI също така предвижда разполагането на комуникационни спътници на ниска околоземна орбита, средна околоземна орбита и геостационарни (космически сегмент), оборудвани с модули за квантово разпределение на ключове и изграждане на оптични наземни станции за свързване на наземния и космическия сегменти. България ще има огромна полза от разгръщането на сегмента EuroQCI Space и ще може да използва комуникационните спътници още преди да стане член на Европейската космическа агенция.

В момента всичките 27 държави-членки на ЕС изпълняват първата фаза на внедряване

на плана за действие EuroQCI. Европейската комисия е осигурила финансиране от ЕС на плана за действие чрез “Дигиталната европейска програма” (DEP). България кандидатства с проект по DEP за 10 милиона евро (ЕС ще възстанови 50% от реалните разходи), Споразумението за безвъзмездна помощ е подписано през ноември 2022 г., а проектът стартира на 01.01.2023 г. с продължителност 30 месеца.

2 На кратко за няколко известни криptosистеми и уязвимостта им от квантовите компютри

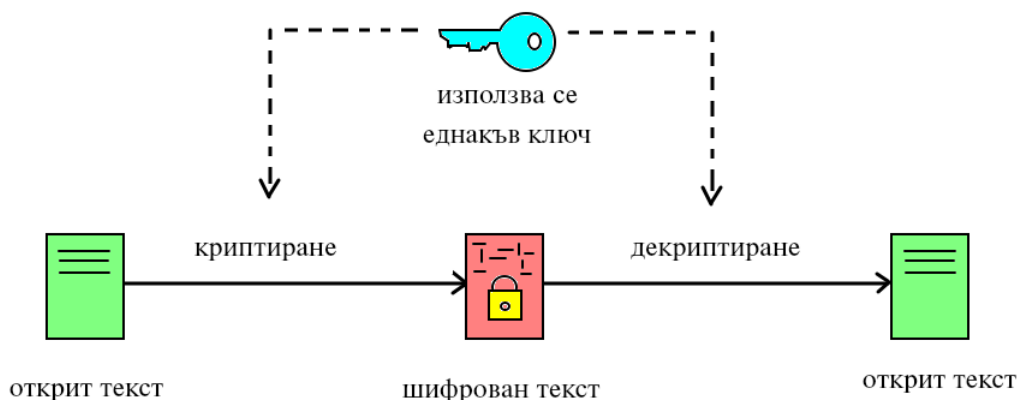
От древни времена различни алгоритми за криптиране са били ползвани с цел защита на чувствителна информация по време на прехвърлянето ѝ между комуникаращите страни. Започваме изложението с един не строг криптографски речник, на кратко описващ основни понятия, които ще използваме:

- *шифроване (криптиране)*: кодиране (трансформация) на данните, за да ги направим неразпознаваеми;
- *декриптиране*: разкодиране (обратно трансформиране) на данните до оригиналния им формат;
- *шифър*: синоним за алгоритъм, по който се извършва криптирането;
- *ключ*: сложна последователност от буквено-цифрови знаци, част от алгоритъмът, с който извършва кодирането и декодирането на данни;
- *открит текст (plaintext)*: декриптирани или некриптирани данни;
- *шифрован текст*: данни, които са криптирани.

2.1 Симетрично и асиметрично криптиране

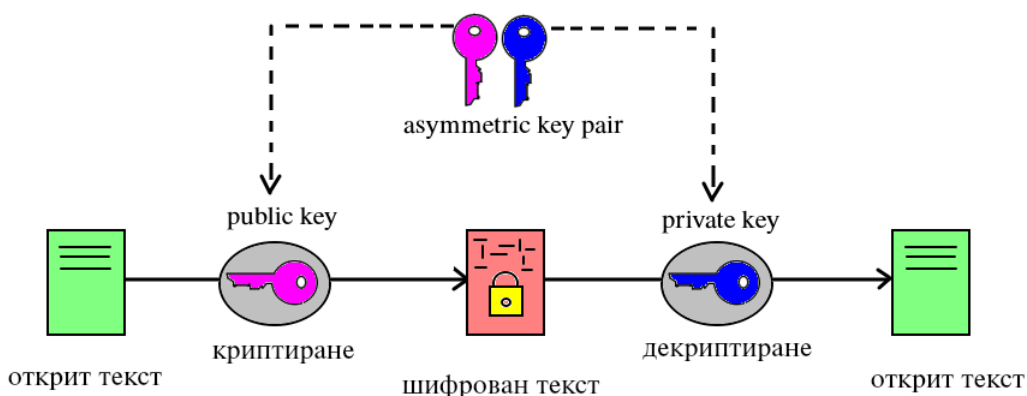
Криптографията осигурява и анализира средствата за сигурна комуникация, т.е. как да се предотврати подслушване (или неоторизиран достъп) до лични съобщения (данни). Разчита в голяма степен на математика, физика, електротехника, компютърни науки и др.

Криптографията може да бъде *симетрична (криптиране със симетричен ключ)* – в този случай се използва един и същ ключ (обикновено низ от символи) за криптиране и описание на съобщението, или *асиметрична (криптиране с асиметричен ключ)* – в този случай се използват различни ключове за криптиране и декриптиране на съобщението. Ключът за криптиране обикновено се нарича публичен ключ, докато ключът за дешифриране е известен като *частен ключ*.



Фигура 1: Симетрично криптиране.

Съществуват много симетрични и асиметрични *криптосистеми*, като под това понятие се разбира структуриран набор от алгоритми, използвани за сигурно преобразуване (кодиране) на обикновен текст в шифрован текст и за преобразуване (декодиране) на шифрвания текст в обикновен текст по сигурен начин. Тук съвсем на кратко ще разгледаме или споменем само някои широко използвани криптосистеми.



Фигура 2: Асиметрично криптиране.

2.2 AES 256

AES (Advanced Encryption System) е симетрична криптосистема, широко внедрена в софтуер и хардуер за шифроване на големи обеми чувствителни данни, напр. самокрип-

тиражи се дискови устройства, криптиране на бази данни, криптиране на архиви. Той е от съществено значение за правителствената компютърна сигурност и е избран от правителството на САЩ за защита на класифицирана информация.

AES 256 се счита за сигурен дори при атаки на квантови компютри, ако AES ключът за криптиране е защитен. Дори и най-добрите криптографски системи могат да бъдат уязвими, ако хакер получи достъп до ключа за криптиране. Тъй като RSA (като метод използван за споделяне на симетричния ключ за AES) е изложен на риск от развитието на квантовите компютри, квантовото разпределяне на ключове (QKD) се явява подходящо решение за генериране и обмен на AES 256 ключове по изключително сигурен начин. Избрахме тази комбинация от AES 256 и QKD за изграждането на първата QKD мрежа в България, като част от европейската квантова комуникационна инфраструктура.

2.3 RSA и ECC

RSA (Rivest–Shamir–Adleman) е пример за *асиметрична криптосистема* с много приложения в наши дни. Сигурността му се основава на изчислителната трудност при разлагане на произведението на две големи прости числа.

Тъй като RSA е с висока изчислителна сложност, не се използва често за директно криптиране на потребителски данни. Вместо това RSA се използва за предаване на секретни ключове за симетрично криптиране (пр. AES 256). RSA може да се използва и като *цифров подпис* - собственикът на частния ключ може да го използва, за да криптира съобщение, което може да бъде декриптирано от всеки, който има публичния ключ.

Квантовите компютри са в състояние да факторизират големи числа (алгоритъм на Шор) много по-бързо от класическите компютри. Тъй като RSA разчита на трудността при факторизиране на големи числа, достатъчно мощни квантови компютри могат да бъдат потенциална заплаха за RSA криптирането.

Криптирането чрез елиптични криви (ECC) е друг пример на асиметрично криптиране, което много се използва за блокчейни. Основава се на алгебричната структура на елиптичните криви над крайни полета.

Алгоритъмът на Шор може да се приложи за разбиване на криптографията с елиптична крива чрез изчисляване на дискретни логаритми. ECC е дори по-застрашен от квантовите компютри, отколкото RSA.

3 QKD протоколи

Основната идея на квантовото разпределяне на ключове (QKD) е, че две комуникиращи страни, традиционно наричани Алис (A) и Боб (B), могат да генерират произволен ключ на разстояние чрез специфична процедура, наречена QKD протокол, чиято сигурност

и защита срещу подслушване се гарантира от свойствата на квантовата система (като например съотношения за неопределеност и теорема за забрана на копиране на произволно състояние в квантовата механика).

Най-популярните и широко използвани алгоритми в настоящата киберсигурност, като Rivest-Shamir-Aldeman (RSA) и криптография с елиптични криви (ECC), или по-общо тези, използвани в криптографията с публичен ключ се основават на трудни за решаване математически проблеми и дългото необходимо време, необходимо за тяхното решаване на класически компютри (дори класически суперкомпютри). Въпреки това, скорошният напредък във физическата реализация на квантовите компютри и тяхното превъзходство над класическите компютри представлява реална заплаха за сигурността на днешните комуникации. Има известни алгоритми за квантови компютри, които могат да разбият както RSA, така и ECC експоненциално по-бързо от най-добрите налични суперкомпютри.

Докато квантовите компютри могат да бъдат заплаха за всеки детерминистичен алгоритъм за генериране на ключове, QKD е неразбиваемо от квантовите компютри, защото те са недетерминистични алгоритми, базирани на стохастичните свойства на квантовите системи. Следователно QKD е най-добрият квантово сигурен криптографски алгоритъм.

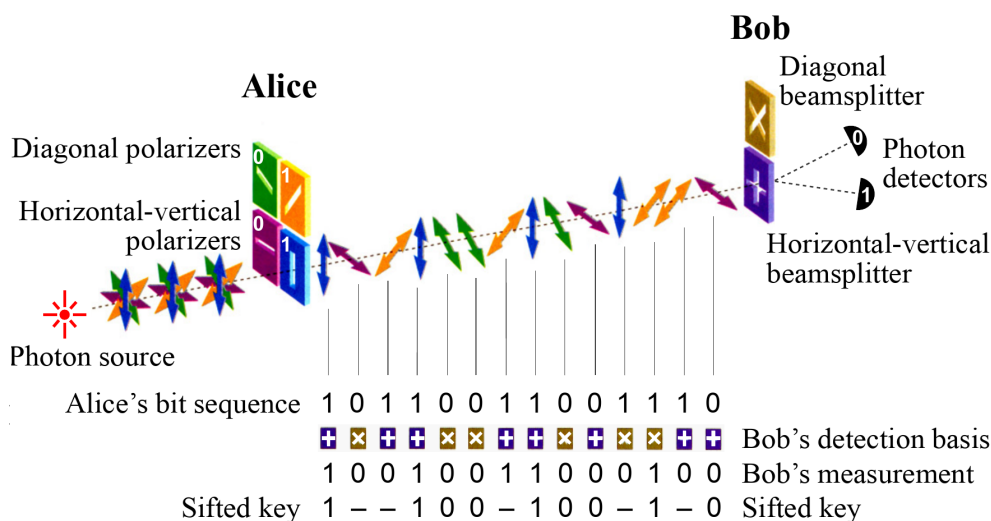
Един от най-обещаващите сценарии за защита на комуникацията е комбинирането на най-доброто от квантовата и класическата криптография. Примерно, QKD ключовете да се използват с класически алгоритми за криптиране със симетричен ключ, като AES 256 криптиори. Широко разпространено е мнението, че ако сесийните ключове на AES криптиорите се променят всяка минута, това е практически неразбиваемо решение.

QKD оборудването използва специфични свойства на квантово-механичните системи за генериране и сигурно предаване на защитен ключ, който след това се използва за класическо криптиране. Сигурността на комуникациите е гарантирана от следствия от принципите и законите на квантовата механика, като теорема за забрана на клониране [1] или свойства на заплетени състояния [2].

Съществува разнообразие от QKD протоколи, класифицирани според някои от техните характеристики. Основната класификация разграничава протоколи *Prepare-and-measure* (базирани на процедурата за измерване на неизвестни състояния в QM) и *протоколи, базирани на квантовото вълитане* (използване на свойствата на вълитани състояния). В зависимост от използваните детектори и източници, QKD протоколите могат да бъдат класифицирани или като такива *сдискретни променливи (DV)* (използват детектори и източници на единични фотони) или като протоколи с *непрекъснати променливи (CV)* (използват кохерентни детектори и източници).

3.1 Протокол BB84

BB84 е вид DV Prepare-and-measure протокол, предложен от Charles Bennett и Gilles Brassard през 1984 година [3]. Идеята е да се кодира и генерира таен ключ (краен низ от битове) с помощта на кубити (квантови битове, т.е. квантова система с две нива), както по-долу е описано. Изпращачът на ключа (отбелязан като Алис) и получателят (отбелязан като Боб) са свързани с два канала: удостоверен публичен класически канал и удостоверен публичен квантов канал, по който се предават квантови състояния.



Фигура 3: Протокол BB84 с фотонна поляризация. Източник: [4].

BB84 със състояния на поляризация

В този случай за кодиране се ползват състояния на поляризация на единични фотони и оптично влакно като квантов канал. Разглеждаме два базиса на поляризация на фотони:

- правоъгълен базис, H-V, който се състои от състояние на хоризонтална поляризация (**H**) и състояние на вертикална поляризация (**V**);
- диагонален базис, D-A, който се състои от две взаимно ортогонални линейни поляризационни състояния, **D** и **A**, така че ъгълът между **H** и **D** е 45° , докато ъгълът между **H** и **A** е 135° .

В базиса H-V, бит “0” е кодиран със състоянието на хоризонтална поляризация, **H**, докато с вертикалната поляризация, **V**, се кодира бит “1”. В базиса D-A, бит “0” е кодиран от **D** (“диагонална поляризация”), докато **A** (“антидиагонална поляризация”) кодира бит 1.

базис	0	1
H-V	H	V
D-A	D	A

В първата стъпка Алис генерира случаен бит. След това се кодира в една от произволно избраните H-V или D-A базиси като **H**, **V**, **D** или **A** състояние на поляризация на един фотон (в зависимост от стойността на бита и избрания базис). След подготовката му поляризацияното фотонно състояние се предава на Боб чрез квантовия канал. Започвайки от случайното генериране на бит, тези стъпки се повтарят многократно (в зависимост от дължината на ключа, видимостта, корекцията на грешките и т. н.). Алис записва състоянието, използвания базис и времето за всеки изпратен от нея фотон.

Когато Боб получава фотон, изпратен от Алис той не знае кой от двата базиси е бил използван за кодиране. Произволно избира H-V или D-A като базис за измерване. Записва момента на получаване, избраният базис и резултата от измерването. След приключване на измерванията на всички получени фотони Боб уведомява Алис по публичен аутентизиран канал, че е получил нейните предавания. Алис обявява (по публичния канал) на Боб базисите, които е използвала за кодирането за всяка една трансмисия. Боб по публичен канал споделя с Алис в кои случаи е използвал различен базис за измерване. И двамата отхвърлят от разглеждане случаите, в които са правени измервания в различни базиси. Алис избира част от останалите битове и ги разкрива на Боб (по публичен канал), който проверява и уведомява Алис, ако достатъчен брой от тези битове съвпадат с неговите измервания. Ако има съгласие, те продължават по-нататък и (след известно съгласуване на информацията и усиляване на поверителността) дестилират секретния ключ от разкритите битове. Ако няма достатъчно ниво на съвпадение между разкритите битове и съответните измервания (поради подслушване или други условия), Алис и Боб прекъсват процедурата и започват отначало.

Потенциален подслушвач (отбелязан като Ева) не може да копира поляризацияните състояния, които Алис изпраща на Боб през квантовия канал, тъй като такава операция не е възможна за неизвестно произволно квантово състояние, съгласно теоремата за забрана на копирането в квантовата механика. Ева не може да отклони част от сигнала без да прекъсне предаването (това е състояние на поляризация на единичен фотон). Тъй като само Алис знае базиса, в който е подготвено състоянието, всяко измерване извършено от Ева ще унищожи първоначалното състояние с вероятност 1/2, според проекционния постулат на квантовата механика. (Например, ако състоянието е подготвено в базиса H-V и Ева избере да измерва в базиса D-A, тя ще получи фотон в състояние **D** или **A**, вместо в **H** или **V**. Ева препраща измерения фотон на Боб и ако той е избрал базиса, който ползва Алис, тогава (след намесата на Ева) с вероятност 1/2 ще регистрира подготвеното от Алис състояние.) Следователно, грешката при комуникацията, която се генерира при опит за подслушване е 25%. Честота на грешките съдържа информация за съществуването на

потенциален подслушвач и колко той може да знае.

При комуникацията възникват и грешки от друго естество. Величината, която е мярка за всичките тези грешки (включително и от послушване) е известна като Quantum Bit Error Rate (QBER). Нейната стойност се използва за да се гарантира, че комуникацията не е компрометирана.

BB84 с кодиране чрез времеви кутии (time-bin encoding)

За постигане на по-ефективни реализации са създадени и възприети различни варианти на протокола BB84. Негова важна адаптация е BB84 с кодиране чрез времеви кутии (time-bin encoding), което наследява устойчивостта на BB84, като същевременно има по-голяма производителност [6, 7].

В рамките на този протокол изпращат се дискретни еднакво раздалечени сигнали, които се наричат времеви кутии (time bins). Те са групирани по двойки и всяка такава двойка се интерпретира като състояние на кубит. За да се генерира сигнал за тези времеви кутии, използва се кохерентен източник на светлина - лазер.

Ключова разлика между тук подробния протокол и BB84 е фактът, че полезната информация се кодира само в един базис, който тук е представен от състоянията “празно, пълно” и “пълно, празно”, в BB84 реализиран със състояния на поляризация те биха съответствали на състоянията $|H\rangle$ и $|V\rangle$. По тази причина не е необходимо да се изхвърля 50% от комуникацията, което прави този вариант на протокола много по-ефективен.

BB84 с фазово кодиране и състояния примамки

Протоколът BB84 може също да работи с фазово или фазово-времево кодиране, което позволява по-големи разстояния на предаване между подателя (Алис) и получателя (Боб) [8].

3.2 Кохерентен еднопосочен протокол

Протоколът Coherent One-Way (COW) е предложен през 2005 г. и използва атенюирани лазерни импулси за установяване на комуникация вместо единични фотони, което е значително по-рентабилно решение. COW може да се класифицира като протокол за подготовка и измерване на дискретна променлива (DV). Подобно на BB84, целта на COW е да гарантира, че две страни - Алис и Боб, генерират криптографски ключ и законите на квантовата физика ще гарантират, че никоя трета страна не може да получи достатъчно информация за въпросния ключ.

Въпреки че не съществува теоретично доказателство за сигурност за COW, е доказано, че е устойчив срещу индивидуални и колективни атаки, докато неговата сигурност срещу съгласувани атаки е евристична – което означава, че няма теоретично доказателство, но

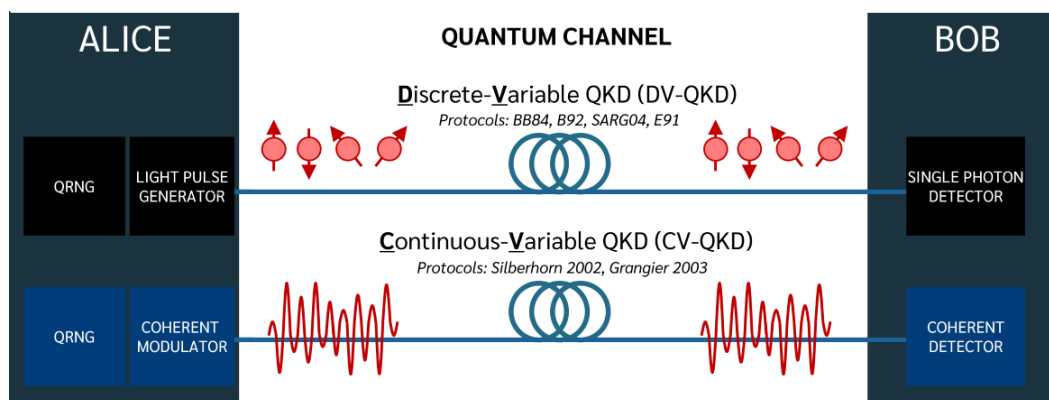
също така няма известна практическа атака срещу него. С изключение на последния клас атаки, сигурността на COW следва от първите принципи на квантовата механика, както и следствия като вече споменатата теорема за забрана на копирането.

3.3 Квантово предаване на секретен ключ с непрекъсната променлива

QKD с непрекъсната променлива (CV-QKD) е много по-обещаваща технология за интегриране в съществуващите телекомуникационни мрежи, въпреки че все още има предизвикателства, които следва да бъдат решени за да получи широко комерсиална употреба.

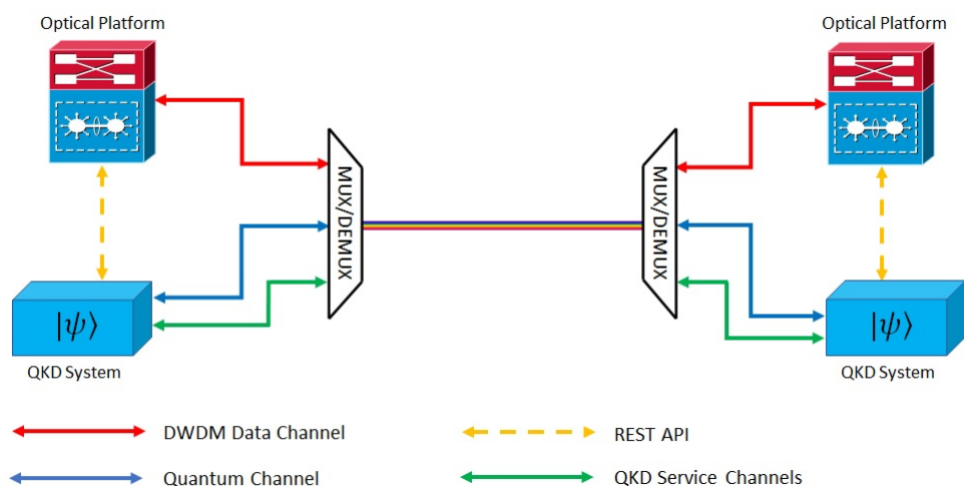
QKD с непрекъсната променлива има следните свойства:

- базирана е на техники за детектиране на кохерентност, използвани и в телекомуникациите;
- технологията е внедрена с използване на стандартни компоненти от телекомуникационната индустрия;
- комуникацията може да става по съществуващи оптични влакна, които едновременно се ползват за пренос и на други данни;
- приемникът на квантовото състояние в CV-QKD използва кохерентно откриване на базата на конвенционални фотодиоди (често използвани в телекомуникациите).



CV-QKD придоби голямо значение през последните години, тъй като системите могат да бъдат произведени с помощта на телекомуникационни компоненти и не изискват SPD, които са скъпа технология, рядко срещана в телекомуникационната индустрия, слабо мащабируема и се нуждае от ниска температура за правилно функциониране. CV-QKD се

счита за най-подходящата технология за интегриране на QKD в настоящите телекомуникационни мрежи.



Това е главно защото CV-QKD, чрез използване на кохерентно откриване, което позволява високо съвместно съществуване (съвместно разпространение) със сигнали за данни по едни и същи оптични влакна, използвайки например DWDM (мултиплексиране с разделяне на плътна вълна).

В CV-QKD се набляга на вълновата природа на светлината, за да се постигне сигурно разпределение на ключовете. При този подход информацията се кодира върху амплитудните и фазовите квадратури на ярък кохерентен лазер от предавателя, а приемникът измерва квадратурите на светлината с помощта на балансирани хомодинни детектори.

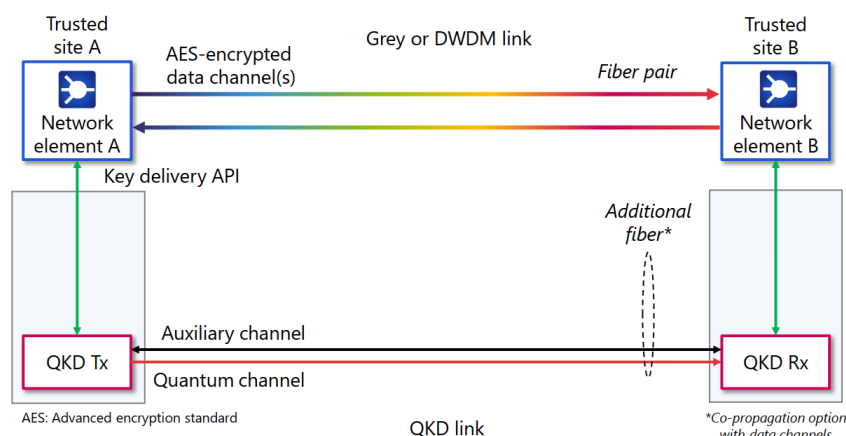
Въпреки че CV-QKD е много по-млада технология, сега тя постига подобни нива на производителност и сигурност като DV-QKD технологиите. CV-QKD обаче предлага значително превъзходен път напред по отношение на цена, форм фактор и производителност, с цената на по-сложна обработка на данни (сложна корекция на грешките).

Технологичният път за CV-QKD използва трите предимства на технологията CV-QKD; високи необработени ключови ставки, намален форм фактор и намалена цена. CV-QKD е съвместим с DWDM, като по този начин поддържа множество канали за постигане на високи ключови скорости, както и поддържа по-гъвкави внедрявания: множество потребители на един оптичен канал, различни топологии и съвместно съществуване със съществуваща телекомуникационна архитектура.

4 Изисквания към инфраструктурата

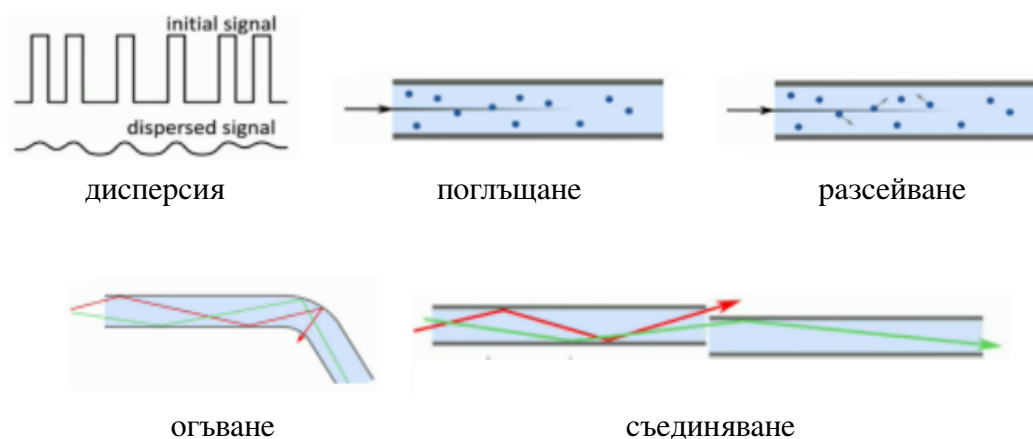
4.1 Параметри на оптичните кабели

Оптичните влакна представляват гръбнака на нашите съвременни комуникационни системи с повсеместно използване от свързване на центрове за данни до връзки на дълги разстояния. В много случаи тези връзки се използват за транспортиране на изключително чувствителна информация.



QKD може да бъде идеално решение за защита на данните с най-високо ниво на сигурност. QKD системите са разработени по начин, който намалява ресурсите, необходими за внедряването им. QKD системите трябва просто да се интегрират с вече съществуващи оптични комуникационни мрежи, без специални изисквания към оптичните кабели.

Съвременните кабели с оптични влакна обикновено са ограничени в това колко далеч могат да пренасят фотони. Обхватът често надминава 100 км. *Естествено, по оптичните влакна има загуби, дължащи се на: дисперсията, абсорбцията, разсейването, огъването, съединяването.* Поглъщането (абсорбцията) и разсейването са неизбежни, защото са резултат от несъвършенството на материалите и производствените технологии..



Фигура 4: Загуби в оптичните влакна.

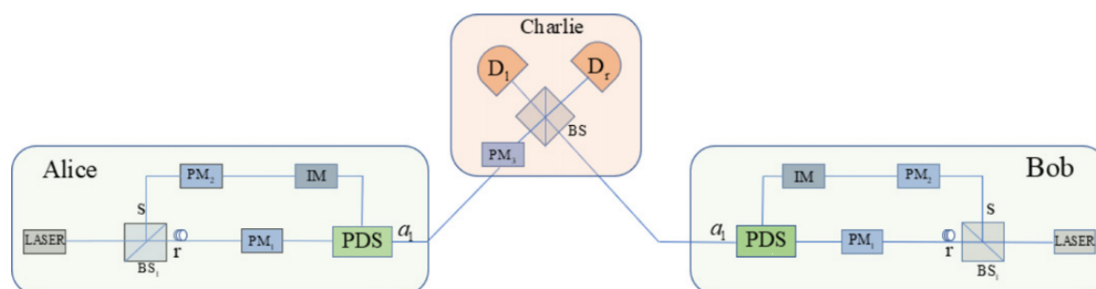
Основните недостатъци на QKD технологиите, използващи оптични влакна при предаването на информацията са:

- много ниско ниво на входния сигнал (< 70 dBm за CV-QKD, единични фотони при DV-QKD);
- невъзможност за усилване или регенериране на сигнала поради неговите квантово-механични свойства;
- ограничено разстояние за предаване и необходимост от релейни станции (т.нар. сигурни възли).

Различни изследователски групи и организации успяват да увеличат обхвата при QKD комуникацията по оптични влакна:

- Университетът на Женева и Corning Inc. конструират система, способна да предаде фотон на 307 km при идеални условия.
- Quantum Xchange стартира Phio, QKD мрежа в САЩ, способна да доставя квантови ключове на практически неограничено разстояние, използвайки чакаща патентована система наречена Phio Trusted Xchange.

Разработват се нови протоколи и технологии за преодоляване на фундаменталното ограничение скорост-разстояние на традиционното QKD, като например Twin-field QKD, което зависи от използваните устройства за QKD.



Фигура 5: Twin-field QKD.

4.2 Комуникация в свободното пространство

Тук терминът “свободното пространство” се отнася за всички приложими среди от естествен произход, които не са оптични влакна (вълноводи):

- въздух/космос близо до земята;
- земна атмосфера;
- вода в реки, езера, морета и океани;
- пространство далеч от Земята – Космос.

Разделянето на 4.2.2 и 4.2.3 е до голяма степен условно и има за цел да подчертае мащаба на използването на различни мобилни платформи - от дронове, включително на голяма надморска височина до самолети, балони и сателити.

4.2.1 Основни инфраструктурни елементи (по важност)

Квантовата комуникация в свободното пространство включва множество основни инфраструктурни елементи, всички от които са важни, но някои могат да се считат за по-критични поради прякото им въздействие върху надеждността, сигурността и ефективността на квантовата комуникационна връзка. Тук представяме едно възможно класиране на тези елементи по тяхната важност.

Следните елементи изглеждат от решаващо значение:

- Квантов източник на светлина: Квантовият източник на светлина, който обикновено генерира единични фотони или заплетени двойки, е фундаментален за квантовата комуникация. Качеството и характеристиките на генерираните квантови състояния пряко влияят върху сигурността и производителността на системата.

- **Квантови детектори:** Специализираните детектори, способни ефективно да измерват квантовите състояния, са от решаващо значение. Точността и ефективността на тези детектори пряко влияят върху надеждността на разпределението на квантовите ключове и други протоколи за квантова комуникация.
- **Протоколи за квантово разпределение на ключове (QKD):** QKD протоколите формират гръбнака на сигурната квантова комуникация. Изборът и прилагането на тези протоколи влияят върху генерирането и споделянето на криптографски ключове, гарантиращи сигурността на комуникацията.
- **Сигурен класически комуникационен канал:** Сигурен класически канал е необходим за класически комуникационни задачи като пресяване на ключове, съгласуване на информация и коригиране на грешки. Сигурността му е от първостепенно значение за предотвратяване на потенциални атаки за подслушване.

От **голямо значение** са следните:

- **Оптични системи за предаване и приемане:** Тези системи, включително компоненти за управление на лъча и фокусиране, са от съществено значение за поддържане на целостта на квантовия сигнал по време на предаване и приемане. Необходим е прецизен контрол, за да се гарантира, че квантовите състояния се доставят правилно.
- **Телескоп и система за управление на лъча:** Телескопите и системите за управление на лъча играят критична роля в насочването на квантово кодирани фотони по връзката на свободното пространство. Тяхната ефективност и прецизност пряко влияят върху цялостната работа на комуникационната връзка.

Следните са със **средна важност**:

- **Квантова обработка на сигнала:** Квантовата обработка на сигнала се справя със задачи като коригиране на грешки и усилване на поверителността. Въпреки че е от съществено значение за осигуряване на целостта на квантовия ключ, неговото въздействие може да бъде донякъде смекчено от напредъка в техниките за коригиране на грешки.
- **Атмосферна компенсация:** Компенсацията за атмосферните условия, включително турбуленцията, е важна за поддържане на стабилността на квантовата комуникационна връзка. Въпреки това напредъкът в адаптивната оптика и други техники подобрява устойчивостта на тези системи.
- **Избор на място:** Изборът на подходящи места за наземни станции е от решаващо значение за минимизиране на смущенията в околната среда. Макар и важен, напредъкът в адаптивната оптика и други технологии може да смекчи някои от предизвикателствата, свързани с избора на място.

Следващите са от **ниска до средна важност**:

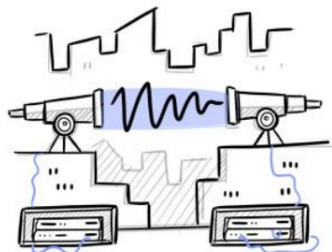
- Контрол на околната среда: Въпреки че поддържането на контролирани условия на околната среда е важно, напредъкът в дизайна и устойчивостта на системата може да помогне за смекчаване на въздействието на факторите на околната среда върху предаването на квантовия сигнал.
- Системи за удостоверяване и оторизация: Удостоверяването и оторизацията са от решаващо значение за цялостната сигурност, но може да не окажат пряко влияние върху надеждността и производителността на квантовата комуникационна връзка.
- Системи за поддръжка и мониторинг: Редовната поддръжка и мониторинг са от съществено значение, но са по-скоро оперативни аспекти, отколкото директни инфраструктурни елементи. Те стават критични за поддържане на дългосрочната функционалност на квантовата комуникационна система.

Въпреки че тази класация предоставя обща насока, важно е да се отбележи, че важността на всеки елемент може да варира в зависимост от конкретните случаи на употреба, технологичния напредък и цялостния дизайн на системата. Напредъкът в една област може да компенсира предизвикателствата в друга, а текущите изследвания продължават да усъвършенстват най-съвременното състояние на квантовата комуникация в свободното пространство.

Тук наблягаме накратко на основните предимства на FSQC и някои казуси и успешни приложения.

4.2.2 QKD в свободно пространство въздух/космос близо до земята

Исторически въздухът/пространството близо до Земята е използвано за предаване на акустични и светлинни (огън или отражение) или други визуални сигнали (особено дим) от много векове чрез прилагане на различни кодове/знаци (например Морз). Всички тези техники се основават на съответните характеристики на въздушния и земния релеф.



В съвременното околоземната въздушно-космическа комуникация се осъществява на базата на радиопредавателни релейни линии/станции. Основното изискване е пряката радиовидимост, като се взема предвид не само профила на релефа. Обичайното разстояние между два възела на линията е под 50 км (като се вземе предвид и кривината на Земята).

Квантовата комуникация в свободното пространство (FSQC) е единственото просто и рентабилно решение в градски райони с голяма плътност без наличие на съответни кабелни връзки. Единствената пречка е сложното градско застрояване и липсата на пряка видимост.

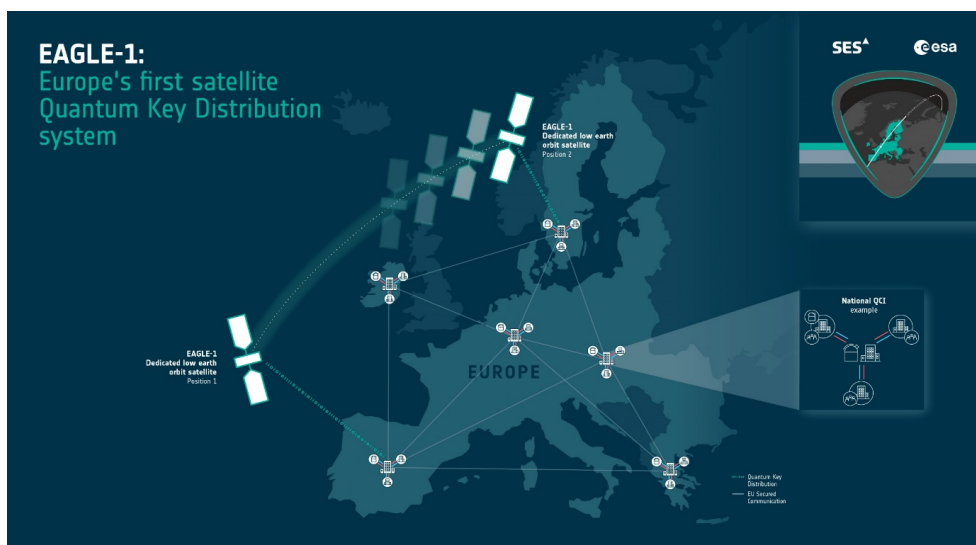
Квантовата комуникация в свободно пространство позволява връзка от точка до точка между две места, без необходимост от оптично влакно и създава редица възможности:

- свързване на отделни оптични влакна по въздушен път;
- избягване на сигурните възли (trusted nodes);
- целодневни операции;
- лесно транспортиране на техниката до различни места
- подходяща е за организации (финансови, правителствени и военни институции), разположени в градски райони;
- лесно интегриране с градски мрежи с оптични влакна.

Това е най-доброто решение за онези места, които не са свързани с оптични кабелни връзки и изискват бърза и/или непостоянна квантова комуникационна връзка. Това е и единственото решение за комуникация с движещи се платформи като дронове, платформа за голяма надморска височина, самолети, кораби.

4.2.3 Земно атмосферна FSQC/сателитна квантова комуникация

Тъй като технологичната зрялост на квантовия повторител все още е далеч от конкретни приложения, най-ефективният начин за разширяване на квантовата комуникация и QKD в глобален мащаб е използването на сателити и наземни станции, които обменят единични фотони.



Фигура 6: В Европейския съюз Eagle-1 ще демонстрира осъществимостта на технологията за квантово разпределение на ключове с помощта на сателитна система. Той ще демонстрира и валидира QKD технологии за разпространение от ниска земна орбита до Земята, ще предоставя ценни данни за разработването и внедряването на EuroQCI и ще бъде интегриран в европейската система за защитена комуникация.

Космическата квантова комуникация изисква способности за проектиране и разработване както на оптичните, така и на квантовите комуникационни системи, разположени на сателита, както и способности за реализиране на специални телескопи, свързани с квантовия хардуер на земята.

Ключова бариера пред квантовите комуникации на дълги разстояния е свързана със загубите - от абсорбция и разсейване - причинени от светлината, пътуваща по оптични влакна или през атмосферата. Докато в класическите комуникации оптичните усилватели могат да се използват като повторители, които компенсират такива загуби, усилването на отделни фотони разваля тяхната квантова информация. Изследователите изследват различни технологии за квантови повторители, които биха могли да преодолеят това ограничение, но квантовите повторители скоро няма да бъдат готови да поддържат междуконтинентални квантови комуникации. Единственият жизнеспособен, краткосрочен подход се предлага от оптичния канал за свободното пространство, свързващ сателити в ниска околоземна орбита със Земята. Предимството на този подход е, че пътят на предаване на фотоните - с изключение на долните 10 km от атмосферата - е практически във вакуум, с незначително поглъщане и разсейване. Сателитна връзка между две наземни станции на 1200 km една от друга (както в демонстрацията на Micius от 2017 г. [12]) е с 15 порядъка по-ефективна по отношение на загубите от връзка с оптични влакна.

4.2.4 Проблеми със сигурността и надеждността

Сигурността и надеждността на FSQC могат да бъдат компрометирани от различни заплахи от естествен и изкуствен източник:

- **Естествени заплахи:**

- Атмосферни условия: атмосферната турбуленция, абсорбцията и разсейването могат да влошат качеството на квантовия сигнал по време на предаване – адаптивните оптични системи могат да компенсират атмосферната турбуленция и внимателният избор на място може да минимизира въздействието на атмосферните условия.
- Намеса в околната среда: природни събития като бури, светкавици и други фактори на околната среда могат да нарушат работата на квантовата комуникационна инфраструктура – контрол на околната среда и защитни мерки могат да бъдат приложени, за да се сведе до минимум въздействието на неблагоприятните метеорологични условия.
- Космическо лъчение: високоенергийните космически лъчи могат да причинят грешки в квантовите детектори и да въведат шум в квантовите комуникационни системи – техниките за екраниране и коригиране на грешки могат да помогнат за намаляване на въздействието на космическото лъчение върху квантовите системи.

- **Изкуствени заплахи:** Подслушване, кибератаки, заглушаване, смущения от изкуствени източници на светлина, саботаж или физически атаки, технологични уязвимости, прекъсвания на захранването и повреда на инфраструктурата.

Внедряването на FSQC инфраструктура за военни или чувствителни приложения въвежда специфични проблеми и уязвимости по отношение на сигурността. Както военните, така и терористичните заплахи могат да бъдат насочени към различни основни елементи на тази инфраструктура. Ето някои основни заплахи:

- **Военни заплахи:**

- Подслушване и прихващане на сигнали: противниците могат да се опитат да прихванат квантови сигнали по време на предаване, за да получат достъп до чувствителна информация – прилагане на усъвършенствани протоколи за разпределение на квантови ключове (QKD) и непрекъснат мониторинг за признаци на подслушване.
- Кибер война: кибератаките, насочени към класическите комуникационни канали и системи за контрол на квантовата инфраструктура, могат да компрометират нейната сигурност и функционалност – стабилните мерки за киберсигурност, криптирането и защитените комуникационни протоколи са от съществено значение за предотвратяване на неотторизиран достъп и подправяне.

- Заглушаване и смущения: умишленото заглушаване на квантови сигнали или електромагнитни смущения могат да нарушат комуникацията – използвайки технологии против заглушаване, прескачане на честотата и резервиране, за да се гарантира устойчивостта на комуникационната връзка.
- Физически атаки: саботаж, вандализъм или физически атаки срещу критични инфраструктурни компоненти могат да компрометират цялата квантова комуникационна система – прилагане на строги мерки за физическа сигурност, наблюдение и резервиране в критични компоненти. Персоналът по сигурността и системите за наблюдение могат да помогнат за откриване и реагиране на физически заплахи.
- Вътрешни заплахи: компрометирани или злонамерени вътрешни лица могат да представляват заплаха за сигурността на квантовите комуникационни системи — строг контрол на достъпа, фонове проверки и непрекъснат мониторинг на персонала с достъп до чувствителни системи могат да помогнат за смекчаване на вътрешните заплахи.

• **Терористични заплахи:**

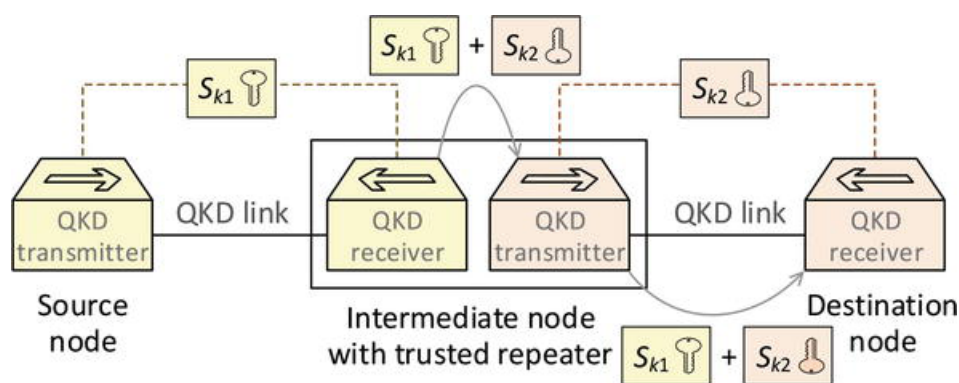
- Прекъсване на критична инфраструктура: терористичните организации могат да се насочат към критични инфраструктурни компоненти, като телескопи или контролни центрове, за да нарушат квантовите комуникационни операции – укрепването на инфраструктурата, прилагането на мерки за сигурност и разполагането на критични компоненти на сигурни места може да намали уязвимостта към физически атаки.
- Кибер тероризъм: кибератаки, целящи компрометиране на целостта или наличността на квантовите комуникационни системи – стабилни практики за киберсигурност, редовни одити и проактивни мерки за справяне с потенциални уязвимости могат да подобрят устойчивостта на системата.
- Злоупотреба с квантова технология: неоторизиран достъп или злоупотреба с квантова технология от терористи за злонамерени цели – строг контрол и регулиране на достъпа до квантова технология, както и мерки за предотвратяване на незаконно придобиване или развитие на квантови комуникационни способности.
- Враждебно поглъщане или окупация: терористичните групи могат да се опитат физически да превземат или окупираят съоръжения, хостващи квантова комуникационна инфраструктура – мерки за сигурност, наблюдение и сътрудничество с правоприлагащи органи и военни структури за предотвратяване на неоторизиран достъп и окупация.
- Използване на квантови уязвимости: терористите може да се опитат да използват уязвимостите в квантовите комуникационни протоколи или хардуера за злонамере-

ни цели – редовни актуализации, изследвания и сътрудничество с научната общност за справяне и отстраняване на потенциални уязвимости в квантовата технология.

Борбата с военните и терористичните заплахи за квантовата комуникационна инфраструктура в свободното пространство изисква всеобхватен и многостранен подход, включващ напреднали технологии, мерки за физическа сигурност и международно сътрудничество за гарантиране на целостта и сигурността на чувствителните квантови комуникационни системи.

4.2.5 Сигурни възли (Trusted nodes)

Скоростта на споделяне на секретни ключове и разстоянието на което може да се осъществи директно споделяне са ограничени поради затихването на слабите квантови сигнали. Квантовите повторители са отвъд всякакви практически технологии днес. Практично решение на проблема са сигурните повторителни възли (*trusted nodes*). Секретните ключове, генерирани в първата QKD връзка, се предават към отдалечен възел в мрежата чрез криптирането им със секретните ключове, генерирани в междинните възли. Секретните ключове са в безопасност, само ако всички междинни възли (*trusted nodes*), чрез които се извършва “ретранслация” са сигурни.



Фигура 7: QKD с един междинен сигурен възел.

На фигура 7:

- QKD приемникът в целевия възел установява QKD връзка с предишния QKD предавател в междинния възел;
- двата QKD линка генерират независимо секретни ключове S_{k1} и S_{k2} , съответно;
- секретният ключ S_{k1} се криптира със секретния ключ S_{k2} и се предава до целевия възел (destination node);

- секретният ключ S_{k1} , след като е споделен, се използва за защита на комуникациите между подателя и получателя;
- този процес на предаване може да продължи с произволно количество междинни възли;

Във стандарта **ETSI GS 014 QKD** сигурен възел (trusted node, TN) е дефиниран по следния начин: възел в QKD мрежата, съдържащ надеждно оборудване, включително едно или повече устройства за управление на ключове и едно или повече QKD устройства, разположени в помещения с гарантирана сигурност.

Към момента няма стандартни изисквания за сигурен възел и обезпечаване на сигурността. Предполага се физическа сигурност и наблюдение, включително огради, камери, стени, наблюдение от оператор и т.н., което предлага физическа защита на критични компоненти, включително QKD релейни възли. По-подробна дефиниция се очаква да бъде посочена в ITU-T SG17 и SG13 през март 2024 г.

5 Оборудване за QKD

Този раздел има за цел да предостави практическа информация относно настройването на QKD оборудването като цяло. Настройването на QKD оборудването включва извършването на няколко стъпки.

Подготвяне на физическото оборудване

Първата стъпка е физическото подготвяне на QKD оборудването. Включва разопаковане, монтаж в шкаф (ако е приложимо), свързване на квантов канал, сервизен канал и всички други необходими връзки. Трябва да се следва процедурата, описана в документацията, предоставена от доставчика на оборудването.

Начална конфигурация

Обикновено тази стъпка включва настройка или промяна на администраторска парола, IP адрес за управление, настройка на правилния час и дата, тъй като QKD протоколите са чувствителни към часовата разлика между системите. Трябва да се следва процедурата, описана в документацията, предоставена от доставчика на оборудването.

Конфигуриране на QKD системата да приема свързвания от клиенти.

Основната цел на QKD оборудването е сигурно да обменя секретни ключове и да ги предоставя на доверен клиент за използване. За да изпълнява функцията за предоставяне на ключове на клиенти, QKD оборудването трябва да бъде конфигурирано според изискванията на стандарта. За установяване на доверителна връзка с клиенти се използва класическа схема на инфраструктура на публичен ключ (PKI): QKD оборудването трябва да има СА (Certificate Authority) сертификат на органа, който е подписал сертификата на клиента.

Клиентът трябва да има СА сертификат на органа, който е подписал QKD сертификат за оборудване. Подробните стъпки как това може да се направи се различават за различните устройства и затова трябва да се използва документацията, предоставена от доставчика.

Конфигуриране на логическите връзки между крайните точки

QKD мрежата може да бъде сложна и логическите връзки трябва да бъдат конфигурирани, за да позволят на крайните QKD системи и техните клиенти да комуникират успешно. Това може да включва използването на сигурни възли (trusted nodes), през които се предават ключове, за да достигнат крайните си дестинации.

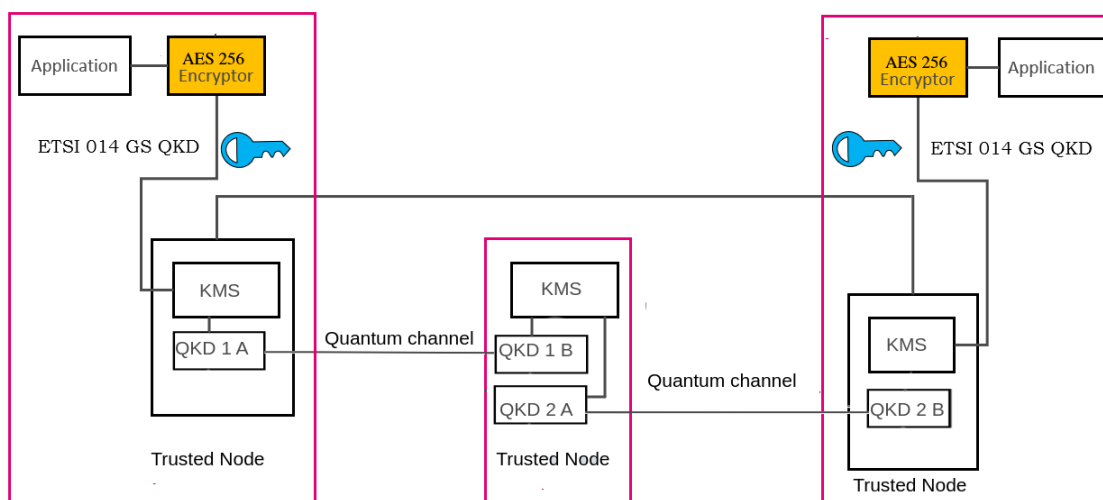
6 Интегриране на платформите за QKD с класически криптиори AES 256

AES (англ. Advanced Encryption Standard) е вариант на симетричен блок шифър на Rijndael. Той е избран от правителството на САЩ за защита на класифицирана информация. Националният институт за стандарти и технологии (NIST) започва разработването на AES през 1997 г., като заместител на стандарта за шифроване на данни DES (англ. Data Encryption Standard), който стана уязвим на brute-force атаки.

QKD е подходящо решение за генериране и обмен на ключове за AES 256 по сигурен начин. Избрахме тази комбинация, от QKD и AES 256, при за изграждането на първата QKD мрежа в България, която е част от Европейската квантово-комуникационна инфраструктура.

Практическата цел на интегрирането на QKD платформи с криптиори AES 256 е да се гарантира, че ключовете, разпространявани от QKD системите, се използват по сигурен начин. Следователно интеграцията изисква внимателно планиране. Някои аспекти на интеграцията включват:

- избор на тип PKI сертификати (RSA, ECC и др.) за комуникация между QKD системите и крипторите;
- избор на Certificate Authority (CA), който ще подписва сертификатите;
- установяване на сигурна връзка между QKD системи и криптиори, използвайки подписани сертификати.



Фигура 8: QKD мрежа с три възли и интегрирани AES 256 криптиори.

Подробните стъпки как това може да се направи се различават за различните устройства и за целта се използва документацията, предоставена от доставчика.

7 Литература

- [1] W. Wootters, W. Zurek, A Single Quantum Cannot be Cloned, *Nature*. 299 (5886): 802–803, doi:10.1038/299802a0. S2CID 4339227, (1982).
- [2] D. Dennis, Communication by EPR devices, *Physics Letters A*. 92 (6): 271–272 doi:10.1016/0375-9601(82)90084-6, (1982).
- [3] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, p. 8. New York, (1984).
- [4] W. Tittel, G. Ribordy, and N. Gisin, Quantum cryptography, *Physics World*, 11:41–45, (1998).
- [5] Raúl García-Patrón, Franco N. C. Wong and Jeffrey H. Shapiro, Optimal individual attack on BB84 quantum key distribution using single-photon two-qubit quantum logic, *Proc. SPIE 7702*, 77020C (2010).
- [6] Boaron, A. et al., Secure quantum key distribution over 421 km of optical fiber, *Physical Review Letters*, 121(19). doi:10.1103/physrevlett.121.190502, (2018).
- [7] Bacco, D. et al, Boosting the secret key rate in a shared quantum and classical fibre communication system, *Communications Physics*, 2(1). doi:10.1038/s42005-019-0238-1, (2019).
- [8] K. Inoue, Quantum key distribution technologies. Selected Topics in Quantum Electronics, *IEEE Journal of*. 12. 888 - 896. 10.1109/JSTQE.2006.876606, (2006).
- [9] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.*, 91(5), 057901, <https://doi.org/10.1103/PhysRevLett.91.057901>, (2003).
- [10] Kržič, A., Sharma, S., Spiess, C. et al., Towards metropolitan free-space quantum networks, *npj Quantum Inf* 9, 95 (2023). <https://doi.org/10.1038/s41534-023-00754-0>
- [11] C. Y. Lu et al., Micius quantum experiments in space, *Rev. Mod. Phys.* 94, 035001 (2022).
- [12] J. Yin et al., Satellite-based entanglement distribution over 1200 kilometers, *Science* 356, 1140 (2017).



EuroQCI



www.euroqci.bg

Проект 101091399 "BG National QCI Plan" е финансиран от Европейския съюз. Изразените възгледи и мнения са само на автора(ите) и не отразяват непременно тези на Европейския съюз или Европейската комисия. Нито Европейският съюз, нито финансиращият орган могат да носят отговорност за тях.