Quantum cryptography and quantum networks

R. Vilela Mendes
CMAFCIO, Universidade de Lisboa
http://label2.ist.utl.pt/vilela/

Introduction

- The security of public key cryptosystems is based on the difficulty to solve some number problems. For example the safety of the RSA cryptosystem (Appendix 1) is based on the difficulty of factorization.

Introduction

- The security of public key cryptosystems is based on the difficulty to solve some number problems. For example the safety of the RSA cryptosystem (Appendix 1) is based on the difficulty of factorization.
- Quantum computing (when available for a sufficient number of qubits) will solve the factorization problem in polynomial time, making RSA unsafe (Appendix 2).

Introduction

- The security of public key cryptosystems is based on the difficulty to solve some number problems. For example the safety of the RSA cryptosystem (Appendix 1) is based on the difficulty of factorization.
- Quantum computing (when available for a sufficient number of qubits) will solve the factorization problem in polynomial time, making RSA unsafe (Appendix 2).
- However if quantum algorithms raise this problem, they also provide the cure by developing the safe quantum key distribution (QKD).

Introduction

- The security of public key cryptosystems is based on the difficulty to solve some number problems. For example the safety of the RSA cryptosystem (Appendix 1) is based on the difficulty of factorization.
- Quantum computing (when available for a sufficient number of qubits) will solve the factorization problem in polynomial time, making RSA unsafe (Appendix 2).
- However if quantum algorithms raise this problem, they also provide the cure by developing the safe quantum key distribution (QKD).
- In parallel with QKD a strong effort is being carried out in the development of quantum resistant (classical) cryptosysytems. See, for example R. A. Perlner and D. A. Cooper; *Quantum resistant public key cryptography: a survey,* IDtrust '09 Proceedings and L. Chen; *Cryptography Standards in Quantum Time*, IEEE Secur Priv. 15 (2017) 51-57.

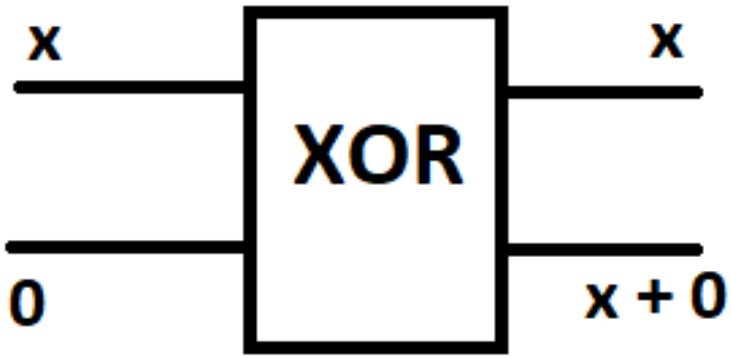
Introduction

- The security of public key cryptosystems is based on the difficulty to solve some number problems. For example the safety of the RSA cryptosystem (Appendix 1) is based on the difficulty of factorization.
- Quantum computing (when available for a sufficient number of qubits) will solve the factorization problem in polynomial time, making RSA unsafe (Appendix 2).
- However if quantum algorithms raise this problem, they also provide the cure by developing the safe quantum key distribution (QKD).
- In parallel with QKD a strong effort is being carried out in the development of quantum resistant (classical) cryptosysytems. See, for example R. A. Perlner and D. A. Cooper; *Quantum resistant public key cryptography: a survey,* IDtrust '09 Proceedings and L. Chen; *Cryptography Standards in Quantum Time*, IEEE Secur Priv. 15 (2017) 51-57.
- Here I will focus on QKD.

The no cloning theorem

At the root of quantum security (security based on quantum keys) is the fact that a quantum state cannot be cloned without disturbing it.

- **Classical cloning**



- **Quantum cloning**
  Would be the existence of a unitary operator U such that

$$U\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle \qquad \forall\psi, \langle\psi\,|\psi\rangle = 1$$

The no cloning theorem

It is impossible to clone a quantum state without disturbing it

Proof:

Let $|\psi\rangle$ and $|\phi\rangle$ be two different states, $|\langle\psi\,|\phi\rangle| < 1$

Then if U exists

$$\begin{aligned} U\left(|\psi\rangle \otimes |0\rangle\right) &= |\psi\rangle \otimes |\psi\rangle \\ U\left(|\phi\rangle \otimes |0\rangle\right) &= |\phi\rangle \otimes |\phi\rangle \end{aligned}$$

Because U is unitary

$$\langle\psi\,|\phi\rangle\,\langle 0\,|0\rangle = \langle\psi\,|\phi\rangle\,\langle\psi\,|\phi\rangle$$

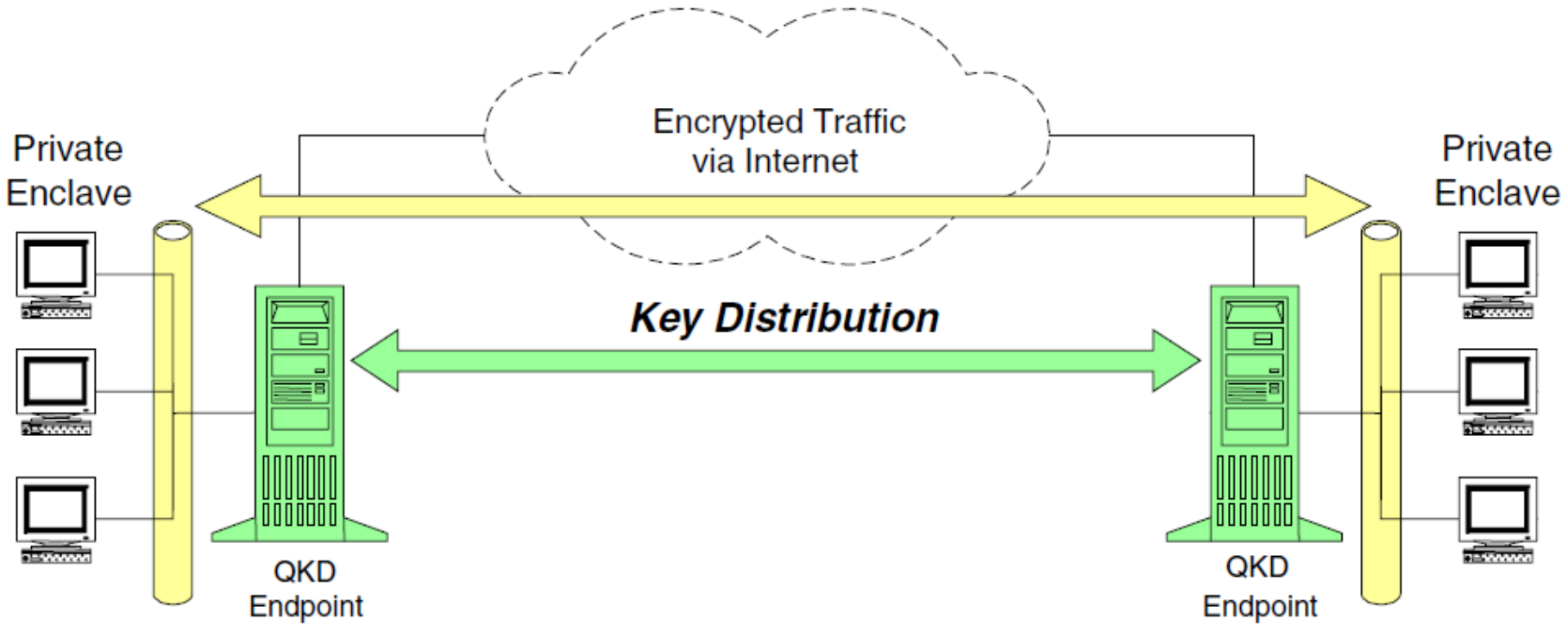
Then $\langle 0\,|0\rangle = 1$ implies $\langle\psi\,|\phi\rangle = 1$, a contradiction.

Private key criptography and quantum key distribution (QKD)

Basic ideas (not necessarily exclusive to quantum security)

- **Private key cryptography:** *Key shared by sender and receiver*
  Example: Vernam cipher, Message + Key = Coded message $\twoheadrightarrow$ *Coded message - Key = Message*
  Requires safe exchange of the key and one-time use (one-time pad).
- In the exchange of the key, discrepancies may arise by eavesdropping or imperfections in the transmission line and detectors.
- **Information reconciliation** and **Privacy amplification** aim at correcting errors and decreasing the mutual information of an eavesdropper with the secret key.
- *Examples: - For a key transmited through a noisy channel, reliability is improved by division in blocks and parity checks. If an error is found in a block, the process is iterated in that block (cascade protocol).*
  - Production of a shorter key by a hash function. If one suspects that x bits of a n-length key are suspect, this produces a safer key.

Private key criptography and quantum key distribution (QKD)



The BB84 protocol for QKD (Bennett, Brassard)

- Two different qubit basis

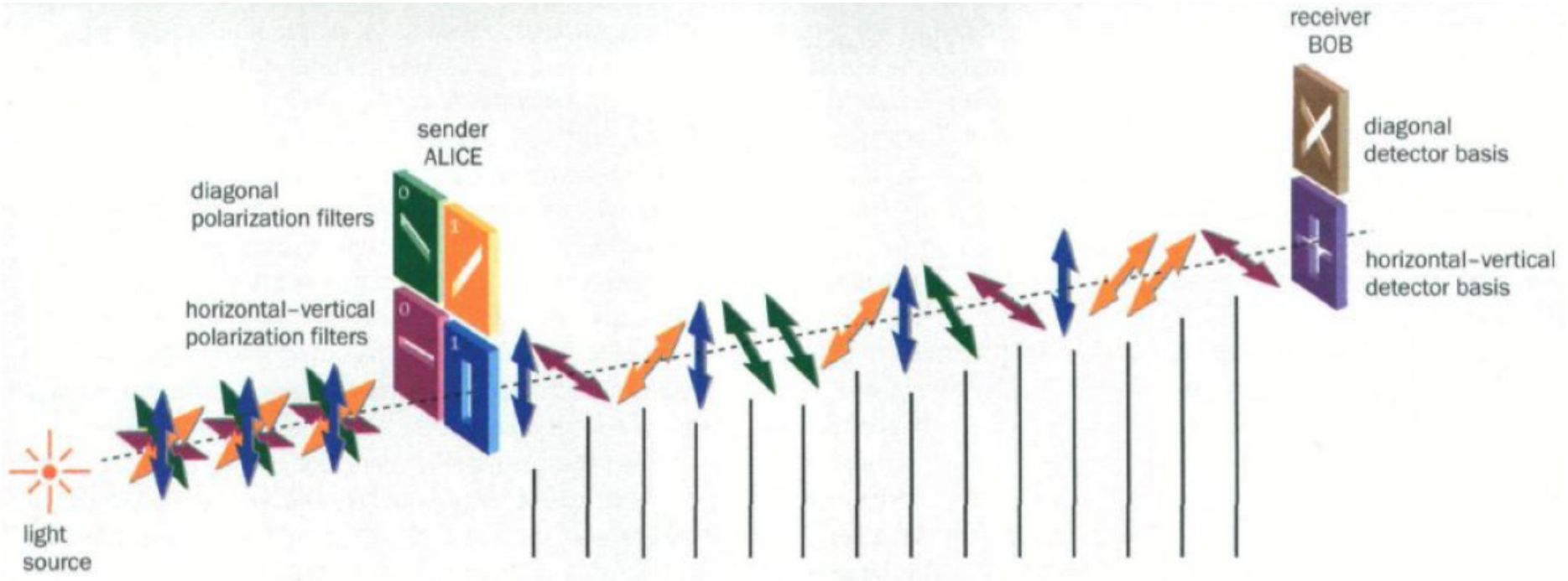
$$\begin{aligned}
\psi_{00} &= |0\rangle & &\longrightarrow & |\longleftrightarrow\rangle \\
\psi_{01} &= |1\rangle & &\longrightarrow & |\updownarrow\rangle \\
\psi_{10} &= \tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) & &\longrightarrow & |\nearrow\rangle \\
\psi_{11} &= \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) & &\longrightarrow & |\nwarrow\rangle
\end{aligned}$$

- The sender (Alice) has two random bit sequences α and β. α is the sequence to be sent, β decides which polarization is used (either the (ψ_{00}, ψ_{01}) basis or the (ψ_{10}, ψ_{11}) basis). The qubits are now in states that are not mutually orthogonal, and thus it is impossible to distinguish all of them with certainty without knowing β.
- The receiver (Bob) also has a random deciding sequence β' which he uses to decode the received signals generating a sequence α'. These might be changed by noise or eavesdropping by a third party (Eve).

The BB84 protocol for QKD (Bennett, Brassard)

- Eve cannot be in possession of a copy of the qubits sent to Bob, by the no-cloning theorem, unless she has made measurements. Her measurements, however, risk disturbing a particular qubit with probability $\frac{1}{2}$ if she guesses the wrong basis.
- After Bob has announced the reception, Alice and Bob communicate through a public (unsafe) channel to determine where β and β' are different. They now discard the bits in α and α' for which β and β' are different.
- Information reconciliation and privacy amplification follow $\Longrightarrow$ secret key.

BB84 with polarized photons



(Single photons, not beams!)

BB84: An example

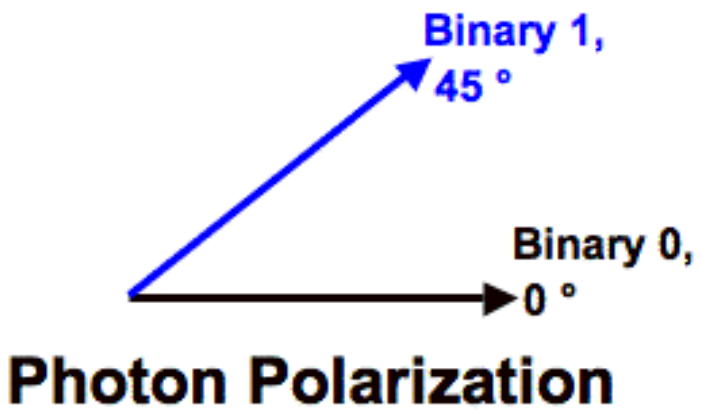
Alice's polar. states	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\searrow\rangle$	$\|\searrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$
Alice's bit value	1	0	0	1	0	0	0	1	1
Bob's basis	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Bob's measured states	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\searrow\rangle$	/	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$
Bob's bit value	1	1	0	1	1	0	/	0	1
Same basis?	Y	N	Y	N	N	Y	/	N	Y
Sifted key	1	/	0	/	/	0	/	/	1

BB84 under an intersect-resent atack

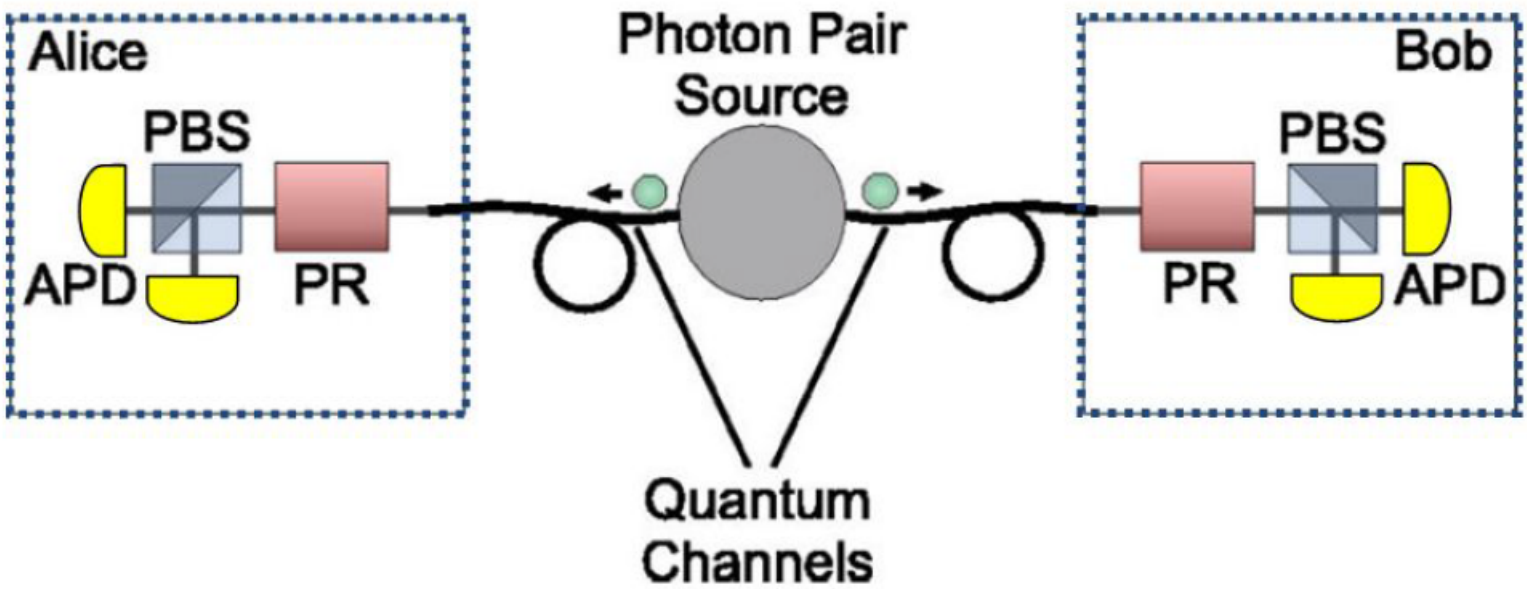
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↕	→	↘	↕	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↕	↗	→	↕	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↕	↗	↗	↘	→	↗	↕	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

B92 protocol

- A simplified version of BB84. The key difference to BB84 is that only two states are necessary rather than the 4 polarization states in BB84. 0 is encoded as 0 degrees in the rectilinear basis and 1 encoded by 45 degrees in the diagonal basis.
- Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use. Bob randomly chooses a basis to measure but if he chooses the wrong basis, he will not measure anything. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.



The entangled pair protocol



The entangled pair protocol

- A source emits pairs of qubits in a maximally entangled state like:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|\updownarrow\rangle \, |\longleftrightarrow\rangle + |\longleftrightarrow\rangle \, |\updownarrow\rangle \right)$$

- Alice and Bob measure their photons with one of three basis randomly chosen from the horizontal-vertical with rotations $\theta = 0, \theta = \frac{\pi}{8}, \theta = \frac{\pi}{4}$
- Alice and Bob release publicly which basis they have chosen for each measurement. They separate the measurements into three groups:
  - 1st group: Measurements using different orientations.
  - 2nd group: Measurements using the same orientation.
  - 3rd group: Measurements in which at least one of them failed to register a particle.
- Alice and Bob announce publicly only their results of the first group. Thus, they can check if eavesdropping has taken place.
- If no eavesdropper has perturbed the system, the second group is used to establish a secure key. The third group is discarded.

Practical implementations of QKD

Although everyday use of quantum computer is years ahead from implementation, quantum key distribution is already a reality and heading to commercialisation. Reliable quantum repeaters don't exist yet, something that constricts the range of a QKD network to a few hundred kilometers.

Some QKD networks

- The DARPA Quantum network has been running since 2004 in Massachusetts, USA.
- SECOQC, a computer network protected by quantum key distribution was implemented in October 2008 in Vienna. Used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west.
- The SwissQuantum network project installed in the Geneva metropolitan area in March 2009, to validate the reliability and robustness of QKD in continuous operation over a long time period in a field environment. The quantum network operated for nearly 2 years until the project was shut down in January 2011.

Practical implementations of QKD

- Chinese networks: May 2009, with a backbone network of four nodes connecting a number of subnets.
- The QUESS space mission, launched in August 2016. Is an international QKD channel between China and the Institute for Quantum Optics and Quantum Information in Vienna, Austria
- The Tokyo QKD Network
- Los Alamos National Laboratory, a QKD network since 2011.
- For recent developments in quantum and quantum-resistant cryptography see I.S. Kabanov et al.; *Practical Cryptographic Strategies in the Post-Quantum Era,* AIP Conference Proceedings 1936 (2018) 020021.

The quantum internet

In networks secured by QKD, the main communication tool are photons in optical fibers or space. In classical networks, losses and noise are compensated by amplification in repeaters. The no-cloning theorem makes this feature unsuitable for quantum communications. To establish a global network secured by QKD the attenuation and dephasing that limits direct quantum links to hundreds of kilometers must be addressed.
Possible solutions:
- Entangled repeaters
- Quantum error correction. Example: Code $|0\rangle$ by $|0000\rangle$ and $|1\rangle$ by $|1111\rangle$. If there is a qubit error, projection to a lower dimension subspace mantains coherence.
- Quantum teleportation of a state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
Let Alice and Bob share an entangled pair

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Quantum teleportation

Alice manipulates two qubits and Bob only one. Initial state (for Alice)

$$|\psi\rangle \otimes |\phi\rangle = \frac{1}{\sqrt{2}} \{\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle\}$$

Alice acts on the initial state by $U_A = U_H \otimes U_{CNOT} \otimes 1$; $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$U_A \frac{1}{\sqrt{2}} \{\alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle\} =$$

$$(U_H \otimes 1 \otimes 1) \frac{1}{\sqrt{2}} \{\alpha |000\rangle + \alpha |011\rangle + \beta |110\rangle + \beta |101\rangle\}$$

$$= \frac{1}{2} \left\{ \begin{array}{c} |00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) \\ + |10\rangle (-\alpha |0\rangle + \beta |1\rangle) + |11\rangle (-\alpha |1\rangle + \beta |1\rangle) \end{array} \right\}$$

Alice now measures the first two qubits and sends that information by a classical channel to Bob. Then he recovers $|\psi\rangle$ by acting on his qubit with the appropriate operator.

Appendix 1: The RSA cryptosystem (Rivest, Shamir, Adleman, 1977)

Public key system (trapdoor one-way function). Security based on the difficulty of factoring large integers, $t(n) \sim \exp\left(n^{1/3}\right)$

\# AT THE RECEIVER END

Pick $N = pq$, p and q two distinct large odd primes

Choose at random E coprime with $\phi(N) = (p-1)(q-1)$

Compute $B = E^{-1} \bmod \phi(N)$

PUBLIC KEY $= (E, N)$

PRIVATE KEY $= (B, N)$

Broadcast public key, keep private key for yourself

\# SENDER

Code each symbol in the message as a number from 0 to $n-1$ according to some known code $\{M_i\}$

Compute $\{C_i = M_i^E \bmod N\}$ and Send $\{C_i\}$

\# RECEIVER

Compute $\{C_i^B \bmod N = M_i\}$

Appendix 2: Cracking RSA with quantum computers

- Let the message be M^E
- Find order r of $M^E \bmod N$ (r is also the order of M because E is coprime to $(P-1)(Q-1)$)
- Find $D' = E^{-1} \bmod r$ (Euclid's algorithm)
- $\left(M^E\right)^{D'} = M \bmod N$ (because $M^r = 1 \bmod N$)

Finding order $\bmod N$. Shor's algorithm

Basic idea: create a state with periodicity r and then apply Fourier transform over Z_Q to reveal the periodicity
Fourier transform over Z_Q

$$|a\rangle \rightarrow \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} e^{2\pi i a b/Q} |b\rangle$$

Shor's algorithm

- $|\overrightarrow{0}\rangle \otimes |\overrightarrow{0}\rangle$
- Apply Fourier transform over Z_Q on the first register
  $\frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |\overrightarrow{0}\rangle$
- Call subroutine that computes $|l\rangle|d\rangle \rightarrow |l\rangle|d \oplus Y^l \bmod N\rangle$
  $\frac{1}{\sqrt{Q}} \sum_{l=0}^{Q-1} |l\rangle \otimes |Y^l \bmod N\rangle$
- Measure the second register
  $\frac{1}{\sqrt{A}} \sum_{l=0|Y^l=Y^{l_0}}^{Q-1} |l\rangle \otimes |Y^{l_0}\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |jr + l_0\rangle \otimes |Y^{l_0}\rangle$
- Apply Fourier tarnsform over Z_Q on the first register
  $\frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} \left(\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} e^{2\pi i (jr+l_0)k/Q} \right) |k\rangle \otimes |Y^{l_0}\rangle$
- Measure the first register. Let k_1 be the result.
- Approximate the fraction $\frac{k_1}{Q}$ by a fraction with denominator smaller than N using continued fractions.
- If the denominator d does not satisfy $Y^d = 1 \bmod N$, throw it away. Else call the denominator r_1.
- Repeat all previous steps poly(log(N)) times to get $r_1, r_2, r_3, \ldots$
- Output the minimal r.