Квантова криптография и квантови протоколи

Автор: Йорданка Жечева

04/01/2025

Квантовата криптография е област от криптографията, която използва принципите на квантовата механика за защита на комуникациите и данните. Тя се основава на уникалните свойства на квантовите частици, като фотони, които могат да се използват за създаване на криптографски системи, които са теоретично неуязвими за подслушване. Квантовата криптография е новаторска, защото възползва от самата природа на квантовите системи, за да осигури сигурност, която е извън обсега на традиционните криптографски методи.

Основни принципи на квантовата криптография

1. **Принципът на неопределеността (Heisenberg Uncertainty Principle)**: В квантовата механика, принципът на неопределеността на Хайзенберг гласи, че не е възможно да се измерват точно два свързани параметъра на квантова частица (например, позиция и импулс) едновременно. Това означава, че ако някой се опита да измери или подслуша квантова част от информацията (като фотон), той ще промени състоянието на частицата. Това прави всякакво подслушване лесно откриваемо.

2. **Принцип на суперпозицията**: Квантовите частици могат да съществуват в множество състояния едновременно, докато не бъдат измерени. Това се нарича суперпозиция. Например, при квантовата криптография може да се използва суперпозиция на фотони, които могат да бъдат в различни състояния на поляризация. Тези състояния могат да се използват за кодиране на информация, като при подслушване или неоторизирани действия ще настъпи промяна в състоянието на фотона, което ще сигнализира за компрометиране на комуникацията.

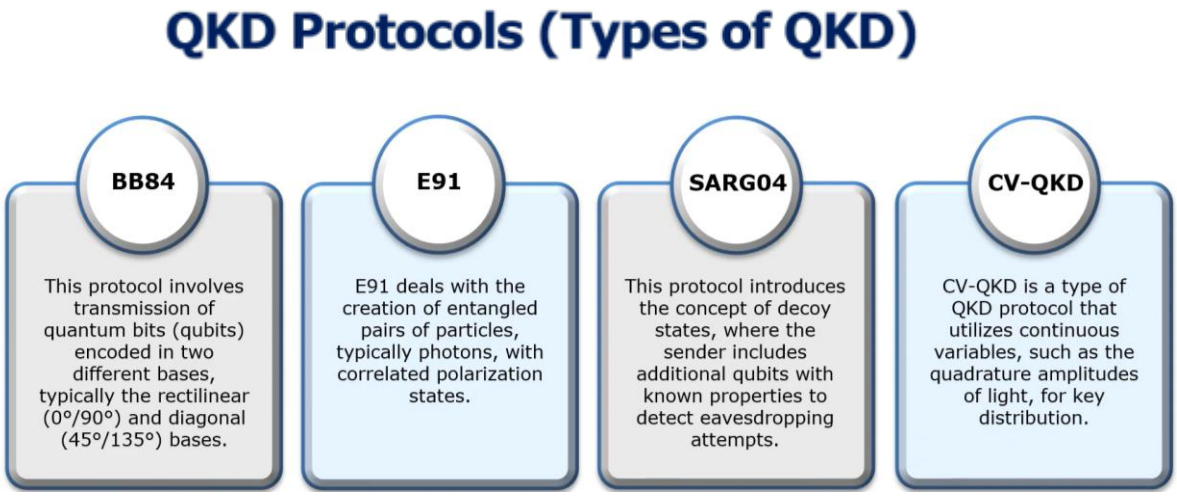
3. **Принцип на квантовата заплетеност (Quantum Entanglement)**: Квантовата заплетеност е феномен, при който две частици могат да бъдат в тясно свързано състояние, така че състоянието на една частица е зависимо от

състоянието на другата, независимо колко далеч се намират те. Това свойство може да се използва за създаване на сигурни канали за обмен на информация, като ако някой се опита да подслушва или интерферира с информацията, ще се наруши заплетеността и ще бъде открито.

Квантова криптография в практика: Квантова ключова разменяна система (Quantum Key Distribution - QKD)

Един от най-известните и широко изследвани методи за квантова криптография е **квантовата ключова разменяна система (QKD)**. QKD позволява на две страни да обменят секретни ключове за шифриране на съобщения, като същевременно осигуряват, че никой трети участник не може да подслушва и копира ключа без да бъде открит. Например квантовите протоколи:

За разлика от класическата криптография QKD и свързаните с него протоколи използват принципите на квантовата механика, за да установят присъщо защитена Public-Key Crypto-System. Тези протоколи притежават забележителната способност да откриват всеки опит за подслушване в системата, като гарантират целостта на процеса на обмен на ключове.



Източник: https://www.youtube.com/watch?v=gnk8VoMsvO8

Encryption Consulting LLC·3.04.2024 г.

Протоколът на BB84

Протоколът **BB84** е първият публично известен протокол за **квантово разпределение на ключове** (Quantum Key Distribution - QKD), разработен през **1984** година от **Чарлз Бенет** и **Жил Браво**. Този протокол е в основата на много от съвременните квантови криптографски системи и е предназначен за осигуряване на сигурен начин за обмен на криптографски ключове между две страни, използвайки квантови принципи.

Протоколът BB84 използва **квантови битове** или **квантови състояния** (известни като **кюбити**), които могат да бъдат измервани и кодирани в различни състояния. Основният му принцип е, че всяко подслушване на квантовия канал води до промяна в състоянието на прехвърлените частици (например фотони), което прави подслушването откриваемо.

Основни елементи на протокола BB84

1. **Състояния на фотони**: Протоколът използва **четири основни състояния на фотони**, които се определят чрез две различни бази за поляризация:

Базис 1 (хоризонтална и вертикална поляризация):

Хоризонтална поляризация (0°): представя 0

Вертикална поляризация (90°): представя 1

Базис 2 (диагонална и антидиагонална поляризация):

Диагонална поляризация (45°): представя 0

Антидиагонална поляризация (135°): представя 1

Тези четири състояния се използват за кодиране на информацията, която ще бъде разменяна между двама участници, наречени **Изпращач** и **Получател**.

2. **Стъпки на протокола**:

Стъпка 1: Изпращачът избира състояния на фотоните
Изпращачът избира произволно едно от четирите състояния (половината от тях в базис 1, а половината в базис 2). Той изпраща фотоните през квантовия канал към получателя, като всеки фотон се изпраща с един от тези четири състояния.

Стъпка 2: Получателят измерва състоянията
Получателят измерва състоянието на всяко получено фотонно съобщение, като избира произволно между двата базиса (хоризонтален/вертикален или

диагонален/антидиагонален). Важно е, че ако получателят избере същия базис, в който е изпратено състоянието на фотона, той ще получи правилния резултат (0 или 1). Ако избере различен базис, резултатът от измерването ще бъде случаен.

Стъпка 3: Обмен на информация за базите (не за състоянията) След като получателят измери състоянията, той информира изпращача по открит канал (например, чрез класически канал) кои бази е избрал за всяко измерване. Те не разкриват самите измервания, а само използваните бази.

Стъпка 4: Изхвърляне на не съвпадащите измервания След този обмен на информация, и изпращачът, и получателят премахват тези измервания, за които базите не съвпадат. Така остава само част от фотоните, за които и двамата са използвали същия базис.

Стъпка 5: Изграждане на споделен ключ След като са изхвърлили не съвпадащите измервания, получателят и изпращачът ще имат еднакви стойности за съответните фотони. Тези стойности се използват за изграждане на споделен криптографски ключ.

3. **Подслушване и сигурност**: Ако някой (например, "Човек в средата") се опита да подслушва комуникацията, той ще трябва да измери фотоните. Обаче, поради **принципа на неопределеността на Хайзенберг** и **състоянията на суперпозиция**, всяко измерване ще промени състоянието на фотона. Това означава, че подслушвателят не може да получи точната информация, без да повлияе на фотоните. Когато изпращачът и получателят сравняват своите резултати за базите, те ще открият дали някой е подслушвал комуникацията, тъй като разликите в резултатите ще се появят заради измерванията, извършени от подслушвателя.

4. **Откритие на подслушване**: Ако има подслушване, изпращачът и получателят ще открият несъответствия в стойностите на съобщенията. Това може да се направи, като сравнят част от резултатите си (например, 10% от ключа). Ако има значителни разлики, те ще разпознаят, че комуникацията е била компрометирана и ще започнат процеса на обмен отново.

Приложения на протокола BB84

Протоколът BB84 има голямо значение в области, които изискват висока сигурност, като например:

- **Разпределение на ключове за криптиране**: Използва се за разпределяне на ключове, които могат да се използват за осигуряване на секретността на комуникации чрез симетрични криптографски методи.
- **Квантови мрежи**: Протоколът BB84 е основа за изграждането на бъдещи квантови мрежи, които могат да осигурят не само защита на ключове, но и на самите съобщения.
- **Безопасни комуникации**: Системите за квантово разпределение на ключове могат да се използват за гарантиране на сигурността в области като правителствени комуникации, военни приложения, финансови транзакции и др.

Протоколът **BB84** представлява основния камък на квантовата криптография и доказва как принципите на квантовата механика могат да се използват за изграждане на сигурни комуникационни системи. Чрез свойствата на квантовите състояния, като **суперпозиция** и **неопределеност**, BB84 осигурява начин за създаване на криптографски ключове, които са теоретично защитени срещу всяко подслушване, което прави този протокол уникален и важен за бъдещето на сигурността на данни.

Протоколът E91

е протокол за **квантова ключова размяна** (Quantum Key Distribution - QKD), предложен през 1991 г. от **Артур Екерт** (Arthur Ekert). Той е втори по значимост след **BB84** и е важен, защото използва **квантова заплетеност** (quantum entanglement) за осигуряване на сигурността при обмена на криптографски ключове между две страни. Протоколът E91 предлага сигурност, основана на квантовата механика и феномена на **квантовата заплетеност**, което дава на участниците способността да откриват евентуално подслушване на комуникацията.

Как работи протоколът E91?

Протоколът E91 се различава от **BB84**, тъй като той използва **квантова заплетеност** между фотонни двойки вместо просто отделни фотони. Това използване на заплетени фотони е ключово за сигурността на комуникацията.

1. Заплетени фотони

В протокола E91, източник на фотони генерира **пари от заплетени фотони** (напр. два фотона с противоположни поляризации). Заплетените фотони имат специалното свойство, че състоянието на един фотон е силно свързано със състоянието на другия, независимо колко далеч се намират те. Този феномен е известен като **квантова заплетеност**.

Фотоните в парите са подредени така, че те могат да имат определени резултати, когато се измерват, например, в посока на поляризацията.

2. Изпращач и получател

След като са създадени заплетените двойки фотони, те се изпращат през квантов канал към двата участника в комуникацията (например, Изпращач и Получател).

- **Изпращачът** измерва поляризацията на един от фотоните в заплетената двойка (например, избира да използва базата за измерване по X или Y).
- **Получателят** измерва поляризацията на втория фотон в двойката, използвайки същата базисна ориентация.

3. Измервания на фотоните

- Всеки от участниците извършва измерванията си върху фотоните. Тъй като фотоните са заплетени, резултатите от тези измервания ще бъдат **свързани** помежду си.
- За всяка измерена двойка, участниците ще получат противоположни резултати (напр. ако Изпращачът получи резултат 0, Получателят ще получи 1, и обратно).

4. Обмяна на информация

След извършване на измерванията, Изпращачът и Получателят обменят информация относно избора на базисите за измерванията (но не и самите резултати). Те правят това по **класически канал**.

- Ако и двамата участници са използвали една и съща базисна ориентация за измерване, тогава техните измервания ще бъдат корелирани, и те ще могат да използват тези измервания за генериране на споделен ключ.
- Ако базисите не съвпадат, измерванията ще бъдат случайни и ще се изхвърлят.

5. Създаване на ключа

От тези измервания, които са извършени с един и същ базис, Изпращачът и Получателят могат да създадат **споделен криптографски ключ**. Това се прави чрез процеса на **съгласуване на ключовете**: те сравняват някаква част от своите резултати и съвпаденията, за да идентифицират общия ключ.

6. Откриване на подслушване

Ако някой трети участник се опита да подслушва комуникацията, той ще се опита да измери фотоните на някой от участниците. Поради **квантовата заплетеност** на фотоните, всяко измерване от подслушвателя ще наруши заплетеността на фотоните и ще доведе до **непокритие** (или грешки) в резултатите на Изпращача и Получателя.

Когато Изпращачът и Получателят сравнят част от резултатите си (например 10% от измерванията), те ще могат да открият аномалии, които показват, че комуникацията е била компрометирана.

Ако има висока степен на грешки (които са извън допустимото), те могат да решат да прекратят обмена и да започнат процеса отново, защото подслушването е било открито.

Сигурност на протокола E91

Протоколът E91 е **сигурен** на основата на **квантовата заплетеност**, която предлага значителни предимства:

1. **Неоткриваемост на подслушването**: Подслушвателят не може да измерва или копира квантовата информация без да наруши състоянието на фотоните, което прави всяко подслушване откриваемо.
2. **Теоретична сигурност**: Протоколът предлага сигурност, която е гарантирана от самата квантова механика, а не от математически проблеми, които

могат да бъдат решени с напредъка в изчислителната мощност (например, квантовите компютри).

3. **Откриване на атаки**: Ако някой се опита да извърши "човек в средата" атака (intercept-resend), пренасочвайки фотоните, те ще нарушат квантовата заплетеност, което ще бъде открито от получателя при проверката на резултатите.

Приложения на протокола E91

Протоколът E91, като част от квантовата криптография, може да бъде използван в различни приложения, където сигурността на комуникациите е критична:

- **Квантови мрежи**: Протоколът може да бъде използван за изграждане на бъдещи квантови комуникационни мрежи, които могат да предложат пълна сигурност, като гарантират, че подслушването е невъзможно без да бъде открито.
- **Безопасен обмен на ключове**: Използва се за генериране на ключове за криптиране, които могат да се използват за симетрично криптиране на данни.
- **Квантови криптографски системи**: E91 е основа за много съвременни квантови криптографски технологии и проекти, които предлагат не само защита на данни, но и защита срещу бъдещи квантови компютри, които биха могли да нарушат традиционните криптографски системи.

Протоколът **E91** е важен етап в развитието на квантовата криптография, който използва принципите на **квантовата заплетеност** за разпределяне на криптографски ключове. Той осигурява високото ниво на сигурност благодарение на уникалните свойства на квантовите частици и предоставя ефективен начин за откритие на подслушване, което го прави перспективен за изграждане на квантови мрежи и системи с висока сигурност.

Протоколът SARG04

(или **SARG** – *State-Authenticated Random Generation*) е квантов криптографски протокол, който е предназначен да осигури сигурност при **квантово разпределение на ключове** (Quantum Key Distribution - QKD) чрез използването на **квантови състояния**, които са автентифицирани по начин, който

ги прави устойчиви на атаки. Този протокол е представен през **2004** г. от **Xiang-Bin Wang** и други изследователи като подобрение на предишни квантови криптографски протоколи, като например **BB84** и **E91**, с цел да се решат някои от проблемите с тяхната сигурност.

Основни цели на SARG04

Протоколът SARG04 е създаден с цел да подобри сигурността и да се защити от различни **атаки с подслушване** (interception attacks) и **атаки със злоупотреба с повторно използване на ключове**. Той съчетава идеите за квантова криптография, като същевременно предлага **методи за автентикация**, които предпазват от подслушване и манипулации с предаваните съобщения.

Как работи протоколът SARG04?

Протоколът SARG04 използва **квантови състояния на фотоните** и работи по начин, подобен на класическите протоколи за квантово разпределение на ключове, като BB84, но с ключова разлика: вместо да се използват стандартни фотонни състояния за създаване на ключове, SARG04 се опитва да избегне възможността за подслушване чрез използването на нови методи за автентикация и проверка на състоянията на фотоните.

Ето как обикновено протича процесът:

1. **Изпращане на заплетени състояния**: Изпращачът генерира **заплетени фотони** в състояния, които са **проверени и автентифицирани**. Тези състояния са подредени така, че да позволяват на получателя да ги измери по определен начин, което намалява вероятността за манипулации.
2. **Измервания на фотоните**: Получателят извършва измервания на получените фотони и ги записва. Ключовата разлика в протокола SARG04 е, че тези измервания са **автентифицирани** – те се извършват по начин, който може да бъде проверен.
3. **Автентикация на измерванията**: Изпращачът и получателят използват специфични методи за **сравняване** и **проверка** на измерванията, за да се уверят, че те не са били манипулирани. Това добавя **допълнителен слой сигурност** към процеса на разпределяне на ключа, като предотвратява **атаки с подслушване** или **повторно използване на ключове**.

4. **Генериране на споделен ключ**: След като се извърши автентикацията и проверката на състоянията на фотоните, Изпращачът и Получателят генерират **криптографски ключ**, който ще бъде използван за сигурна комуникация. Това се прави чрез съвпадение на измерванията и състоянията, които те са споделили, като в процеса се изхвърлят несъответствията и грешките.

5. **Откриване на подслушване**: Ако някой трети участник се опита да подслушва комуникацията, това ще доведе до нарушаване на автентикацията и ще бъде открито от Изпращача и Получателя при сравняване на част от измерванията им.

Основни предимства на SARG04

1. **Подобрена сигурност**: SARG04 осигурява допълнителен слой автентикация, което прави комуникацията по-сигурна в сравнение с други квантови протоколи като **BB84**, които са уязвими на атаки, свързани с **повторно използване на ключове** или **неправилно измерване** на състоянията на фотоните.

2. **Откритие на манипулации**: Чрез автентикацията и проверката на състоянията на фотоните, SARG04 позволява откритие на подслушване и манипулации, което го прави много ефективен срещу различни типове атаки.

3. **Гарантирана защита срещу атаки с "човек в средата"**: Протоколът защитава срещу атаки с "човек в средата" (Man-in-the-Middle), които са често срещани в традиционните криптографски системи, като в този случай подслушвателят не може да прехване или манипулира ключовете, без да бъде открит.

Защо SARG04 е важен?

1. **Сигурност и автентикация**: Механизмите за автентикация в SARG04 добавят допълнителен слой защита срещу атаки. Това прави протокола изключително подходящ за чувствителни комуникации, които изискват висока степен на сигурност, като например финансови транзакции, правителствени комуникации и военни приложения.

2. **Съответствие с квантовата механика**: Както всички протоколи за квантова криптография, SARG04 се основава на принципите на квантовата механика, като използва квантовата заплетеност и други специфични за квантовата физика свойства, за да осигури сигурността на комуникацията. Тези свойства осигуряват, че всяко подслушване или манипулация ще бъде открито.

Протоколът **SARG04** е значителен напредък в развитието на **квантовата криптография**, като предлага нови методи за **автентикация** и **проверка** на измерванията, което гарантира по-висока сигурност в разпределението на криптографски ключове. С помощта на **квантова заплетеност** и допълнителни механизми за автентикация, той е по-сигурен и устойчив на атаки в сравнение с по-старите протоколи като **BB84**. Това го прави важен избор за изграждане на квантови комуникационни мрежи и приложения, които изискват висока степен на сигурност.

CV-QKD (Continuous-Variable Quantum Key Distribution) е вид **квантова ключова разпределителна система** (QKD), която използва **непрекъснати променливи (continuous variables, CV)** за създаване на криптографски ключове. В контекста на квантовата криптография, непрекъснатите променливи обикновено се свързват с **положението** и **импулса** на фотоните или други квантови състояния, вместо да се използват отделни **кюбити** (квантови битове), както в протоколите като **BB84** и **E91**.

CV-QKD се предлага като **алтернатива** на традиционните дискретни квантови протоколи, като BB84, и има значителни предимства, особено в контекста на практическото приложение на квантовите комуникации.

Основни характеристики на CV-QKD:

1. **Непрекъснати променливи**: В **CV-QKD** се използват непрекъснати променливи, като амплитудата и фазата на електрическите полета на фотоните. Въпреки че основната идея на **QKD** е да осигури секретен криптографски ключ, при CV-QKD, вместо да се използват дискретни състояния на фотоните (като при BB84), се използват **класически променливи**, като например:

- Позицията и **импулсът** на квантови състояния.

- **Амплитуда** и **фаза** на квантовите полета.

2. **Използване на квантови оптични техники**: За осъществяване на CV-QKD се използват **квантови оптични техники**, които включват **интерферометрия**, **оптични измервания** и **принципи на квантова механика** (като квантова суперпозиция и индетерминираност). Протоколът включва използването на фотонни пътеки и измервания, за да се разпределят сигурни криптографски ключове.

3. **Генериране на ключ**: Процесът на генериране на споделен ключ в CV-QKD обикновено включва два основни етапа:

Етап 1: Изпращане на квантови състояния: Изпращачът генерира квантови състояния, които включват непрекъснати променливи (например амплитуда и фаза) и ги изпраща към получателя.

Етап 2: Измервания и ключова преработка: Получателят измерва тези състояния и сравнява получените резултати с тези на изпращача чрез класически канал. След това използват тези измервания, за да генерират общ ключ. За постигане на висока сигурност, те могат да използват корекция на грешки и автентикация.

4. **Безопасност срещу подслушване**: В CV-QKD, ако някой трети участник се опита да подслушва комуникацията, той ще наруши квантовото състояние и ще бъде открит. Това е в съответствие с основните принципи на квантовата механика, като **неопределеността** (Heisenberg Uncertainty Principle) и **неопределената заплетеност**. Всеки опит за измерване на квантовите състояния, които са част от комуникацията, ще доведе до **неочаквани отклонения** и следователно ще бъде открит.

Процес на работа на CV-QKD

CV-QKD работи в следните основни стъпки:

1. **Генериране на квантови състояния**: Изпращачът създава квантови състояния, като **квантови лазери** или други квантови източници. Тези състояния могат да бъдат описани чрез променливи като амплитуда и фаза.

2. **Изпращане на състояния по канала**: Състоянията се изпращат по оптичния канал към получателя. Поради квантовата природа на състоянията, те

не могат да бъдат наблюдавани без да се променят (по принципа на квантовата механика).

3. **Измерване на квантовите състояния**: Получателят извършва измервания на амплитудата и фазата на тези състояния. Възможността за измерване на тези параметри се избира така, че получателят да може да съпостави резултатите си с тези на изпращача, като в същото време гарантира сигурността на ключа.

4. **Корекция на грешки и генериране на споделен ключ**: След измерванията, Изпращачът и Получателят обмени информации за параметрите на измерванията си, за да идентифицират съвпаденията. Ако има грешки или несъответствия в измерванията, те използват корекция на грешки, за да поправят тези несъответствия и да получат общ споделен ключ.

Протоколи за CV-QKD

Някои от най-известните протоколи за **CV-QKD** включват:

1. **Gaussian Modulated Coherent States (GMCS)**: В този протокол, квантовите състояния се модулират с **Гаусова разпределение** на амплитудата и фазата. Това е широко използван метод за CV-QKD.

2. **Displaced Phase Shift (DPS)**: В този протокол амплитудата на фотоните се променя, като се използват различни фази, за да се контролира информацията, която се прехвърля.

3. **X-или Y- Basis Protocol**: Този метод използва два основни базиса (например амплитудно и фазово) за кодиране на информацията. Получателят извършва измервания по тези базиси, за да определи споделен ключ.

Предимства на CV-QKD

1. **Съвместимост с класическата инфраструктура**: CV-QKD може да се използва с **класическа оптична инфраструктура**, като например стандартни оптични кабели, без да изисква специални квантови компоненти, което го прави по-практичен и по-лесен за внедряване в съществуващи мрежи.

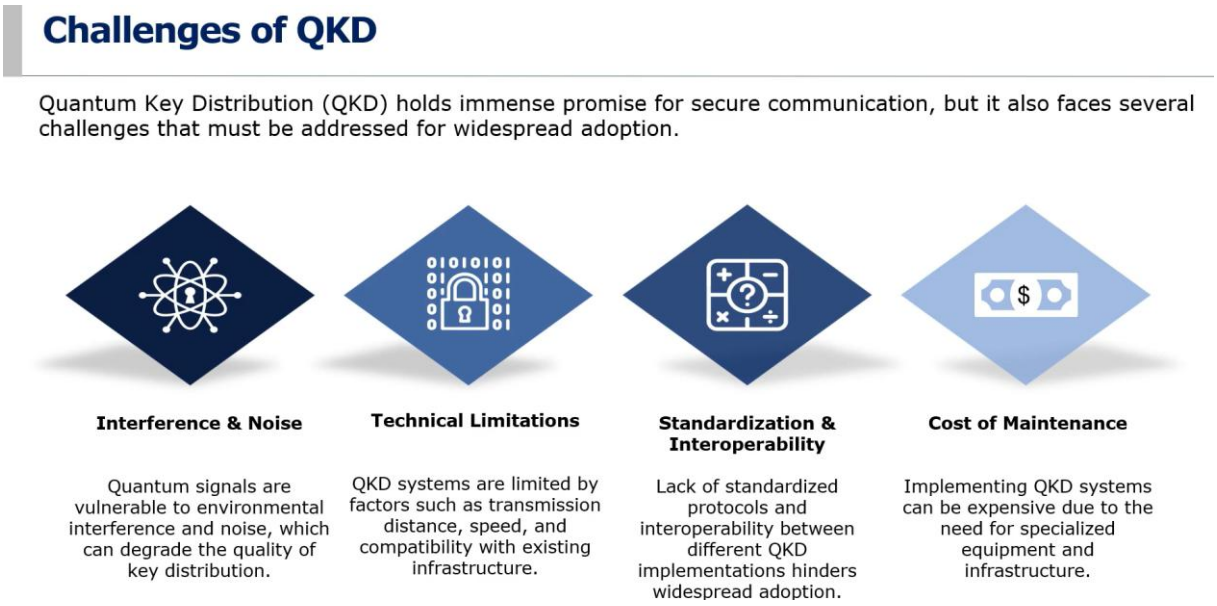
2. **По-добра ефективност за дълги разстояния**: CV-QKD показва **по-добра ефективност** за комуникация на дълги разстояния, благодарение на

използването на **непрекъснати променливи**, които имат по-малка склонност да се губят по време на предаване през каналите.

3. **По-ниски изисквания за технически ресурси**: Тъй като CV-QKD не изисква създаването на състояния на квантови битове (кюбити), той може да бъде по-прост за реализация и по-лесен за интегриране в съществуващите комуникационни мрежи.

4. **Мощен инструмент за сигурност**: Използването на принципите на квантовата механика в CV-QKD предлага силни гаранции за сигурност. Всеки опит за подслушване или манипулация на квантовите състояния ще бъде открит веднага.

CV-QKD представлява иновативен подход в квантовата криптография, който използва **непрекъснати променливи** за генериране на криптографски ключове. Той предлага значителни предимства в сигурността и практическото внедряване, като осигурява висока ефективност за дълги разстояния и може да бъде използван с класическа оптична инфраструктура. С нарастващото значение на квантовата криптография за бъдещето на комуникациите, CV-QKD е едно от обещаващите решения за изграждане на защитени комуникационни мрежи.



Източник: https://www.youtube.com/watch?v=gnk8VoMsvO8

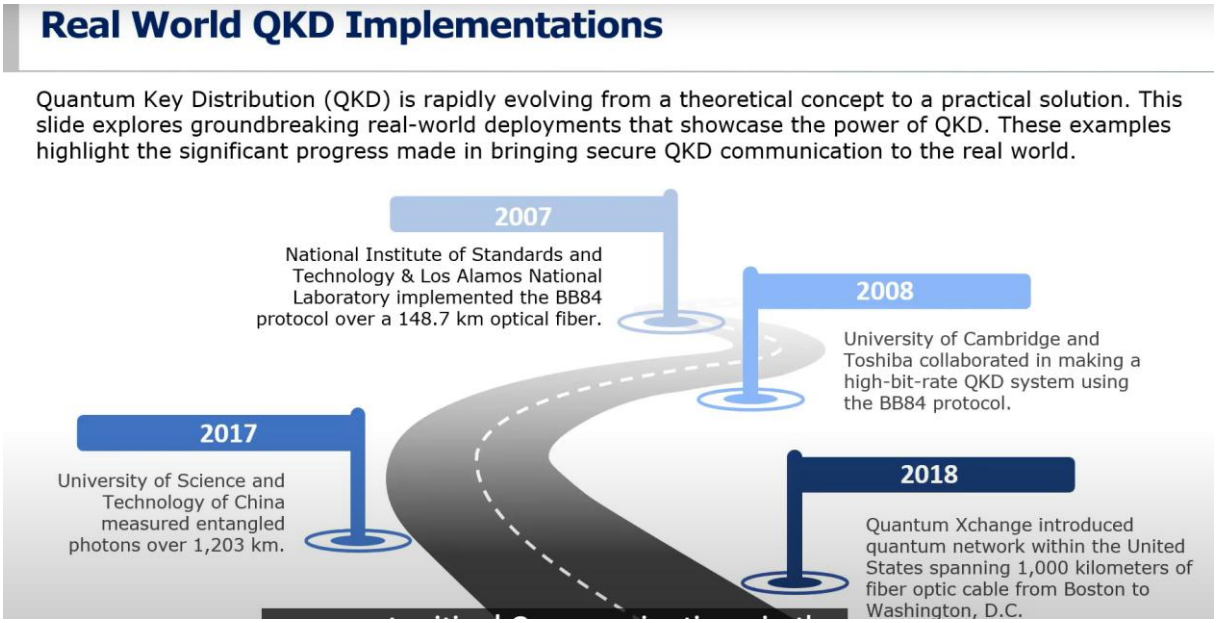
Encryption Consulting LLC·3.04.2024 г.

Приложения на квантовата криптография

- **Сигурен обмен на ключове**: Един от основните начини за прилагане на квантова криптография е за обмен на криптографски ключове за симетрични криптографски системи. Тези ключове могат да се използват за осигуряване на конфиденциалност на съобщения.
- **Сигурни комуникации**: Квантовата криптография може да се използва за създаване на канали за сигурна комуникация, които не могат да бъдат подслушвани без да бъдат открити.
- **Блокчейн технологии**: Квантовата криптография може да бъде използвана за подобряване на сигурността на блокчейн мрежите, като осигури по-силни криптографски ключове и защита срещу бъдещи квантови атаки.

Предизвикателства и бъдещи перспективи

1. **Технологични ограничения**: Въпреки големия напредък, квантовата криптография все още е на етап на изследвания и разработка. Технологиите, които позволяват стабилно и ефективно предаване на квантови състояния на големи разстояния, все още не са напълно разработени.
2. **Квантови компютри**: Ако бъде създадено достатъчно мощно квантово изчислително устройство, теоретично то би могло да наруши много от традиционните криптографски системи, като RSA. Въпреки това, квантовата криптография предлага начини за защита от такива бъдещи заплахи.
3. **Практическо приложение**: Въпреки теоретичните предимства, прилагането на квантовата криптография на големи разстояния и в реални условия е все още трудност. Квантовите канали изискват специализирано оборудване и не могат да се използват лесно в съществуващата инфраструктура.



Източник: https://www.youtube.com/watch?v=gnk8VoMsvO8

Encryption Consulting LLC·3.04.2024 г.

Квантовата криптография предлага нови и революционни възможности за осигуряване на сигурност в комуникациите, използвайки принципите на квантовата механика. Въпреки че технологията все още е в процес на развитие, тя обещава да осигури не само защита срещу настоящите заплахи, но и срещу бъдещите предизвикателства, които могат да възникнат със създаването на квантови компютри.