Comunicazioni Sicure

devim

Indice

Introduzione

La comunicazione sicura di informazioni critiche è una questione importante che diventa una necessità quando si vuole proteggere il proprio anonimato. Con riferimento al caso d'uso, quando ci si trova in un ambiente non fidato, come ad esempio un servizio nascosto di terze parti, si può ricorrere alla cifratura del messaggio per evitare che altri ne leggano il contenuto. Un'altra soluzione è quella di utilizzare un canale sicuro, come ad esempio un proprio servizio nascosto protetto con credenziali di accesso, ma questo presuppone che il destinatario conosca tutti i dettagli su tale canale, nell'esempio sono l'indirizzo del servizio e le credenziali. Dunque è necessario poter comunicare queste informazioni in maniera sicura, perciò il problema persiste.
Scambiare un segreto tra due persone anonime può risultare non essere così semplice. Si illustreranno alcune tecniche con relative problematiche e si procederà poi con l'introduzione di alcune possibili soluzioni.

Problematiche nello scambio delle chiavi

Per inviare un messaggio sicuro da un utente A (Alice) ad un utente B (Bob) lo si può cifrare con una chiave condivisa. Tale chiave spesso viene usata per una cifratura simmetrica del messaggio, infatti algoritmi di cifratura asimmetrica per messaggi lunghi diventano inefficienti. La chiave segreta condivisa S deve, però, essere inizialmente scambiata tra A e B. In genere per riuscire a condividere questo segreto in maniera sicura si utilizzano protocolli basati su cifratura asimmetrica, come RSA o Diffie-Hellman. Una problematica fondamentale è che in entrambi i casi si è vulnerabili ad attacchi Man-in-The-Middle a causa della mancanza di autenticazione (Figura 1). Infatti, ad esempio, all'interno della rete TOR se un utente inviasse la propria chiave pubblica ad un altro utente all'interno di un servizio nascosto, il server stesso potrà vedere la chiave pubblica. Il problema è che quindi il server potrebbe potenzialmente sostituire la chiave pubblica con un'altra. In particolare, se Alice scrivesse un messaggio a Bob con la propria chiave pubblica (P_A), il servizio nascosto X che stanno usando potrebbe sostituire P_A con la propria chiave pubblica P_X. Bob riceverà P_X, ma crederà che si tratti di P_A, quindi la userà per cifrare il segreto che spedirà come risposta. Il server può quindi intercettare e decifrare il messaggio di Bob indirizzato ad Alice, ottenendo la chiave segreta S, cifrarlo nuovamente con P_A e infine inoltrarlo ad Alice. È quindi necessaria una terza parte fidata (es. Certification Authority) alla quale Bob si può rivolgere per verificare che la chiave pubblica ricevuta sia effettivamente quella di Alice. Questo rappresenta una limitazione che è possibile superare con opportuni accorgimenti o con l'utilizzo di differenti approcci. Un metodo alternativo che permette di scambiare una chiave senza il ricorso ad una terza parte fidata è il *password-authenticated key agreement* che però si basa sull'assunzione che entrambe le parti conoscano già un segreto condiviso, quindi il problema sullo scambio di una chiave segreta iniziale rimane.

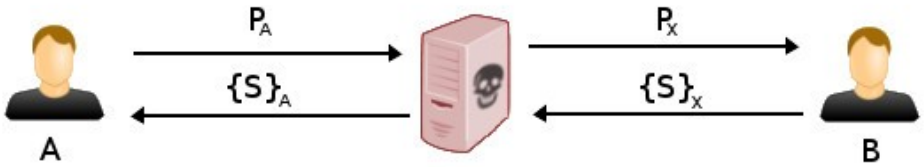

Figura 1. Illustrazione dello schema di un attacco MITM durante lo scambio di un segreto S.

Contromisura all'attacco MiTM

Una semplice, ma efficace, soluzione per evitare un attacco MiTM consiste nello sfruttare molteplici canali di comunicazione. Con riferimento all'esempio fatto nel paragrafo precedente, se Alice ripetesse l'invio della chiave P_A all'utente Bob usando N servizi nascosti, allora Bob potrà assumere di aver ricevuto correttamente P_A se in tutti gli N casi avesse ricevuto la stessa chiave (Figura 2). Inoltre, Bob si potrà anche accorgere di quanti e quali server stiano tentando un attacco MiTM con N sufficientemente grande rispetto al numero di server malevoli. Tenendo conto del caso d'uso preso in considerazione, utilizzare la stessa chiave pubblica più volte in contesti diversi potrebbe mettere a rischio l'anonimità, quindi anziché inviare ripetutamente la chiave pubblica la si può dividere in N parti ciascuna delle quali sarà inviata utilizzando un servizio nascosto differente. Usando quest'ultima variante, Bob non si potrà rendere conto se la chiave ricevuta sia effettivamente corretta, ma usandola per cifrare il messaggio e rispedendolo ad Alice sarà quest'ultimo a verificare con la propria chiave privata se il messaggio ricevuto sia corretto. Infatti, gli eventuali server malevoli potranno al più cambiare una parte della chiave, invalidando la comunicazione.

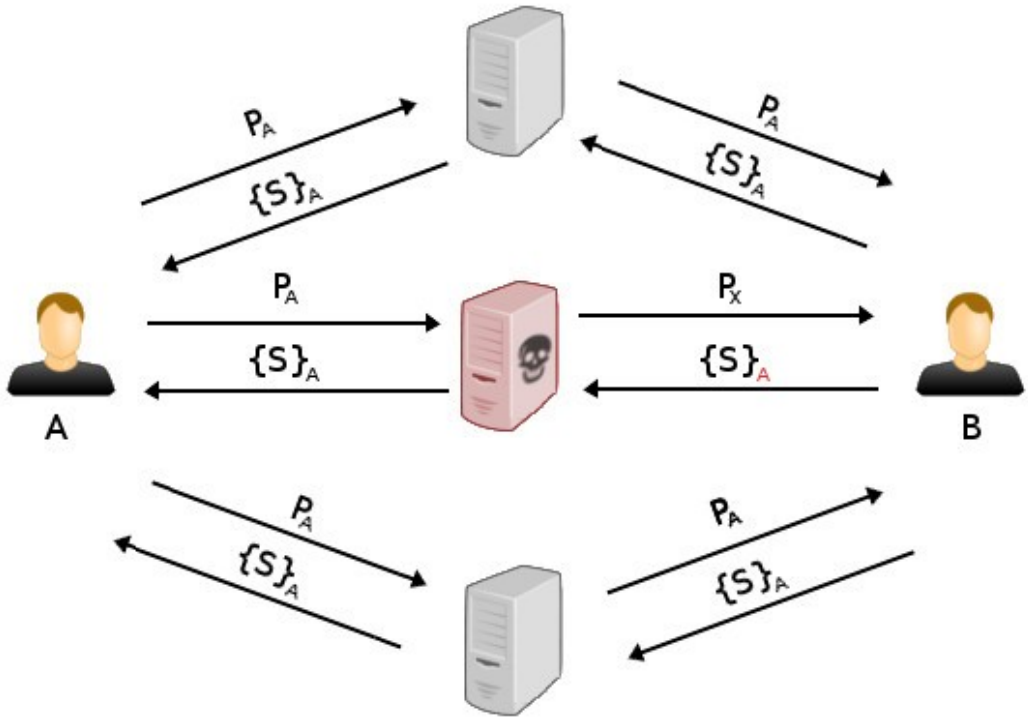

Figura 2. Schema che mostra come potersi accorgere di un attacco MITM sfruttando molteplici canali.

Sicurezza degli attuali algoritmi di cifratura asimmetrica

Prendendo in considerazione due dei più diffusi algoritmi asimmetrici, RSA e Diffie-Hellman, ci si può accorgere che essi si basano su problemi matematici computazionalmente onerosi da risolvere. Si noti che tali problemi non sono NP-completi, semplicemente la loro sicurezza è basata sull'assunzione che con la tecnologia attualmente disponibile si debba impiegare un tempo troppo lungo per riuscire a decifrare il messaggio senza possedere la chiave giusta.
La tecnologia dell'era moderna si sta sviluppando molto velocemente, si consideri ad esempio la *legge di Moore*, questo implica che la tecnologia adatta per risolvere tali problemi matematici efficientemente potrebbe diventare realtà in breve tempo. Nello stato dell'arte sono stati già ottenuti diversi risultati, come la fattorizzazione di una chiave RSA di 512 bit nel 1999 [1] e nel 2010 la fattorizzazione di una chiave RSA di 768-bit [2]. Ulteriori risultati riguardanti la fattorizzazione di interi, su cui si basa RSA, possono essere consultati nei riferimenti [3]. Quindi, studiando ed utilizzando tecniche sempre più efficienti per fattorizzare numeri interi e vasti insiemi di calcolatori (*cloud computing*) si è riusciti a mettere in discussione la sicurezza di RSA con chiavi "brevi" (inferiori a 1024 bit). Inoltre, sono stati teorizzati dispositivi hardware appositi per tentare di risolvere la fattorizzazione di interi efficientemente [4], fino ad arrivare alla definizione di un dispositivo che potenzialmente potrebbe riuscire a fattorizzare una chiave RSA da 1024-bit in un anno [5].
Attualmente si lavora molto anche su un nuovo tipo di tecnologia: i computer quantistici, che si basano sulla meccanica quantistica e che sono in grado di risolvere efficientemente (tempo polinomiale) la fattorizzazione di interi usando l'algoritmo di Shor [6]. Per fare un esempio, l'algoritmo di Shor potrebbe potenzialmente violare una chiave RSA di 4096 bit in circa un'ora. Per AES esiste, invece, l'algoritmo di Grover che però è meno efficiente. Risolvere la fattorizzazione di interi è sufficiente per risolvere il problema del logaritmo discreto, sul quale si basa Diffie-Hellman, e viceversa [7].
Anche utilizzando differenti algoritmi asimmetrici, ancora oggetto di studi, considerati attualmente "resistenti" ad attacchi effettuati mediante computer quantistici [8], solamente perché non è ancora noto un algoritmo abbastanza efficiente per risolverli, rimane il problema di fondo; per la natura stessa dei problemi matematici sui quali si basano sarà sempre possibile iniziare un attacco *brute-force* che in un momento indefinito del futuro avrà successo.

Crittografia quantistica

A partire dal 1980 è stato introdotto il concetto di computer quantistico, ambito nel quale si continua tutt'ora a lavorare e intorno al quale sono stati fatti diversi studi anche relativi alla crittografia. Una tale architettura è strutturata in maniera differente rispetto ai comuni calcolatori, infatti si basa sui *quantum bits* (*qubits*). Un *qubit* può assumere due stati, i quali indicano uno 0 o un 1, come ad esempio la polarizzazione di un fotone. La polarizzazione può essere orizzontale (indicando uno 0) o verticale (indicando un 1) nel caso si utilizzi una base computazionale (*rectilinear*/*computational basis*). I rispettivi simboli matematici per rappresentare tali stati sono: $|0\rangle_+$ e $|1\rangle_+$. Nel caso si abbiano due utenti, Alice e Bob, la trasmissione di un bit da Alice a Bob può avvenire usando una fonte luminosa (es. laser), che supponiamo per semplicità emettere un singolo fotone, e due polarizzatori (o lenti polarizzanti) come in figura 3. Se i due polarizzatori orienteranno il fotone nello stesso verso, allora vi passerà attraverso altrimenti non arriverà a Bob. Quindi, Bob assumerà di aver ricevuto uno 0 quando non vedrà nulla e un 1 quando riceverà il fotone.

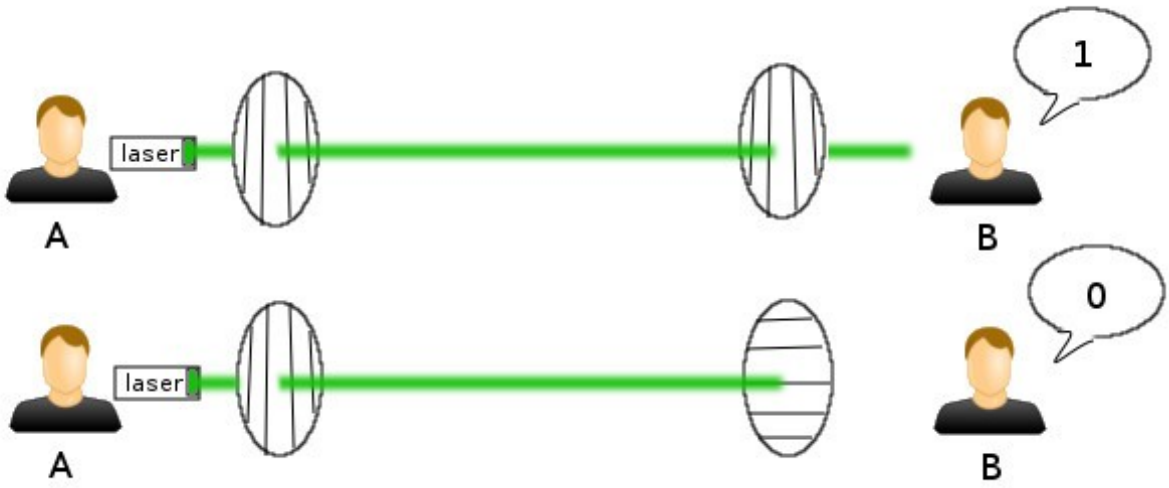

Figura 3. Illustrazione per la trasmissione di qubit. I polarizzatori sono indicati con degli ovali le cui righe interne ne specificano il verso di polarizzazione.

In questo contesto se un osservatore effettuasse una misurazione sullo stato del fotone durante la trasmissione potrebbe vedere con certezza il valore del bit che Bob riceverà.
Orientando diversamente i polarizzatori è possibile anche polarizzare i fotoni con altre angolazioni rispetto quella orizzontale o verticale. Inclinando di 45° in senso antiorario il polarizzatore che prima era verticale, si avranno dei fotoni polarizzati in maniera tale da rappresentare un 1 e inclinandolo, invece, di 45° in senso orario si avrà uno 0. In quest'ultimo caso si è cambiata la base che viene detta diagonale (o di *Hadamard*), con associati i seguenti simboli: $|0\rangle_\times$ e $|1\rangle_\times$ (figura 4).

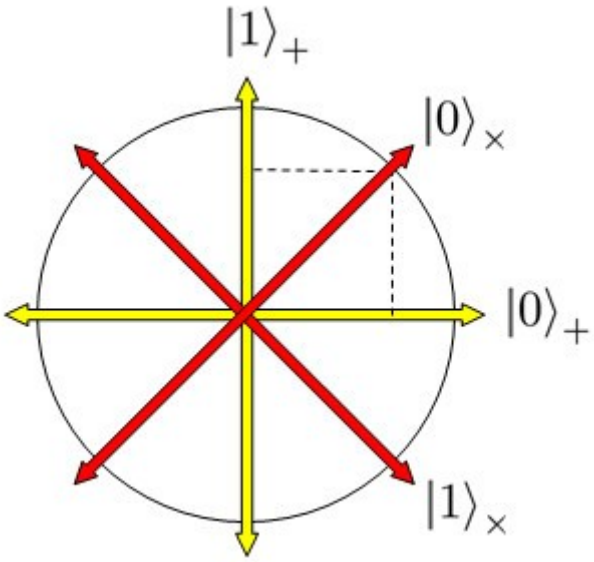

Figura 4. Rappresentazione grafica della base computazionale (in giallo) e della base diagonale (in rosso).

Lo stesso ragionamento fatto per la trasmissione di un bit con base computazionale rimane valido anche se con base diagonale. Lo stato $|0\rangle_\times$ è una combinazione lineare di $|0\rangle_+$ e $|1\rangle_+$, che si dice perciò essere una sovrapposizione (*superposition*) poiché, considerando la base computazionale, un fotone si trova contemporaneamente in due stati. Se Alice utilizzasse un polarizzatore in base diagonale e Bob un polarizzatore in base computazionale allora un fotone avrebbe il 50% di possibilità di passare, quindi Bob riceverà un bit in maniera casuale. In questo caso, se un osservatore effettuasse una misurazione sullo stato del fotone, usando una base diversa, otterrà in maniera imprevedibile uno 0 o un 1 e avrà l'effetto di far “collassare la funzione d'onda”,

ovvero di fissare lo stato del fotone in maniera tale che qualsiasi altro numero di misurazioni fatte in momenti successivi mostrerà il fotone sempre nello stesso stato [9]. Analogamente gli stessi ragionamenti valgono anche per $|0\rangle_+$ che è una combinazione lineare di $|0\rangle_\times$ e $|1\rangle_\times$.

Quantum Key Distribution

La distribuzione di un segreto (es. una chiave) tra due utenti, Alice e Bob, può avvenire in maniera sicura sfruttando un protocollo basato sulle leggi della meccanica quantistica e non su problemi computazionalmente onerosi. Come detto da Christian Schaffner al *Chaos Communication Congress* del 2015 [10] bisogna notare che per utilizzare un protocollo di questo tipo non è necessario avere a disposizione dei computer quantistici, ma basta avere un più semplice *quantum channel*, per cui esistono già dispositivi commerciali che lo implementano.
Una proprietà importante alla base di tali protocolli è il *No-Cloning Theorem* il quale afferma e dimostra che non è possibile duplicare esattamente uno stato quantistico sconosciuto a priori [11]. Un famoso protocollo di questo tipo è il BB84 [12] (figura 5). Nel BB84 Alice invia una serie di qubit casuali a Bob, ad esempio $|0\rangle_\times \quad |1\rangle_+ \quad |1\rangle_\times \quad |1\rangle_+ \quad |0\rangle_+$. Bob per ciascun qubit che riceve, poiché non conosce la base con cui è espresso, sceglie casualmente una base con cui interpretare il bit ricevuto. Inevitabilmente Bob otterrà una chiave con alcuni bit sbagliati, per rimediare a questo problema successivamente Alice lo informa sulle basi utilizzate, nell'esempio: $\times + \times + +$. Una volta ricevute le basi corrette, Bob può scartare quei bit per i quali ha usato una base diversa e comunicare ad Alice le posizioni dei bit da scartare. Alice e Bob a questo punto condivideranno una chiave che solo loro possono conoscere, infatti se ci fosse un utente malintenzionato (Eve) che volesse spiare la conversazione, per il *No-Cloning Theorem* non potrebbe copiare i qubit trasmessi. Se Eve dovesse interferire durante la trasmissione anche solo cercando di osservare lo stato dei qubit, nello stesso istante cambierebbe il loro stato. Più un utente malintenzionato prova ad apprendere osservando i qubit e più interferirà nella trasmissione rendendo evidente la sua presenza ad Alice e Bob che si potranno accorgere dell'intruso a causa dell'alto tasso di errori. Successivamente il protocollo prevede una fase di correzione degli errori e infine una fase chiamata *privacy amplification* che consiste nel ridurre la dimensione della chiave.

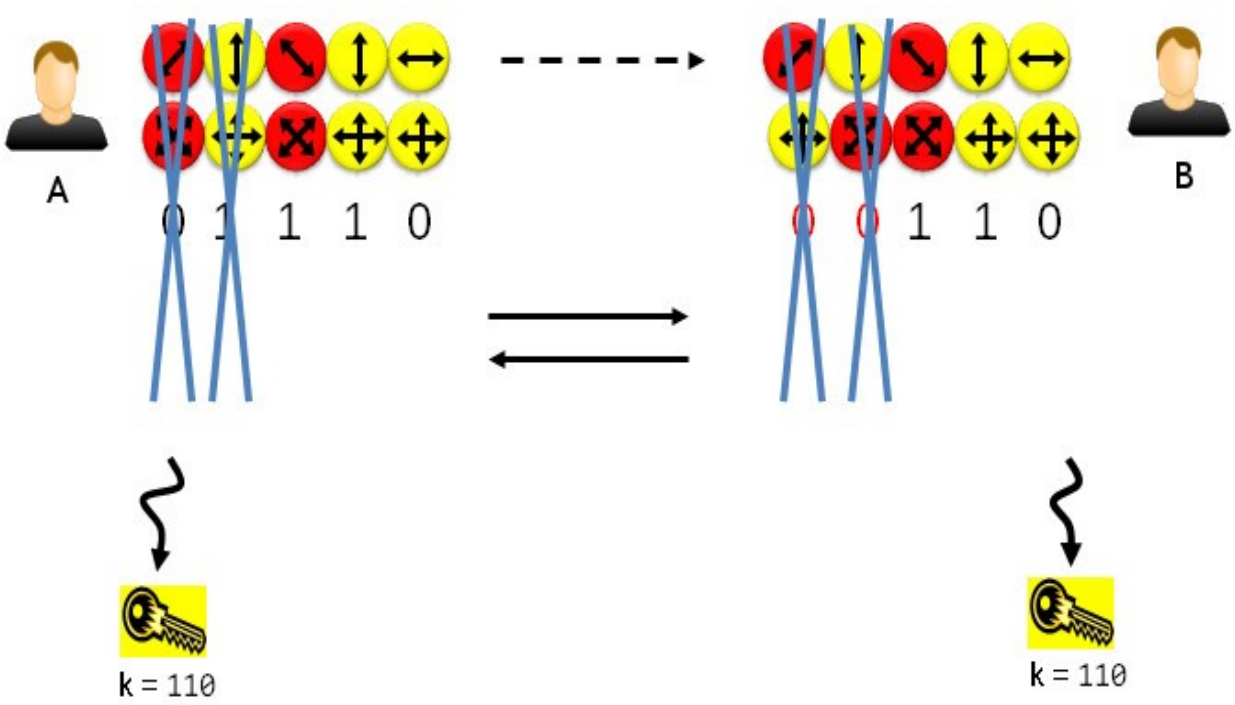

Figura 5. Trasmissione di una serie di qubit da A a B attraverso un *quantum channel* (trattegiato) come previsto dal protocollo BB84.

Protocolli come il BB84 si basano su una sicurezza matematicamente provata e quindi gli attacchi si concentrano soprattutto sui difetti delle implementazioni, come ad esempio sorgenti di fotoni imperfette [13].
Il BB84 prevede uno scambio di informazioni tra le due parti (es. le basi usate) attraverso un classico canale autenticato, sfruttando ad esempio RSA, ma nel caso non fosse possibile averlo, allora il protocollo sarebbe comunque vulnerabile ad un attacco Man-in-The-Middle. Un recente studio del 2015 mostra come utilizzando particolari MAC sia possibile garantire un canale autenticato sicuro e di come sia possibile mitigare eventuali attacchi MiTM nel caso si abbia un'autenticazione debole [14].

Correlazione quantistica

Un altro importante aspetto della meccanica quantistica sono gli stati correlati (*entangled*), ovvero insiemi di sistemi sovrapposti per i quali la singola misurazione effettuata su uno di essi determina anche lo stato degli altri. Ne sono un esempio le coppie EPR (*Einstein, Podolsky, Rosen*) ovvero coppie di qubit che si trovano in un particolare stato correlato (detto stato di *Bell*). Anche se distanti l'uno dall'altro, la misurazione effettuata su uno di essi produce con il 50% di probabilità uno 0 o un 1 fissandone lo stato e allo stesso tempo tale misurazione fissa anche lo stato dell'altro al medesimo valore. Questa caratteristica rende possibile il teletrasporto di uno o più qubit [15], il fenomeno viene detto *quantum teleportation*. Prima di sfruttare le proprietà di due sistemi correlati è necessario dividerli tra le due parti che desiderano sfruttarli, siano esse Alice e Bob. La *quantum teleportation* è ancora oggetto di molti studi, ad esempio nel settembre del 2015 il NIST ha stabilito un nuovo record di distanza [16]. Questo fenomeno sembrerebbe andare contro la teoria della relatività di Einstein, poiché sembrerebbe che l'informazione viaggi ad una velocità superiore a quella della luce. In realtà, la teoria della relatività rimane valida, poiché non c'è modo di trasferire informazione (*No-Communication theorem*) [17]. Alice non può inviare a Bob una serie di bit scelti sfruttando una coppia EPR, poiché l'unica cosa che è concessa ad Alice è quella di ottenere una

serie casuale di bit che allo stesso tempo sarà posseduta anche da Bob. Sistemi quantistici correlati possono quindi permettere la generazione di un segreto condiviso, uno dei primi protocolli basati su questa caratteristica è stato definito nel 1991 da Artur Ekert per la sua tesi di dottorato ad Oxford.

Riferimenti

[1] “Factorization of a 512-bit RSA Modulus”, 1999, http://www.iacr.org/archive/eurocrypt2000/1807/18070001-new.pdf

[2] “Factorization of a 768-bit RSA Modulus”, 2010, https://eprint.iacr.org/2010/006.pdf

[3] “Integer factorization records”, https://en.wikipedia.org/wiki/Integer_factorization_records

[4] “TWINKLE”, 1999, https://en.wikipedia.org/wiki/TWINKLE

[5] “TWIRL”, 2003, https://en.wikipedia.org/wiki/TWIRL

[6] “Shor's algorithm”, 1994, https://en.wikipedia.org/wiki/Shor's_algorithm

[7] Eric Bach, “Discrete logarithms and factoring”, 1984, https://www.eecs.berkeley.edu/Pubs/TechRpts/1984/5973.html

[8] “Post-quantum cryptography”, https://en.wikipedia.org/wiki/Post-quantum_cryptography

[9] “Wave function collapse”, https://en.wikipedia.org/wiki/Wave_function_collapse

[10] Christian Schaffner, “Quantum Cryptography”, 2015, https://www.youtube.com/watch?v=424LHQQB2DE

[11] W. K. Wootters e W. H. Zurek, “A single quantum cannot be cloned”, Nature 299, 1982, http://www.nature.com/nature/journal/v299/n5886/abs/299802a0.html

[12] C. H. Bennett e G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", 1984, http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

[13] Dominic Mayers e Andrew Yao, “Quantum Cryptography with Imperfect Apparatus”, 1998, http://arxiv.org/abs/quant-ph/9809039

[14] “Attacks on quantum key distribution protocols that employ non-ITS authentication”, 2015, http://arxiv.org/abs/1209.0365

[15] New York Times, “Scientists Teleport Not Kirk, but an Atom”, 2004, http://www.nytimes.com/2004/06/17/us/scientists-teleport-not-kirk-but-an-atom.html

[16] NIST, “NIST Team Breaks Distance Record for Quantum Teleportation”, 2015, http://www.nist.gov/pml/nist-team-breaks-distance-record-for-quantum-teleportation.cfm

[17] “No-Communication theorem”, https://en.wikipedia.org/wiki/No-communication_theorem