Introduction to Quantum Computing
量子計算入門

Rod Van Meter
rdv@tera.ics.keio.ac.jp
September 28-30, 2004
@Aizu U.

with help from
伊藤公平
阿部英介
and slides from BBN

Course Outline

- Lecture 1: Introduction
- Lecture 2: Quantum Algorithms
- Lecture 3: Quantum Computational Complexity Theory
- Lecture 4: Devices and Technologies
- Lecture 5: Quantum Computer Architecture
- Lecture 6: Quantum Networking
- Lecture 7: Wrapup

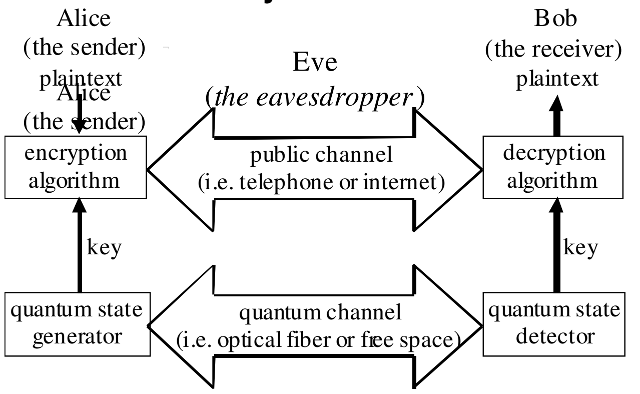
量子ネットワーク

- Quantum Key Distribution (QKD)
- Teleportation
- (Superdense coding)
- All discovered by Charles Bennett (IBM) & associates

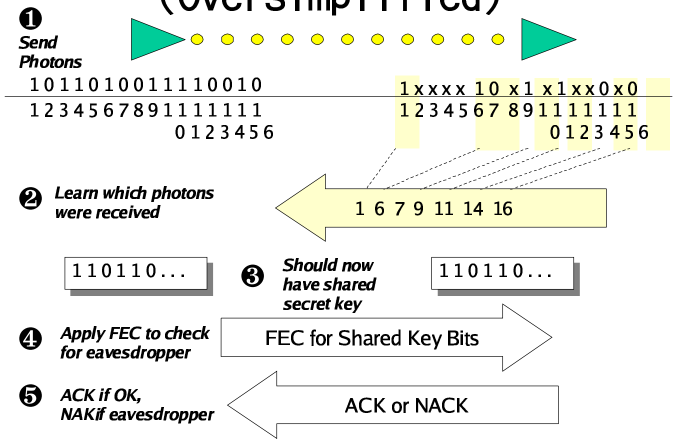
Quantum Key Distribution

- Bennett & Brassard, BB84 protocol
- Key distribution only, not data encryption
- Requires authenticated (not encrypted) classical channel to complete protocol
- Many, many places working on this!
  - BBN, Harvard, Boston U. for DARPA
  - MagiQ Technologies
  - CERN
  - 東大

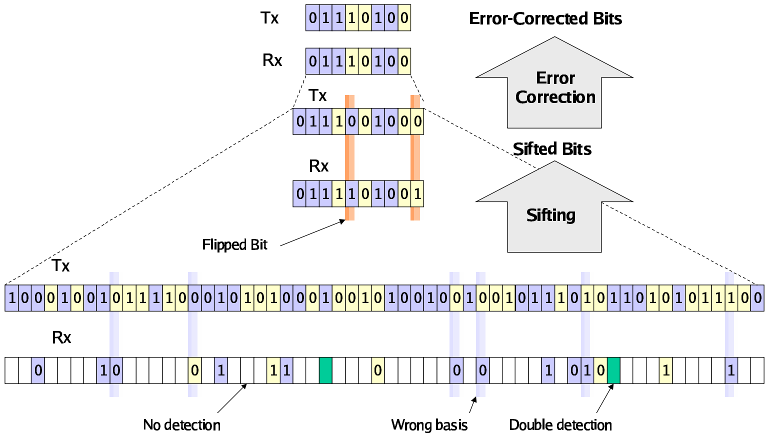
A New Kind of Key Distribution – Quantum Key Distribution



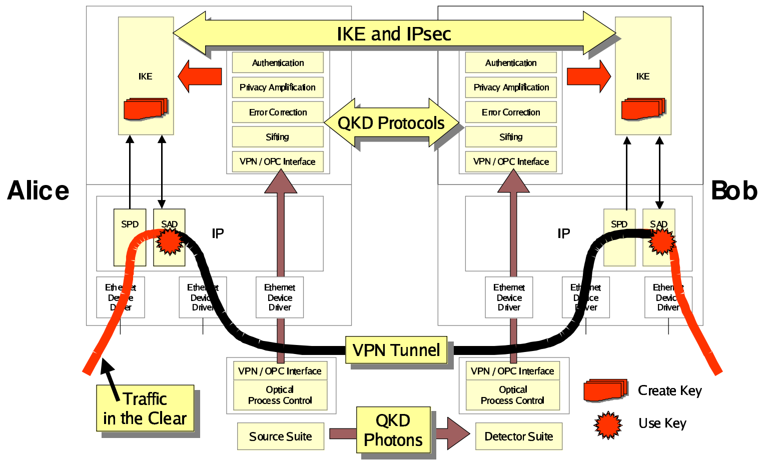
QKD Basic Idea (Oversimplified)



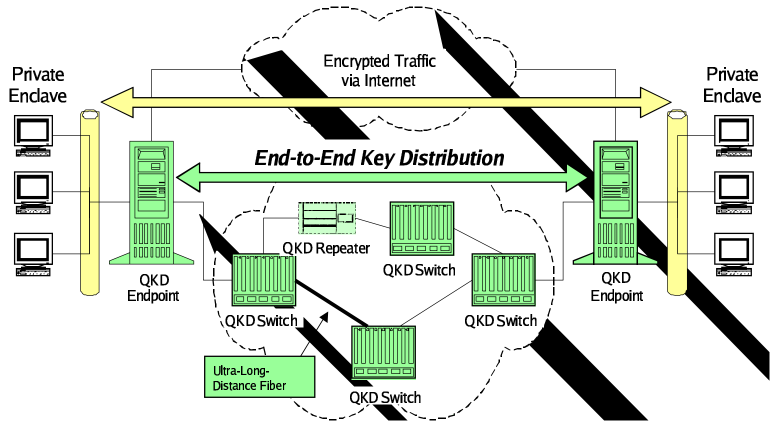
The Quantum Cryptographic Protocols



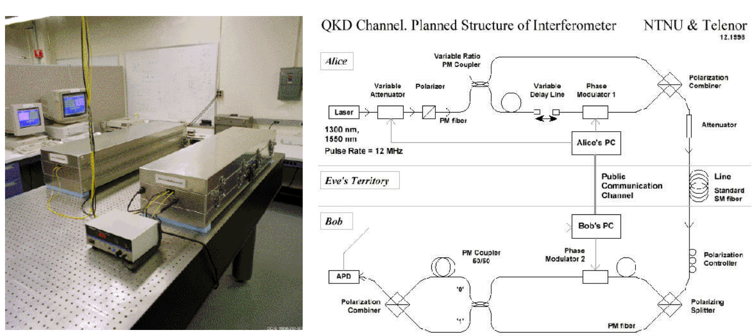
Putting It All Together



The DARPA Quantum Network

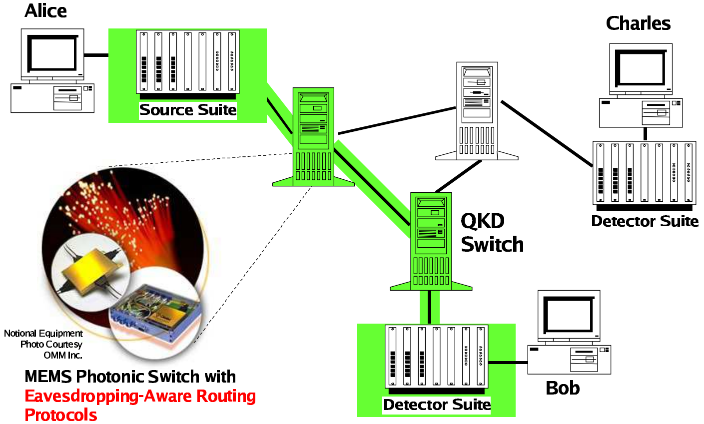


Current State of the Art

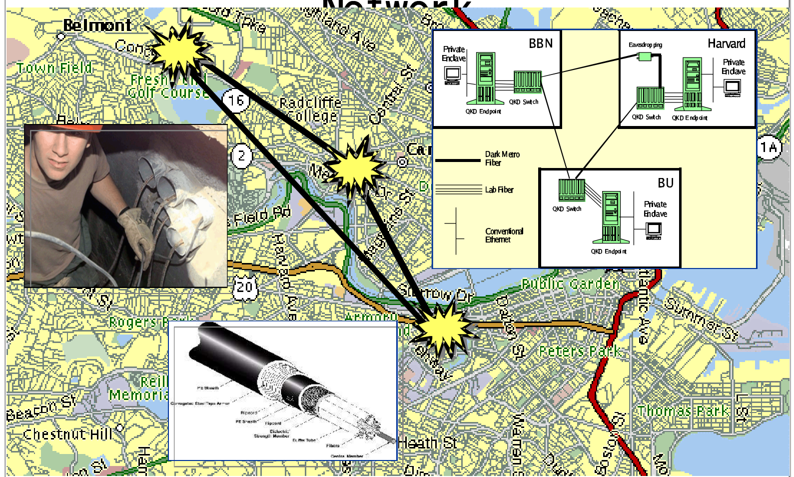


- Single Fiber Link, Point to Point
- Approx 50 Km through telco fiber
- Approx. 20 Kbps for key exchange

The DARPA Quantum Network – 3rd Year (2004?)



Building the DARPA Quantum Network



Repeaters

- Over long distances, probability of loss increases
- "Repeaters" essentially perform hop-by-hop QKD, meaning repeaters (routers) must be trusted
- Not yet demonstrated?
  (BBN demo now multi-node, not sure about multi-hop)

QKD and Shor

- QKD does not fix what Shor broke
- Primary impact of Shor is on *authentication* (public key crypto)
- QKD is (naturally) key *distribution*
- QKD still depends on authenticated channel
- Existing (classical) mechanisms for key distribution not broken by Shor
- Authentication is still possible even without public-key crypto

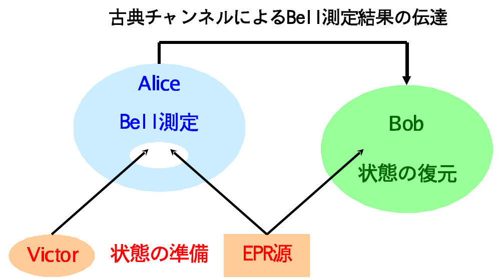
QKD Notes

- QKD can also be done through free space or the atmosphere, detecting single photons from several kilometers away
- Value of QKD in complete secure network architecture is debatable
  - Will people deploy an extra physical network simply to get more secure keys?

Teleportation

- 奇妙なことですが...
- 計算する前に、entangled pairをshareする
  - 一つを持って、一つを相手に送る
- 計算して（結果はAとよぶ)、持っているqubitにentangleして、測定して、古典的な結果を相手に送る
- 相手はその結果を使って、少し量子計算して、Aが出て来る。

量子テレポーテーション



$|\psi\rangle_V = \alpha|0\rangle_V + \beta|1\rangle_V$ $\quad |\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$
$$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$
$$XZ|\psi\rangle = \alpha|1\rangle - \beta|0\rangle$$

Bell基底

$$|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$
$$|\beta_{01}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$$
$$|\beta_{10}\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$$
$$|\beta_{11}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$$

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

確認

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

左辺を展開 $\quad |\psi\rangle_V|\beta_{00}\rangle_{AB} = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

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

右辺を各項ごとに展開

$$|\beta_{00}\rangle_{VA}|\psi\rangle_B = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \frac{\alpha}{\sqrt{2}}|000\rangle + \cancel{\frac{\beta}{\sqrt{2}}|001\rangle} + \cancel{\frac{\alpha}{\sqrt{2}}|110\rangle} + \frac{\beta}{\sqrt{2}}|111\rangle$$

$$|\beta_{10}\rangle_{VA}Z|\psi\rangle_B = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes (\alpha|0\rangle - \beta|1\rangle) = \frac{\alpha}{\sqrt{2}}|000\rangle - \cancel{\frac{\beta}{\sqrt{2}}|001\rangle} - \cancel{\frac{\alpha}{\sqrt{2}}|110\rangle} + \frac{\beta}{\sqrt{2}}|111\rangle$$

$$|\beta_{01}\rangle_{VA}X|\psi\rangle_B = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \otimes (\alpha|1\rangle + \beta|0\rangle) = \frac{\alpha}{\sqrt{2}}|011\rangle + \cancel{\frac{\beta}{\sqrt{2}}|010\rangle} + \cancel{\frac{\alpha}{\sqrt{2}}|101\rangle} + \frac{\beta}{\sqrt{2}}|100\rangle$$

$$|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \otimes (\alpha|1\rangle - \beta|0\rangle) = \frac{\alpha}{\sqrt{2}}|011\rangle - \cancel{\frac{\beta}{\sqrt{2}}|010\rangle} - \cancel{\frac{\alpha}{\sqrt{2}}|101\rangle} + \frac{\beta}{\sqrt{2}}|100\rangle$$

QTの実行

Step.1 状態の準備

$$|\psi\rangle_V|\beta_{00}\rangle_{AB} = \frac{1}{2}|\beta_{00}\rangle_{VA}|\psi\rangle_B + \frac{1}{2}|\beta_{10}\rangle_{VA}Z|\psi\rangle_B + \boxed{\frac{1}{2}|\beta_{01}\rangle_{VA}X|\psi\rangle_B} + \frac{1}{2}|\beta_{11}\rangle_{VA}XZ|\psi\rangle_B$$

Step.2 AliceによるBell測定(Bell基底による測定)

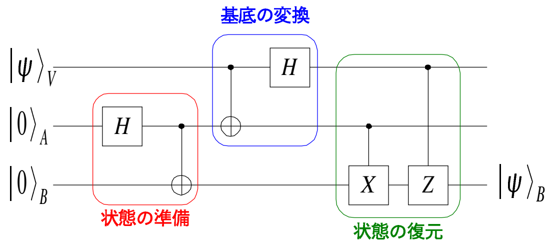
例えば $|\beta_{01}\rangle$ を得たとする．この時点でBobの状態は $X|\psi\rangle_B$ に確定
しかし，まだBobはそのことを知らないし，測定もしていないので
Bobの状態は壊れていない．

Step.3 古典チャンネルによるBell測定結果の伝達

Step.4 Bobによる状態の復元

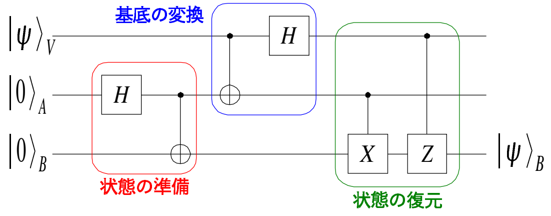
BobはAliceから得た情報を元に，自分の状態にPauli-X ゲートを施す．
Bobの状態は $X(X|\psi\rangle_B) = |\psi\rangle_B$ となり，テレポーテーション完了

QTを量子回路で考える



$$|\psi\rangle|0\rangle|0\rangle \xrightarrow{H_A} |\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \xrightarrow{C_{AB}} |\psi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$= (|00\rangle + |11\rangle)/\sqrt{2} \otimes |\psi\rangle$$
$$+ (|00\rangle - |11\rangle)/\sqrt{2} \otimes Z|\psi\rangle$$
$$+ (|01\rangle + |10\rangle)/\sqrt{2} \otimes X|\psi\rangle$$
$$+ (|01\rangle - |10\rangle)/\sqrt{2} \otimes XZ|\psi\rangle$$

QTを量子回路で考える(続き)



$$\begin{array}{c}(|00\rangle+|11\rangle)/\sqrt{2}\otimes|\psi\rangle+\\(|00\rangle-|11\rangle)/\sqrt{2}\otimes Z|\psi\rangle+\\(|01\rangle+|10\rangle)/\sqrt{2}\otimes X|\psi\rangle+\\(|01\rangle-|10\rangle)/\sqrt{2}\otimes XZ|\psi\rangle\end{array} \xrightarrow{C_{VA}} \begin{array}{c}(|00\rangle+|10\rangle)/\sqrt{2}\otimes|\psi\rangle+\\(|00\rangle-|10\rangle)/\sqrt{2}\otimes Z|\psi\rangle+\\(|01\rangle+|11\rangle)/\sqrt{2}\otimes X|\psi\rangle+\\(|01\rangle-|11\rangle)/\sqrt{2}\otimes XZ|\psi\rangle\end{array} \xrightarrow{H_V} \begin{array}{c}|00\rangle\otimes|\psi\rangle+\\|10\rangle\otimes Z|\psi\rangle+\\|01\rangle\otimes X|\psi\rangle+\\|11\rangle\otimes XZ|\psi\rangle\end{array}$$

$$\xrightarrow{CX_{AB}} \begin{array}{c}|00\rangle\otimes|\psi\rangle+\\|10\rangle\otimes Z|\psi\rangle+\\|01\rangle\otimes|\psi\rangle+\\|11\rangle\otimes Z|\psi\rangle\end{array} \xrightarrow{CZ_{AB}} (|00\rangle+|10\rangle+|01\rangle+|11\rangle)\otimes|\psi\rangle$$

測定と古典チャンネル

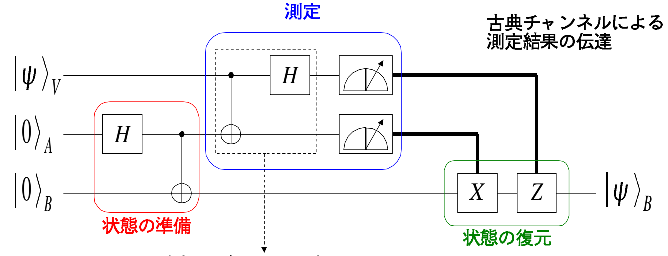
先に測定をしてしまって，必要なゲート操作だけを行っても問題ない

測定

$$\boxed{|00\rangle}\otimes|\psi\rangle+\boxed{|10\rangle}\otimes Z|\psi\rangle+\boxed{|01\rangle}\otimes X|\psi\rangle+\boxed{|11\rangle}\otimes XZ|\psi\rangle$$

復元

$$\xrightarrow{I}|\psi\rangle \qquad \xrightarrow{Z}|\psi\rangle \qquad \xrightarrow{X}|\psi\rangle \qquad \xrightarrow{ZX}|\psi\rangle$$



Bell測定が許される場合は不要．

$|\beta_{xy}\rangle$ arrow $|xy\rangle$ と対応させればよい

Wrap-Up

- Quantum Key Distribution provides "tamper-evident" packaging for your keys
- Quantum teleportation can be used to move a superposition from one place to another

References

- Elliott, "Quantum cryptography in practice," SIGCOMM 2003