

Sbobbinate del seminario Crittografia Quantistica (16-12-2004).

Data 23-12-2004

Questo seminario sarà molto introduttivo quindi chi avrà familiarità con la crittografia quantistica potrebbe annoiarsi, è pensato per un audience privo di qualunque conoscenza di base di meccanica quantistica. Illustrerò molto brevemente gli argomenti di cui si parlerà. Inizierò a descrivere cosa è un

- Sistema crittografico a chiave pubblica.
- Sistema a chiave privata.

Questo servirà per fissare lo scenario e spiegare il ruolo che giocano in questi due sistemi i protocolli di crittografia Quantistica, che come vedremo dovrebbero essere più propriamente descritti come ***Protocolli di Distribuzione Quantistica di Chiavi*** .

1. Dovremo poi descrivere
 - cosa è un fotone
 - e cosa è la polarizzazione di un fotone
2. Spiegheremo questo per due motivi
 - il primo per un problema concettuale: il fotone e la proiezione di un fotone è il sistema più semplice che ci permette di spiegare cosa è una sovrapposizione quantistica di stati e che cosa è quello che viene oggi definito un ***Bit quantistico*** .
 - D'altro canto sono proprio i fotoni, i sistemi ottici che vengono usati nella implementazione e sperimentazione reale dei sistemi di crittografia quantistica di chiavi.

3. Dopo introdurremo quello che è storicamente il primo sistema crittografico quantistico a stati non ortogonali. (Primo sistema crittografico quantistico)
4. Andremo a vedere e fare una analisi delle tecniche di intrusione (*eavesdropping*) su questo tipo di protocolli di distribuzioni di chiavi e finiremo poi con l'argomento più esotico del seminario, vedremo cioè una classe di sistemi di distribuzione di chiave crittografiche che si basano su una proprietà dei sistemi quantistici.

Crittografia deriva del greco e vuol dire scrittura nascosta. In linea di principio ci sono due personaggi, Alice e Bob che vogliono trasmettersi delle informazioni importanti, cifrate, nascoste a parti ostili (Eve nel nostro esempio). I tre attori saranno sempre Alice e Bob che vogliono scambiarsi informazioni e Eve che cerca di carpire, intercettare e conoscere le informazioni acquisite. Alice & Bob usano per realizzare la loro trasmissione sicura un processo di cifratura. Alice converte attraverso un algoritmo il testo in chiaro che vuole trasmettere, in un testo cifrato intellegibile a chiunque lo intercetti e provi a leggerlo. Nello scenario ideale Eve lo intercetta ma non estrae alcuna informazione. Bob Riceve il testo cifrato e con un algoritmo di decodifica estrae nuovamente il testo in chiaro. Questo processo di criptazione e decriptazione fa uso di alcune informazioni segrete mescolate con il testo in chiaro dette *chiavi* e note soltanto a Alice & Bob. Esistono diverse famiglie di sistemi crittografici ad esempio sono molto comuni sistemi crittografici a *chiave asimmetrica*. L'idea di fondo è che l'algoritmo di criptazione (che crea il testo cifrato a partire da testo in chiaro e dalla chiave) utilizza una chiave diversa dall'algoritmo che consente di decriptare il testo (trasformare il testo cifrato in testo in chiaro). Quindi sono presenti chiavi Pubbliche e chiavi Private, una serve per rendere intellegibile il testo in chiaro, l'altra serve per recuperare l'informazione. Bob vuole ricevere un messaggio segreto da Alice, dunque fornisce al mittente la chiave pubblica e Alice codifica il messaggio con tale chiave e manda il messaggio a Bob. Per la decodifica verrà usata un'altra chiave quella privata che possiede soltanto Bob. E' come se Bob avesse una casella di posta pubblica dove chiunque può imbucare le lettere verso Bob ma solo Bob ha la chiave per aprire la casella e leggere poi la posta. Questi sistemi sono molto agevoli dal punto di vista pratico ma hanno anche dei difetti. Un esempio tipico è l'RSA. Di fatto questi sistemi si basano sul fatto che esistono problemi difficili da risolvere, ad esempio fattorizzare un

grosso numero. Non essendo provata la loro sicurezza questi algoritmi sono convenienti e ha senso usarli ogni qualvolta le risorse necessarie per decodificare il messaggio da parte di Eve (supponendo che sia riuscita a riceverlo) sono tali da rendere essenzialmente non conveniente il loro uso, ad esempio il tempo necessario per codificarlo sarebbe troppo lungo oppure, il valore stesso delle risorse necessarie per codificarlo è maggiore del vantaggio che si trarrebbe dal conoscere il contenuto del messaggio stesso. C'è un altro problema, la difficoltà computazionale di molti problemi non è provata. Non si sa se esiste un algoritmo classico efficiente che consente di fattorizzare grossi numeri in tempo polinomiale e non è detto che se qualcuno scoprisse questo algoritmo lo renderebbe pubblico. E' noto d'altro canto che esistono algoritmi quantistici cioè che potrebbero girare su un hw quantistico che riescono a fattorizzare grossi numeri in tempo polinomiale. Un'altra famiglia di sistemi crittografici sono quelli a chiave privata o simmetrica. In questi algoritmi entrambe le chiavi usate da Alice & Bob sono le stessa, sia in fase di codifica che di decodifica. ***Un esempio tipico è il cosiddetto cifrario di Vernam o One Time Pad. Alice vuole trasmettere il messaggio, lo esprime in binario e l'algoritmo di codifica somma modulo 2 il testo (stringa) in chiaro con una chiave (stringa random) anche essa codificata in binario di uguale lunghezza del testo (si ottiene così il testo cifrato). L'algoritmo di decodifica è lo stesso dell'algoritmo di codifica, cioè Bob recupera il testo cifrato, usa la stessa chiave ed effettua MOD 2 la somma tra Chiave e Testo Codificato***. Poiché la somma è distributiva e la somma di una stringa con se stessa MOD 2 è sempre la stringa nulla, Bob recupera nuovamente il testo. Shannon prima dello scoppio della seconda guerra mondiale (anche se l'articolo fu pubblicato successivamente) dimostrò la sicurezza incondizionata del cifrario. ***In altre parole anche se Eve riesce a carpire il messaggio cifrato non se ne fa niente, cioè l'informazione che Eve ha sul messaggio intercettato è la stessa di quella che Eve ha prima di intercettare il messaggio, e questo perché se io ho una stringa ottenuta dalla somma MOD 2 (XOR bit a bit) tra il testo in chiaro e una stringa Random, questa è anche essa random e non ha alcuna informazione utile per definizione. Però***

bisogna dire che questo cifrario è incodizionatamente sicuro se e solo se la (chiave) stringa sia realmente random, la lunghezza della stringa (chiave) sia uguale a quella del testo, e venga usata una sola volta e che sia segreta. Lunga quanto il testo perchè se fosse altrimenti, cioè di lunghezza minore allora si potrebbero iniziare a fare analisi statistiche anche spezzando il testo cifrato e individuando informazioni utili sulla chiave, se ad esempio la chiave viene usata più volte(2) Eve può fare l'XOR fra due testi cifrati. Lo Xor tra due testi cifrati è essenzialmente la Xor tra due testi in chiaro perchè facendo tale operazione due volte sui testi elimino essenzialmente la chiave. Lo Xor tra due testi in chiaro non è assolutamente random contiene in qualche modo qualche informazione utile. Il problema principale è però che la chiave deve essere segreta. Alice e Bob devono essere in possesso di una chiave sufficientemente lunga e soprattutto nota soltanto a loro. Quindi ho usato un corriere o si incontrano e scambiano personalmente tale chiavi. Uno dei punti deboli di questo tipo di sistemi crittografici è essenzialmente la distribuzione della chiave. Vedremo che è in questo punto che entra in gioco la meccanica quantistica, cioè quello che si intende per crittografia quantistica **sono dei protocolli di distribuzione di chiavi crittografiche da utilizzare in protocolli crittografici a chiave simmetrica che consentono a due utenti di scambiarsi messaggi anche se siamo in presenza di parti ostili.** In altre parole come vedremo tra poco supporremo di avere Alice e Bob vogliono scambiarsi messaggi e per far questo hanno bisogno di scambiarsi una chiave crittografica, **allora i protocolli di crittografia quantistica consentono a Bob ed Alice di stabilire una stringa random condivisa e segreta anche se c'è Eve che sta tamponando con il loro canale di comunicazione.** Iniziamo la parte noiosa in cui cerco di spiegarvi le regole della meccanica quantistica, che vengono utilizzate in questo contesto. Iniziamo con un sistema puramente classico, un'onda elettromagnetica, cioè una onda monocromatica piana cioè un'onda sinusoidale che si propaga in questo caso (vedi slide) nella direzione Zeta. Per polarizzazione si intende il piano di oscillazione del campo elettrico di un'onda elettromagnetica se in questa radiazione di propagazione il campo elettrico oscillerà in una direzione sempre perpendicolare alla direzione di propagazione, il piano in cui oscilla il campo elettrico prende il nome di piano di polarizzazione di un

onda elettromagnetica. Per le onde elettromagnetiche vale il principio di sovrapposizione cioè se io ho un'onda A e un'onda B io posso sovrapporre le sue onde e ottenere un'onda C. Di conseguenza se io ho un'onda polarizzata in un modo e un'onda polarizzata in modo diverso e li sovrappongo otterrò una terza onda che in generale è polarizzata in modo diverso rispetto alle due onde precedenti. Un esempio tipico supponiamo di avere un'onda polarizzata verticalmente, che è l'esempio A. Supponiamo che le onde si stiano propagando dallo schermo verso di noi con le frecce rosse che stanno indicando il piano di oscillazione del campo elettrico. Con l'esempio A abbiamo un'onda elettromagnetica polarizzata nella direzione verticale. Sotto nell'esempio B abbiamo un'onda polarizzata orizzontalmente. Io posso sovrapporre in modo opportuno quindi aggiustando la fase relativa alle due onde, posso sovrapporre l'onda A e l'onda B in modo tale da ottenere un'onda come nel caso D a più 45 gradi, o come nel caso C a meno 45 gradi quindi supponete un'onda elettromagnetica che oscilla nel piano verticale e una che oscilla nel piano orizzontale, se sovrappongo questi due moti ottengo un moto che è a 45 gradi (se li faccio oscillare in fase). Se li faccio oscillare con fase opposta il moto sarà a meno 45 gradi. Se io ho due onde di uguale ampiezza e le faccio oscillare con differenza di fase di 90 gradi quindi quando una è al massimo e una al minimo ottengo un'onda polarizzata circolarmente, in senso orario o antiorario a seconda della fase relativa se è più o meno 90 gradi la differenza di fase. Ma quello che è importante sapere è che io posso sovrapporre (già classicamente) onde con polarizzazioni diverse ad esempio orizzontale e verticale per ottenere una polarizzazione a più o meno 45 gradi. A questo punto introduciamo uno strumento di cui faremo largo uso in tutto il seminario **il**

Polarizzatore. Supponiamo di avere un'onda non polarizzata, cioè un'onda in cui il piano di oscillazione del campo elettromagnetico (P.O.C.) va fluttuando molto rapidamente quindi supponete che il P.O.C. elettromagnetico vada fluttuando su scale dei tempi dell'ordine dei nanosecondi. La luce che viene emessa ad esempio dal proiettore con cui vengono visualizzate le nostre slide è non polarizzata, è una sorgente termica e dunque essenzialmente all'eccitazione termica degli elettroni che stanno all'interno della resistenza della lampadina, questi si agitano emettono luce ma emettono luce ognuna per i fatti suoi quindi questa polarizzazione va fluttuando rapidamente. A questo punto inserisco un polarizzatore (oggetto indicato con la lettera A). Il polarizzatore è un mezzo trasparente in modo anisotropo cioè è **un materiale che trasmette**

o assorbe la luce a seconda della luce incidente (gli occhiali polaroid degli anni 70 sono fatti con questo materiale). Questo materiale **ha la caratteristica di far passare solo la luce che è polarizzata lungo il suo asse**. La luce che viene polarizzata lungo l'asse ortogonale viene totalmente assorbita. Supponiamo di avere un fascio non polarizzato che incide sul polarizzatore A la luce che emerge da polarizzatore A sarà sempre verticalmente polarizzata se l'asse di polarizzazione è verticale. Supponiamo di mettere un secondo polarizzatore dopo il polarizzatore A e supponiamo di mettere l'asse del polarizzatore B ad un angolo θ rispetto al polarizzatore A e cosa succede? Succedono due cose. Mentre la luce che esce da A ed incide su B che è polarizzata verticalmente, la luce che emerge dal secondo polarizzatore sarà polarizzata di un angolo θ quindi la prima cosa che osserviamo è una rotazione del piano di polarizzazione. La seconda cosa che osserviamo è che la luce ha un'intensità più bassa (per questo viene usata per gli occhiali da sole) cioè la luce che emerge dal polarizzatore B ha un'intensità minore della luce che emerge dal polarizzatore A. Se uno smanetta e prende una lavagna luminosa e mette sopra due fogli di polaroid e va ruotando, vede sperimentalmente che il fattore di attenuazione della luce che incide sul polarizzatore B e quella che emerge è essenzialmente un fattore $\cos^2(\theta)$, cioè se io ho una luce che polarizzata verticalmente incide su un polarizzatore ad un angolo θ la luce che emerge dal polarizzatore sarà attenuata rispetto alla luce incidente di un fattore $\cos^2(\theta)$, questa prende il nome di legge di Malus. Un altro strumento è il beam-splitter cioè una lamina che in parte riflette e in parte assorbe, qualunque dielettrico o vetro delle comuni finestre in parte riflette in parte assorbe. Però queste materie vengono fatte in modo tale (sempre per un beam splitter da 50%) che l'intensità della luce trasmessa e della luce riflessa sia uguale, io posso utilizzando opportune tecniche di fabbricazione, cambiare il rapporto tra luce riflessa e luce trasmessa posso avere dei beam-splitter che riflettono molto e dei beam-splitter che trasmettono molto, ma in generale tutto quello cui andremo a vedere noi altri nel resto del nostro seminario sono dei fifty-fifty beam splitter cioè dei beam splitter che fanno passare riflettono & trasmettono luce in uguale intensità quindi se I_0 è l'intensità della luce incidente la luce trasmessa avrà intensità di $I_0/2$ e la luce riflessa avrà intensità $I_0/2$. Questo banalmente per un principio di conservazione dell'energia. L'intensità del fascio luminoso dice essenzialmente quanta energia trasporta l'onda elettromagnetica, l'energia si deve conservare e quindi in parte verrà

trasmessa in parte riflessa si devono conservare i quadrati dell'intensità....
 uno strumento che a noi interesserà di più sono invece polarized
 beam-splitter cioè beam splitter che si comportano da polarizzatori.
 Consideriamo questi beam splitter polarizzanti PBS sono dei beam splitter
 che fanno la seguente cosa : hanno un loro asse di polarizzazione
 supponiamo verticale allora se sul beam splitter incide un fascio
 verticalmente polarizzato questo fascio viene totalmente trasmesso se
 d'altro canto su questo beam splitter incide un fascio luminoso polarizzato
 orizzontalmente questo fascio viene riflesso che cosa succede per una
 polarizzazione che sia diversa da verticale orizzontale quindi supponiamo di
 avere un fascio polarizzato ad un angolo θ rispetto la direzione verticale.
 Bene quello che succede è che in trasmissione si comporta a tutti gli effetti
 come se fosse un polarizzatore cioè l'intensità della luce trasmessa sarà
 essenzialmente uguale all'intensità della luce incidente moltiplicato per un
 fattore $\cos^2(\theta)$. A questo punto vedete quanto deve essere l'intensità della
 luce riflessa. Per la conservazione dell'energia tutta la luce quello che
 succede è che che entra deve in qualche modo uscire come intensità la luce
 che viene riflessa viene attenuata con un fattore $\sin^2(\theta)$. Un angolo
 arbitrario parte della luce viene trasmessa ,parte della luce viene riflessa
 luce trasmessa ha un intensità pari a quella incidente per un fattore \cos^2 la
 parte riflessa viene attenuata con un fattore $\sin^2(\theta)$ dove θ vi ripeto è
 l'angolo tra l'asse del polarizing beam splitter e la polarizzazione della luce
 incidente. Abbastanza noioso ma, adesso passiamo ai Fotoni. Fino ad ora
 abbiamo descritto la luce essenzialmente come un onda elettromagnetica
 classica ,quantisticamente la luce viene descritta in termini di pallettoni,
 cioè quanti di energia, Immaginate un fascio luminoso come un insieme di
 particelle senza massa che si muovono tutte alla stessa velocità, velocità
 della luce naturalmente, tutte indivisibili, immaginate come se fossero dei
 quanti di energia il termine particella sta ad indicare suggerire l'idea di
 quanto di energia quindi immaginateli come dei pallettoni che viaggiano che
 non posso dividere in alcun modo che hanno tutti la stessa energia, e hanno
 tutti la stessa energia e hanno tutti la stessa velocità inoltre il fotone ha
 una polarizzazione, il fotone oltre ad avere una certa energia, e corrisponde
 ad un campo di una certa frequenza ha una sua polarizzazione, l'intensità del
 fascio luminoso è proporzionale a quanti fotoni per unità di tempo questo
 fascio trasporta, ogni fotone ha una sua polarizzazione, se io ho un fascio
 luminoso polarizzato verticalmente ad esempio significa che tutti i fotoni
 che sono nel fascio hanno tutti la stessa polarizzazione, mentre un fascio

non polarizzato corrisponde ad un fascio luminoso in cui i fotoni sono distribuiti in modo Random secondo una certa distribuzione di probabilità cioè ogni fotone ha cioè una sua polarizzazione che rimane fissa nel tempo, però abbiamo una distribuzione statistica di polarizzazione. Veniamo alla parte un po' più hard un po' più tecnica (un po' Quantistica) abbiamo visto che classicamente possiamo sovrapporre stati cioè onde elettromagnetiche con polarizzazione differenti lo stesso principio di sovrapposizione vale in meccanica quantistica. Indichiamo con questo simboletto di parentesi lo stato di un fotone, (Questa notazione è dovuta a Dirac) e questi simboli si chiamano cat. Con il simbolo V_i indico un fotone polarizzato verticalmente, con il simbolo H_i indico un fotone polarizzato orizzontalmente io posso aver un fotone nello stato A che è una sovrapposizione di un fotone polarizzato verticalmente e uno polarizzato orizzontalmente cioè lo stato di un fotone viene descritto quantisticamente dando a queste quantità αV_i αH_i che prendono il nome di ampiezze di probabilità e sono numeri complessi con il vincolo che il modulo quadro di αV_i più il modulo quadro di αH_i sia uguale ad uno. Quindi la somma dei moduli quadri deve essere uguale ad uno quindi la somma dei moduli quadri deve essere uguale ad uno. Una cosa importantissima che useremo pesantemente quando incominceremo a vedere nel resto del Talk quando cominceremo a vedere come funzionano questi sistemi crittografici quantistici è che dato un fotone, lo stato di un singolo fotone posso esprimerlo in modo non unico a seconda delle basi che utilizzo, in altre parole torniamo al caso classico, io posso esprimere un'onda polarizzata a 45 gradi come la sovrapposizione di due onde una orizzontalmente e una verticalmente polarizzata ma dall'altro canto io posso descrivere un'onda verticalmente polarizzata come la somma di un'onda a 45 e una a -45. Lo stesso vale quantisticamente io posso iscrivere lo stato di un fotone polarizzato a 45 gradi per esempio come la somma di uguale ampiezza di un fotone polarizzato orizzontalmente e uno polarizzato verticalmente così un fotone potrà essere a meno 45 gradi posso scriverlo in questo modo, così il contrario posso esprimere un fotone polarizzato orizzontalmente nella base verticale orizzontale è semplicemente ruotare il sistema di riferimento. Andiamo a vedere come viene interpretato il funzionamento di PBS quando la luce viene descritta non più in termini di una onda elettromagnetica classica bensì in termini di un fascio di fotoni **Vi ricordo che i fotoni sono indivisibili**, supponiamo di avere un fotone che incide... ma prima di andare a vedere gli esempi che ci sono sullo schermo, Supponiamo

di avere un PBS con un asse verticale e di illuminarlo e di fare incidere su di esso un fascio luminoso polarizzato verticalmente, significa che tutti i fotoni del fascio sono tutti polarizzati verticalmente e tutti quanti vengono trasmessi. Ogni singolo fotone che entra esce in trasmissione viceversa posso avere una situazione in cui i fotoni sono tutti polarizzati orizzontalmente e in questo caso vengono tutti quanti riflessi se io ho un fascio luminoso polarizzato ad un certo angolo, Questi fotoni cosa succede ,questi fotoni arrivano sul polarized beam splitter, non possono essere divisi quindi il fotone cosa fa nel modo random il fotone viene trasmesso oppure viene riflesso, la probabilità che il fotone venga trasmesso è proporzionale al \cos^2 di θ ,la probabilità che il un fotone venga riflesso è proporzionale al \sin^2 di θ . Supponiamo di vedere arrivare un singolo fotone al PBS io non ho modo di sapere se viene trasmesso o riflesso, l'evento riflessione trasmissione è totalmente random ,l'unica cosa che posso dare sono le probabilità a priori che venga riflesso o trasmesso, se io conosco la polarizzazione del fotone incidente posso assegnare queste probabilità che sono $\cos^2\theta$ e $\sin^2\theta$. guardate che $\cos^2\theta$ e $\sin^2\theta$ sono i quadrati dell'ampiezza di probabilità quindi quando io esprimo lo stato di un fotone in termini di ampiezze di probabilità rispetto ad una base significa che il modulo quadro di quelle ampiezze di P è la probabilità di misurarlo nello stato di quella base in soldoni supponiamo di avere un fotone polarizzato a 45 gradi se un fotone è polarizzato a 45 gradi che incide su questo dispositivo nella metà dei casi in modo totalmente random io lo osservero in modo trasmesso ,nella metà dei casi io lo osservero trasmesso nella metà dei casi io lo osservero riflesso,**questo esempio è importante perché un tipico esempio da manuale di quello che è un processo di misura quantistico**, notate che lo stato del fotone all'uscita del PBS è cambiato inizialmente il fotone è polarizzato a 45 gradi dopo l'uscita dal PBS lo trovo o verticalmente o orizzontalmente polarizzato, questa specie di ..che io vado segnando sono dei **fotorivelatori**. Supponiamo di avere questi fotoni che arrivano e questi fotorivelatori che fa un clic ogni volta che arriva un fotone e ogni volta che arriva fa clic o il fotorivelatore presente in alto nell'esempio oppure quello in basso nell'esempio l'unica cosa che posso dire è la probabilità che faccia un clic. Ad un certo punto il fotone arriva su PBS e deve essere misurato e si mettono due fotorivelatori e si vede quale dei due clicca. **notate che lo stato del fotone dopo che ha attraversato il PBS è bruscamente cambiato non è più lo stesso di prima quindi il processo di misura**

cambia lo stato. Seconda cosa l'unica cosa che posso dare è una probabilità di un risultato di misura dato la conoscenza dello stato di partenza. Bene ora ho finito di annoiarvi con le regole della meccanica quantistica. Arriviamo ai protocolli di crittografia quantistica. Il primo protocollo storicamente è quello di BB84 dove BB non sta per Brigitte e Bardoux bensì per Bennett e Brassard (84). Provate ad immaginare come potremmo usare i fotoni per distribuire le stringhe da poi usare come chiave crittografica. La cosa più naïf da fare sarebbe questa. Alice prende una stringa random e la vuole trasmettere a Bob per fare questo codifica lo zero ad esempio nella polarizzazione verticale e l'1 nella polarizzazione orizzontale, prende questi fotoni e li spedisce a Bob ovviamente non funziona. Supponiamo che ci sia Eve che vuole intercettare la chiave. Se lei sa che Alice invia fotoni nella base orizzontale o verticale quello che fa è semplicemente prendere un PBS. Se Alice manda solo fotoni verticalmente polarizzati o orizzontalmente polarizzati Eve mette uno di questi apparecchi in mezzo e il fotone lo fa sbattere lì se il fotone è polarizzato verticalmente clicca il detector in alto se è polarizzato orizzontalmente clicca il detector in basso, sa quale è lo stato di polarizzazione del fotone ne crea uno uguale e lo spedisce a Bob. Bob non può accorgersi della presenza di Eve. Quindi questo schema non funziona. La soluzione a questo schema è la seguente Alice codifica 0 1 non usando sempre la stessa base ma cambiandola in modo random. Cioè essenzialmente quello che fa è scegliere due basi distinte fra di loro, o la base verticale orizzontale o la base $+45$ che per comodità chiamerò base più e base per e codifica 0 in $+45$ e 1 in -45 se ha sorteggiato la base per oppure 0 in verticale e 1 in orizzontale se ha deciso di usare la base più. Adesso c'è un problema Bob non sa in che base Bob gli ha mandato il messaggio quindi non sa come orientare il suo PBS. La soluzione è semplice prova a caso quindi come è che si procede Alice sceglie a caso una base manda il fotone polarizzato secondo della base scelta quindi codifica il fotone in una certa base e li spedisce Bob li riceve e sceglie in modo random come orientare il suo PBS per misurare il fotone. Se le basi coincidono e non c'è Eve in mezzo in questo caso Bob misurerà esattamente il bit spedito da Alice. Se le basi di Bob non coincidono con la base di Alice Bob codificherà con uguale probabilità il bit trasmesso da Alice. Perché con uguale probabilità? Supponiamo che Alice abbia deciso di codificare uno zero in un fotone a 45 gradi Bob orienta il suo polarized beam splitter con l'asse verticale e essendo nell'asse verticale osserverà con uguale probabilità osserverà un fotone verticale e con uguale probabilità osserverà un fotone

orizzontale. Quindi con uguale probabilità misurare uno 0 o un 1. Ecco ora il protocollo. la prima cosa che fa Alice è la seguente sceglie una sequenza random di basi, sceglie in modo random una stringa binaria, codifica questa stringa binaria secondo la convenzione detta prima (verticale +45, orizzontale +45) a seconda della scelta di base random fatta prima, prende questi fotoni e li spedisce a Bob, la spedizione avviene o attraverso laser o in fibra ottica. Bob sceglie in modo random la sequenza di Basi su quale effettuare la misura. Misura lo stato dei fotoni sulla base di quanto scelto al passo prima. Cos'hanno Alice e Bob alla fine di questo stadio del protocollo. Alice ha una Stringa binaria che è la stringa binaria che vuole spedire Bob ha un'altra stringa binaria che è la stringa binaria che vuole spedire, Bob ha un'altra stringa binaria che è il risultato della sua misura. Le due stringhe sono correlate solo nel 50% dei casi. Perché con probabilità del 50% Bob ha scelto la base sbagliata e quando ciò succede vi ricordo il risultato della sua misura totalmente scorrelato con quello che ha mandato Alice. Protocollo continua e Alice usa un canale pubblico cioè un canale a cui tutti hanno accesso può essere una radio hanno accesso tutti e la conversazione avviene in pubblico questa è una cosa importante. Dunque Alice comunica in pubblico la base che ha utilizzato per la codifica quindi vi comunica tutte le stringhe più o per quindi la sequenza di basi per codificare i fotoni ma non dice i bit che ha voluto codificare in quella base. Allora Bob cosa fa? prende quella stringa e fa confronti dopo aver confrontato la sequenza di basi utilizzate da Alice per la codifica con quelle usate da lui per la misura. Sempre nel canale pubblico dunque accessibile a tutti comunica ad Alice in quali casi le basi sono coincidenti e in quali casi no in Questo caso loro buttano circa il 50% dei dati a loro disposizione. Alla fine di questo stadio Alice e Bob condividono una stringa che in assenza di sdropping dovrebbero coincidere. Questa stringa prende il nome di *stringa settacciata*, dovrebbero coincidere in assenza di sdropping. esempio: Alice sceglie una sequenza di basi e Alice sceglie di voler mandare una sequenza di bit se sceglie la base più manda un fotone come polarizzato orizzontalmente o se vuole la base più e vuole mandare uno zero usa un fotone polarizzato verticalmente. Bob fa anche lui una scelta random di basi e in questo caso il bit spedito da Alice viene correttamente letto da Bob. Alice & Bob confrontano pubblicamente in quali casi le basi sono le stesse la dove coincidono i bit viene tenuto la dove i due bit non coincidono il bit viene scartato. e qui siamo in uno scenario dove Eve non c'è. In uno scenario dove Eve intercetta il messaggio (fotoni) e ha i mezzi per misurarli, ma ricorda che ogni

qualvolta che uno cerca di misurare lo stato di un fotone e non sa qual'è lo stato del fotone viene disturbato e abbiamo visto che posso misurare lo stato di un fotone solo se so in quale base di partenza è codificato, se non so in che base è codificato non so come orientare il PBS dunque come risultato della misura otterro un cambiamento dello stato del fotone quindi lo avro disturbato vedremo poi strategie sofisticate per posizionare correttamente un PBS. Nel momento in cui Eve fa una misura quello che succede è che io introduco rumore cioè introduco una discrepanza tra le stringhe che hanno alic e bob ed è proprio il fatto che una misura disturba irreversibilmente lo stato di un fotone che rende possibile a bob di accorgersi della presenza di Eve Proprio il fatto che delle stringhe che dovrebbero coincidere non coincidono è indicativo della presenza di qualcuno che sta tampinando e intercettando fotoni durante la comunicazione quindi regole della MQ permettono una diagnosi della presenza di un intruso e proprio questa la parte cruciale è questo il motivo per cui la scelta di base in cui vengono codificati i fotoni viene scelta in modo random. A questo punto alic e bob cosa fanno, prendono la sottostringa decidono di sacrificare alcuni dei bit della stringa che vorrebbero usare come chiave crittografica per fare un analisi statistica dei casi in cui le due stringhe non coincidono dunque fanno una analisi statistica degli errori la percentuale di errori commessi si chiama QBER (quantum bit error rate) quindi essenzialmente mi da la percentuale dei casi in cui i risultati delle misure dei casi fatti da bob non coincidono con il bit trasmesso da alic. questo consente di stimare quante informazioni Eve è riuscita ad avere sui fotoni in transito. quanta più informazione riesce ad avere Eve sul sistema sui fotoni in transito tanto è maggiore il rumore-disturbo introdotto. A questo punto loro confrontano il QBER con una soglia di sicurezza. Esistono dei criteri che dicono che sotto una certa soglia di sicurezza puoi continuare oppure no, inquest' ultimo caso la chiave pè sicura ed è inutilizzabile riavvia il protocollo quando le condizioni garantiscono una trasmissione sotto la soglia di sicurezza. Vedete la logica dei protocolli di crittografia quantistica è quella di consentire di essere in possesso di una chiave segreta anche se siamo in presenza di Eve e vedere se questa chiave è sicura oppure no. Se siamo al di sotto della soglia di sicurezza e dunque è accettabile il livello di errore introdotto da Eve è sufficientemente basso, esistono dei protocolli detti di amplificazione di privacy che consentono di estrarre dalla stringa settacciata una stringa piu corta tale che su di esse Eve non ha alcuna informazione. Dalla stima dell'errore alic e bob stimano che informazione Eve ha sulla loro stringa e

nel processo di amplificazione di privacy si estrae dalla stringa di partenza una stringa sulla quale Eve non ha inciso alcun errore prima di fare questo si mette in moto un processo di error correction .quello che si fa se la chiave ha degli errori che vengono corretti con codici standard efficienti (che raggiungono il limite di Shannon). A questo punto Alice e Bob hanno una stringa che coincide perfettamente ma sulla quale Eve ha delle informazioni allora a partire da questa stringa estraggono una stringa più corta sulla quale Eve non sa più nulla. Vediamo un esempio. Supponiamo che Eve sa qualche cosa e conosce il valore di alcuni bit (bit A e bit B) se Alice e Bob prendono questi due bit e decidono di non usare questo valore bensì la loro somma modulo 2 come chiave l'informazione che Eve ha sulla stringa è più bassa, c'è in qualche modo un abbassamento della conoscenza che Eve ha sulla chiave riconciliata ,ovviamente non è necessario sacrificare il 50% dei bit esistono algoritmi più efficienti, ma la logica è che esistono protocolli classici sviluppati dopo l'avvento della crittografia quantistica perché c'è una necessità pratica per questo tipo di protocolli che consentono di estrarre, essenzialmente delle stringhe sicure sulle quali Eve ha in qualche modo della conoscenza alcuni commenti alcuni li ho già fatti consente ad Alice e Bob il primo è appunto a cosa serve un protocollo di distribuzione di chiavi quantistiche, consente ad Alice e Bob di condividere una chiave privata e sapere se essa è sicura una altra cosa importante che fino ad ora non ho detto e che ai professionisti non sarà sfuggito è che il canale deve essere autenticato, cioè un attacco semplice come il man in the middle. alla fine di questa procedura se Alice e Bob non si accorgono di Eve in mezzo Eve può ricevere, codificare e poi ritrasmettere un altro messaggio a Bob. Vi faccio presente che nei sistemi crittografici a chiave pubblica che sono a sicurezza incondizionata la trasmissione del testo cifrato può avvenire sul canale pubblico non è necessaria alcuna segretezza del canale di trasmissione quello che è necessario è che sia segreto la chiave. Per autenticare il canale è necessaria una chiave può sembrare una soluzione tipo comma 22 (ho bisogno di una chiave per autenticare una chiave? Può essere possibile), in realtà la cosa non è così perché l'autenticazione può avvenire con una chiave crittografica corta, allora cosa faccio io. Alice e Bob si incontrano una volta per tutte al bar si scambiano una chiave corta poi se ne vanno uno a Roma e uno a Milano Cominciano a mettere in moto il protocollo e se il canale è autenticato e se hanno successo hanno stabilito la chiave crittografica più lunga, in questo senso alcuni chiamano i protocolli di crittografia quantistica protocolli di accrescimento di chiave crittografica

cioè c'è un meccanismo per cui da una chiave più piccola 10 bit uno riesce ad avere una chiave più lunga 10^4 , si può scegliere di mantenere gli ultimi 10 bit della stringa come chiave crittografica la volta seguente che abbiamo bisogno di metterci in contatto e di stabilire una chiave. Esempio corrotto: a sinistra abbiamo un laser, che emette fotoni polarizzati verticalmente, Alice usa una cella pocket cioè una scatoletta che a seconda degli impulsi elettrici ricevuti va ruotando la polarizzazione del fotone. Lungo la fibra ottica (linea lunga nell'esempio) viaggiano dei fotoni con polarizzazioni di direzioni stabilite. Bob utilizza anche lui una cella pocket per variare la polarizzazione del fotone incidente e fa una misura con un PBS. A questo punto vediamo cosa può fare Eve cioè è importante perché abbiamo bisogno di stabilire quella soglia di sicurezza. Allora la strategia più semplice per Eve è quella di prendere un fotone, lo intercetta lo misura e lo ritrasmette a Bob. Eve non conosce che base ha utilizzato Alice per codificare il suo fotone l'unica cosa che può fare è conoscerla in modo random così come Bob daltronde, o Eve ha misurato nella base corretta se ha misurato la base corretta allora è molto fortunata perché conosce il bit che ha trasmesso Alice, rimanda a Bob un fotone polarizzato nella base corretta e Bob non ha alcun modo di accorgersi del fatto che Eve è nel mezzo perché il valore del bit trasmesso da Alice, misurato da Eve e poi ritrasmesso e infine misurato da Bob sono tutti e tre coincidenti, Bob non ha alcun modo di accorgersi della presenza di Eve, tutta via può darsi che Eve ha misurato nella base quadrata. In tal caso ci sono due conseguenze. Eve non conosce quale è il valore del bit perché il valore della sua misura è scorrelato ma essendo scorrelato il valore della sua misura la polarizzazione del fotone che manda a Bob è scorrelata con quella che ha mandato Alice quindi supponiamo che Alice ha mandato un fotone polarizzato a 45 gradi Eve misura nella base orizzontale/verticale ottiene con uguale probabilità zero od uno supponiamo abbia preso 0 quindi secondo Eve il fotone è polarizzato orizzontalmente Eve manda un fotone polarizzato orizzontalmente a Bob e quest'ultimo usa la stessa base che ha usato Alice quindi i due risultati dovrebbero coincidere ma siccome il fotone è polarizzato orizzontalmente e lei usa la base a 45 gradi il risultato è con egual probabilità zero o uno quindi i due risultati sono totalmente scorrelati nella metà dei casi coincidono ma nell'altra metà dei casi il bit di Alice e quello di Bob che dovrebbero coincidere sono differenti. In generale siccome Eve può sbagliare base nella metà dei casi e nella metà dei casi può essere scoperta su un singolo bit la probabilità che venga scoperta se faccio il confronto è dell'

ordine del 25% considerate poi che i bit che vengono confrontati sono dell'ordine del migliaio segue che la probabilità di non essere scoperti è molto bassa. Si potrebbe obiettare che la stupidaggine sta nel fatto che Eve si ostina ad intercettare i fotoni e volerli misurare, perché non se ne fa una copia guarda in che stato è spedisce l'originale a bob e fa una misurazione sulla copia senza rovinare l'originale; purtroppo non ciò non funziona perché uno dei teoremi fondamentali della meccanica quantistica è che se ho un fotone in uno stato quantistico e non so che stato è non posso fare una copia immaginate che il pallino rosso dell'esempio sul lucido sia una macchina che prende un fotone in uno stato sconosciuto e ne produce due nello stesso stato di polarizzazione, è bene questa macchina non esiste e non può essere costruita in nessun modo non esistesse un meccanismo di clonazione di un fotone di cui non si conosce lo stato in cui è in partenza, una cosa che si può fare comunque è una clonazione parziale cioè una copia approssimata di un fotone di cui non si sa qual'è lo stato di partenza. Esiste tutta un'industria di ricercatori che va studiando qual'è il cloning ottimale che si può avere data una certa famiglia di stati. Il problema è che fare delle copie approssimate comunque disturba l'originale ogni qualvolta Eve cerca di raccogliere delle informazioni sul sistema sui fotoni in transito disturba il loro stato più informazione acquisisce più lo stato è disturbato questa è in qualche modo una sorta di conseguenza del teorema di indeterminazione di Heisenberg Allora notate a questo punto che una cosa importantissima dal punto di vista pratico dal punto di vista dei protocolli la crittografia quantistica è quando Alice manda degli impulsi laser con dei fotoni a Bob, questi impulsi devono contenere realmente un fotone, il problema che a Bob gli impulsi laser che hanno mediamente un fotone possono emettere due un impulso laser ha un fotone Alice può fare la seguente cosa prende un beam splitter cioè una certa probabilità che un fotone venga trasmesso a Bob e c'è una certa probabilità che l'altro rimanga a lei, ecco che con quest'ultimo lei può fare una misura senza essere osservata mentre Bob misura l'originale che non è disturbato quindi dal punto di vista sperimentale questa è una cosa difficile da analizzare è importante essere sicuri che la sorgente sia a singolo fotone, abbiamo un laser che manda degli impulsi così deboli da contenere un fotone per volta abbiamo cioè un laserino con raggio poco luminoso, siccome l'intensità è proporzionale al numero di fotoni il raggio è così poco luminoso che va sputtacciando un fotone per volta (mai due tre fotoni per volta) e questo è un problema sia pratico che teorico, avere laser così deboli e così affidabili

non è una cosa banale. Andiamo a vedere quali sono le strategie più sofisticate che può avere Eve. **Per stabilire la soglia di sicurezza bisogna sapere qual è la massima informazione che può ottenere Eve sui fotoni in transito.** A questo punto uno può prendere due approcci totalmente distinti uno è dire con la tecnologia disponibile adesso cosa può fare Eve questo è carino ma non va bene (il perché dovrebbe essere chiaro ad un informatico) perché **nessuno vieta ad Eve di avere una tecnologia migliore di quella che ha adesso. Quando si fa un'analisi di Eavesdropping cioè di va a vedere cosa può fare Eve sul segnale, bisogna sempre assumere che Eve non abbia limiti tecnologici ha tutti gli strumenti possibili e tutti gli strumenti che sono perfetti, L'unico limite che Eve ha sono le leggi della quantistica perché il laser sarà bello quanto vuoi ma sempre un sistema quantistico ma sempre un sistema quantistico e così via per beam splitter e fotorivelatori, una cosa l'imperfezione tecnologica una cosa è leggi a cui il dispositivo deve ubbidire l'unica cosa che si deve assumere è che Eve sia un oggetto quantistico.** Allora i primi attacchi che si possono fare sono gli attacchi individuali le linee blu dell'esempio sono sostanzialmente i fotoni in transito con Alice a sinistra e Bob a destra, **Alice prepara e spedisce fotoni a Bob. Eve fa interagire ognuno dei fotoni con un sistema ausiliario (striscette in rosso) . Sistema ausiliario significa essenzialmente fare una copia imperfetta. Fa delle coppie imperfette e le va misurando una ad una. Bob riceverà degli stati che sono disturbati.** Questo tipo di attacchi prende il nome di attacchi individuali questo perché i fotoni in transito vengono misurati uno ad uno . Esiste una seconda strategia più sofisticata quella detta degli attacchi coerenti. **Allora Eve è ancora più furba e può fare interagire ognuno dei fotoni in transito da Alice a Bob con un probe però anziché misurarli uno ad uno li conserva tutti e aspetta che la trasmissione sia terminata alla fine fa la sua misura.** Questo dal punto sperimentale conservare lo stato di un fotone in modo coerente e aspettare una ventina di minuti e anche secondi e immagazzinare questi fotoni per congelarli per poi misurarli alla fine non è una cosa che si

possa ancora fare però in linea di principio è una strategia che uno deve poter immaginare. L'attacco più generale è l'ultimo in basso nella slide; l'attacco più generale possibile è questo **Alice spedisce dei fotoni a bob Eve ha un sistema ausiliario molto più grande che va interagendo consecutivamente con tutti quanti i fotoni in transito quindi fa una misura sull'insieme dei fotoni intransito, si conserva il sistema probe in un congelatore quantistico che impedisce tutte le incoerenze, alla fine della trasmissione fa una misura.**

Questa classe di attacchi richiede tecnologie sempre più avanzate e perfette in una situazione pratica gli attacchi che vengono considerati sono quelli della classe 1 attacchi individuali. Anche perché degli attacchi individuali esiste una teoria consolidata e si sa ancora meno degli altri due attacchi, per chi si volesse appassionare al campo voglio dire che la teoria dell'analisi delle tecniche eavesdropping (IMP) è veramente diventata sofisticata. Nel giro di 5 anni ha raggiunto livelli di sofisticazione matematica veramente notevoli quindi anche se nel campo non ha raggiunto lo stadio finale ha già raggiunto una soglia di sofisticatezza notevole. Andiamo a vedere concettualmente come si procede nell'analisi di eavesdropping nel caso di attacchi individuali. In questo caso succede che Alice e Bob si scambiano i fotoni fanno le loro misure e anche Eve fa le sue misure quindi alla fine di tutte le misure esistono tre misure di bit quella spedita da Alice e quelle misurate da Bob e Eve. Queste stringhe sono rispettivamente A B ed E sono delle variabili random classiche che sono distribuite con una probabilità congiunta $P(A,B,E)$. Alice e Bob hanno accesso solo alle loro distribuzioni marginali cioè hanno accesso alla probabilità $P(A,B)$ confrontando i loro dati e conoscendo $P(A,B)$ devono cercare di stimare la probabilità congiunta $P(A,B,E)$ quindi da una distribuzione marginale devono cercare di conoscere la probabilità originaria che è una cosa non banalissima ma qualcosa si riesce a fare. **A questo punto cosa succede Alice e Bob dalla conoscenza che loro riescono ad ottenere della probabilità $P(A,B,E)$ loro devono stimare quanta informazione ha Eve sulle loro stringhe (informazione nel senso di Shannon, entropia di partenza e entropia incodificata), quant'è la mutua informazione che ha Eve sulla stringa di Alice e quant'è la mutua informazione che ha Eve sulla stringa Bob, confrontano la stima che loro hanno il valore max che**

eve può avere sulle loro stringhe con la muta informazione che Alice ha su Bob o Bob su Alice allora se la muta informazione di Alice su Bob è maggiore della muta informazione che Eve ha su Alice o su Bob allora esiste un teorema di crittografia classica di ..Cassirer e Corn è possibile stabilire una chiave segreta usando semplicemente error correction e amplificazione di informazione (privacy). Se uno fa un'analisi dell'attacco individuale più generale possibile per il BB84 si può vedere che la soglia di errore più tollerabile al di sotto della quale è possibile stabilire una chiave segreta anche se c'è Eve è dell'ordine del 15% cioè è possibile tollerare un QBER è dell'ordine del 15% in realtà si può fare anche di più con delle tecniche che non descrivo qui tecniche di advantage amplification che sono delle tecniche con un QBER dell'ordine anche del 25 consentono comunque di stabilire una chiave segreta random, sono protocolli classici però sono molto meno efficienti degli error-correction & privacy. Adesso arriviamo alla parte più esotica o esoterica del seminario. Il protocollo che vi ho descritto prima è il cosiddetto BB84 ed esistono delle varianti che sono concettualmente simili. Se voi fate attenzione l'uso di due basi è piuttosto ridondante quello che è importante e che vengano spediti stati che non sono ortogonali tra di loro, **esiste un protocollo che prende in nome di Bennett92 che invece di aggiungere 4 stati verticale orizzontale ± 45 usa 2 stati di polarizzazione non ortogonali tra di loro**, però non è concettualmente molto diverso dal BB84; Discutiamo invece di questo protocollo che fu sviluppato nel '91 da Ekert. Ekert usa un altro ingrediente, una delle cose più curiose della meccanica quantistica il cosiddetto entanglement. Supponiamo di aver due fotoni che stanno nello stato ψ raffigurato indicato nella slide sopra all'inizio questo stato prende il nome di **stato EPR** (Einstein Poldosky Rosen); Einstein che è il papà del concetto di fotone in realtà ha sempre creduto che la meccanica quantistica avesse sempre qualcosa di sbagliato, e per tutta la vita cercò sempre di dimostrare che qualcosa non andava, quello che fece fu porsi il seguente esempio: Supponiamo di avere questo stato, dove i fotoni sono o verticale orizzontale oppure, con uguale ampiezza orizzontale/verticale; Supponiamo che Alice faccia una misura del suo fotone; Alice può trovare con eguale probabilità il fotone nello stato verticale oppure orizzontale, però la cosa interessante è che Alice una volta che misura il suo fotone nello stato verticale istantaneamente lo stato del

fotone di bob collassa nello stato orizzontale. Così come istantaneamente se Alice misura lo stato del suo fotone nello stato orizzontale quello di Bob collassa nello stato orizzontale, (capite che il concetto di qualcosa che avviene istantaneamente non garbasse molto ad Einstein) però succede realmente questo ma succede anche di più. Questo tipo di variazioni sono spiegabili in linea di principio sono spiegabili anche classicamente cioè io posso aver un sistema che classicamente correlato tale che se io misuro orizzontale lui è sempre verticale posso cioè immaginare sempre un sistema classico che abbia statisticamente questa stessa distribuzione di risultati e allora facciamo una cosa, anziché tenere lo stesso stato abbiamo detto che lo stesso stato possiamo esprimerlo in un'altra base supponiamo di esprimerlo nella base $+45$ gradi oppure in una base n dove n è una qualunque direzione di polarizzazione ed n_{\perp} perpendicolare che è la direzione di polarizzazione ortogonale. Bene potete vedere dalla slide che lo stato di polarizzazione mantiene sempre la stessa forma quindi questa correlazioni non locali istantanee dove a seguito di una misura so istantaneamente cosa misura il destinatario li valgono qualunque sia la base in cui Alice e Bob fanno la misura purché sia la stessa purché Alice e Bob sappiano in partenza in che base stanno facendo la misura, sanno anche che ogni qualvolta Alice misura verticale Bob misura orizzontale e viceversa oppure se Alice misura a $+45$ Bob misura a -45 e lo fanno istantaneamente.

vediamo dunque meglio questo protocollo eckert91 nella sua variante semplice. La versione alla bb84 è la seguente supponiamo di avere una sorgente di stati EPR entanglement correlati quantisticamente una copia c'è lì ha Alice una copia ce li ha Bob e Alice e Bob decidono di misurare o nella base verticale orizzontale o nella base $+45$ in modo random. Se sono ognuno nella opportuna base i loro dati sono correlati oppure non hanno nessuna relazione l'uno con l'altro. Il resto del protocollo è identico a bb84. La versione originale del protocollo di eckert91 utilizza però quella che viene chiamata disuguaglianza di Bell quindi è un poco diverso; Alice e Bob fanno delle misure ma non scegliendo in modo random fra due basi bensì scegliendo in modo random tre direzioni di polarizzazione. Quando Alice e Bob misurano nella stessa base i risultati sono correlati quando misurano in basi diverse, però esiste una cosa che si chiama teorema di Bell che dice la distribuzione statistica di questi risultati deve violare una certa

disuguaglianza. Allora Alice e Bob anziché scartare i risultati delle misure che non coincidono li confrontano, fanno un'analisi statistica e vede se questi dati statistici soddisfanno una certa disuguaglianza. Se la disuguaglianza viene soddisfatta vuol dire che realmente lo stato è realmente uno stato entanglement, se c'è stato Eve che è andato tamponando questi fotoni in transito, questa natura non locale istantaneamente correlata si perde. nel momento in cui Alice fa una misura distrugge queste correlazioni non locali istantanee e uno se ne può accorgere facendo una stima dei dati e vedendo se questa disuguaglianza viene violata oppure no. Quello in figura è un modello sperimentale del protocollo Ekert91. Abbiamo una sorgente di fotoni entangled, che sono degli stati non lineari che vengono pompati con un laser di non molto alta intensità. I fotoni del laser vengono convertiti in fotoni a più bassa frequenza ma quantisticamente correlati questi vengono spediti in fibra ottica ad Alice e Bob che hanno una cella Pockel che li consente di orientare la base e fare la misura con i PBS. Qual'è il messaggio che cerco di dare con questo messaggio, è che l'uso di sistemi quantistici e una serie di protocolli essenzialmente classici, consente a due parti Alice e Bob di condividere una stringa di dati random segreta anche se siamo in presenza di eavesdropping cioè in presenza di qualcuno che va tamponando con i fotoni in transito. Mi scuso per non aver portato delle trasparenze con delle belle foto sexy sperimentali che fanno vedere laser in azione però questa non è fantascienza esistono prototipi preindustriali da diversi anni 2001-2002 che funzionano su fibra ottica telecom 1.5micron sotto il lago di Ginevra su distanze dell'ordine dei 100km esistono prototipi industriali che funzionano in free space quindi essenzialmente via laser. Vedete che queste distanze sono dell'ordine di una LAN quindi uno può pensare ad applicazioni di protocolli di crittografia quantistica con un bit-rate abbastanza efficiente con un rate di creazione di chiave sufficientemente elevato da essere poi praticamente utile su distanze dell'ordine delle centinaia di km esistono poi enti che stanno provando a fare crittografia quantistica da satellite con laser a singolo fotone da terra e facendo singole misure poi non locali non è facilissimo ma ci si sta lavorando anche se il bit-rate è molto più basso quindi si può pensare anche sistemi distribuiti. Ma intanto sicuramente sui sistemi a terra su fibra orrica qualcosa si ottenuto.