Interplay between Quantum Computation and Quantum Information

Akihisa Tomita

Quantum Computation and Information Project, ERATO-SORST, JST
Graduate School of Information Science and Technology, Hokkaido University
Contents

• Introduction
  – Fundamental concepts of quantum information processing
  – Quantum Computation Science, Quantum Information Science, and Physics
  – ERATO-SORST Project and Quantum Networks

• Quantum $k$-Merlin Arthur Game

• Quantum Leader Election
  – algorithm
  – implementation

• Quantum key distribution

• Conclusion
Fundamental concepts of Computer Science and Information Science

This figure is taken from the text book “Quantum Computation and Quantum Information” by M.A. Nielsen & I. Chuang (Cambridge Univ. Press)
Quantum State (qubit)

- A vector in 2-dim Hilbert space

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \text{where} \quad |\alpha|^2 + |\beta|^2 = 1 \]

\[ |\psi\rangle = \cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle \]

- Implementation by photon
  - Polarization
  - Relative phase
  - vacuum/one photon
  - and more

Bloch sphere
Mixed States

- an ensemble of pure quantum states denoted by classical probability distribution $p_i$ taking state $|\psi_i\rangle$
- described with a density operator $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i |$
  - eigen values $\rho \geq 0$ ; Tr $\rho$ = 1
- Reduced density operator $\rho^A = \text{Tr}_B (\rho^{AB})$
  - If $\rho^{AB} = \rho \otimes \sigma$, then $\rho^A = \text{Tr}_B (\rho \otimes \sigma) = \rho$
Quantum gates

- **quantum gates** = Unitary trans.
  - single qubit gates = $2 \times 2$ Unitary matrices
  - Any $2 \times 2$ unitary matrices can be approximated with three matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad i\sigma_y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$i\sigma_y = \sigma_z \sigma_x$$

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\sigma_z : |0\rangle \rightarrow |0\rangle, |1\rangle \rightarrow -|1\rangle$$
$$\sigma_x : |0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$$
$$\sigma_y : |0\rangle \rightarrow i|1\rangle, |1\rangle \rightarrow -i|0\rangle$$

NOT
Two-qubit gate (ex. CNOT)

\[ \frac{1}{\sqrt{2}} \left( |0\rangle + |1\rangle \right) \]

C-unitary gates, in general

\[ \frac{1}{\sqrt{2}} \left( |00\rangle + |11\rangle \right) \]

\[
\begin{array}{cccc}
|0\rangle_C |0\rangle_T & \rightarrow & |0\rangle_C |0\rangle_T \\
|0\rangle_C |1\rangle_T & \rightarrow & |0\rangle_C |1\rangle_T \\
|1\rangle_C |0\rangle_T & \rightarrow & |1\rangle_C |1\rangle_T \\
|1\rangle_C |1\rangle_T & \rightarrow & |1\rangle_C |0\rangle_T \\
\end{array}
\]

NOT op. only when C=1

C-Unitary gate + single qubit gates = universal
Quantumness relevant to information processing

• Superposition
  – Quantum parallelism
  – No cloning

• Entanglement (inseparability)
  – State control
  – Monogamy

• Measurement
  – State collapse; projection
Quantum Computation

$2^N$ states

$|0\rangle + |1\rangle |0\rangle + |1\rangle |0\rangle + |1\rangle$

$|\psi\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$

$= \frac{1}{\sqrt{8}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$

Superposition
Quantum parallelism

$\psi$

interference
entanglement

solution extraction
(amplifying state amplitude)

Quantum Fourier Transform

ex: $f(x_1), f(x_2), \ldots, f(x_8)$
Quantum Information

Mission impossible: to distinguish two states with a single measurement

• classical states = possible
• orthogonal states = possible
• non-orthogonal states = impossible

If you had many copies, it would be possible without a trace disturbance upper bound of information

error free 50% error

accept! reject!
How close are the two states?

• Pure states $|\psi\rangle$ and $|\phi\rangle$:
  – Fidelity $F = |\langle \psi | \phi \rangle|^2$

• Mixed states $\rho$ and $\sigma$:

$$F = \max |\langle \phi_\rho | \phi_\sigma \rangle|^2 = \left( \text{Tr} \sqrt{\sqrt{\sigma} \rho \sqrt{\sigma}} \right)^2$$

• Properties
  – $F=1$ for identical states
  – $F=0$ for perfectly distinguishable states
  – $F(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2) = F(\rho_1, \sigma_1)F(\rho_2, \sigma_2)$
  – $F(\rho, \sigma)^2 + F(\sigma, \xi)^2 = 1 + F(\rho, \xi)$
Entanglement

• non-local (quantum mechanical) correlation

Measurement results of two remote particles, which interacted in the past, yield a correlation, though no interaction is applied between two.
Entanglement (cont.)

- **Correlation**
  - entanglement assisted communication
  - exponential speed up (?)
  - quantum game (pseudo-telepathy); multi-prover interactive poof

- **monogamy**
  - quantum cryptography

- **decoherence**
  - information-disturbance trade-off; error correction
Entangled state

- **Separable states**
  \[ |\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi'\rangle_B; \rho_{AB} = \rho_A \otimes \rho_B \]
  - ex. \[ |1\rangle_A |0\rangle_B \]

- **Entangled states**
  - not described by a tensor product
  - Bell states
    \[ \frac{1}{\sqrt{2}} \left( |0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B \right); \frac{1}{\sqrt{2}} \left( |0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B \right) \]
  - GHZ state
    \[ \frac{|00\cdots0\rangle + |11\cdots1\rangle}{\sqrt{2}} \]
  - W state
    \[ \frac{|0\cdots01\rangle + |0\cdots010\rangle + \cdots |010\cdots0\rangle + |10\cdots0\rangle}{\sqrt{N}} \]

- **Partial trace of a pure state**
  - separable: pure
  - entangled: mixed

**deg. of entanglement:** \( S(\text{Tr}_B(|\varphi\rangle\langle\varphi|)) \)
The two cultures: 
Computer Science and Information Science

This figure is taken from the text book “Quantum Computation and Quantum Information” by M.A. Nielsen & I. Chuang (Cambridge Univ. Press)
The three cultures: CS, IS, and Physics

• “They are playing their own games, which are almost independent of physics, once the rules are established. We still have to consider physical systems (It’s annoying…”

• “They cannot treat things rigorously, and tend to jump to unreasonable conclusions, so that we have to direct them.”

• “They made a useful theory, only after we taught them what really matters.”
• Designed to promote cooperation between QCS, QIS, and Physics (theory & experiment)

• Five (3+2) year Project; the successor of ERATO Quantum Computation and Information Project (2000.10-2005.10) headed by Prof. Imai (Univ. Tokyo)
Challenges in IT and Quantum Solution

Cryptography

(1) Menace to conventional crypto with innovating technology
(2) Increasing demand for secure network
  - Government, Defense
  - Electronic Commerce
  - Medical, genome, biometrical, etc.

Quantum Cryptography
unconditionally, provable security

Computation

(1) Fundamental limit in computers
  - supercomputers
  - limit in nano-lithography
    - power
    - physical limit in FETs
(2) Ultra-high speed computing
  - climate, molecular design (pharmacy),...
  - drive innovation

Quantum ICT network

- government
- academic
- business
- medical
- quantum distributed computing

Ex. designing protein structure

Quantum Computers
quantum parallelism

65TFLOPS → PFLOPS
Safe and Secure Society by Quantum Network

- e-commerce
- Access
- e-voting
- Quantum Protocol
- Government
- Data Storage
- Data Processing
- Ultra-fast
- Masquerade Detection
Quantum Network

**Application layer**
- distributed computing
- cryptography

**Communication layer**
- channel capacity
- coding theory
- network theory

**Physical layer**
- implementation
- state preparation/measurement
- devices (memory, gate, ..........)

Quantum Computing Gr.
Quantum Information Theory Gr.
Quantum Information Experiment Gr.
Application layer

• Algorithm
  – distributed computation
  – complexity

• Protocols
  – non-cryptographic
    • Quantum Leader Election
  – cryptographic
    • Pseudo-telepathy Game
    • Quantum Key Distribution
    • Computational Cryptography
    • Interactive Proof
Application

- Algorithm
  - distributed computation
  - complexity
- Protocols
  - non-cryptographic
- Quantum Leader Election
- Cryptographic
- Interactive Proof
- Game

An Improved Claw Finding Algorithm Using Quantum Walk
Optimal Claw Finding Algorithm Using Quantum Walk
Quantum Property Testing of Group Solvability
Computational Geometry Analysis of Quantum State Space and Its Applications

Exponential Separation of Quantum and Classical Online Space Complexity
Quantum Weakly Nondeterministic Communication Complexity
The One-Way Communication Complexity of Group Membership
The quantum query complexity of certification

Exact Quantum Algorithms for the Leader Election Problem
Generating facets for the cut polytope of a graph by triangular elimination
Bell inequalities stronger than the Clauser-Horne-Shimony-Holt inequality for three-level isotropic states
On the Relationship between Convex Bodies Related to Correlation Experiments with Dichotomic Observables

Oracularization and Two-Prover One-Round Interactive Proofs against Nonlocal Strategies
Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?
Quantum Communication Between Anonymous Sender and Anonymous Receiver in Presence of Strong Adversary
Quantum Non-local Boxes and their Use in Computer Security

Practical Evaluation of Security for Quantum Key Distribution
Upper bounds of eavesdropper's performances in finite-length code with the decoy method
General theory for decoy-state quantum key distribution with arbitrary number of intensities
Security Analysis of Decoy State Quantum Key Distribution Incorporating Finite Statistics
Communication layer

• Quantum network architecture
  – entanglement, robustness, routing

• Quantum coding
  – channel capacity
    • quantum/classical, entanglement assisted, …
  – QECC

• network coding

• Entanglement theory
Communication layer

- Quantum network architecture
  - entanglement, robustness, routing
- Quantum coding
  - channel capacity
  - quantum/classical, entanglement assisted, ... 
  - QECC, network coding
- Entanglement theory
  - Additivity and multiplicativity properties of some Gaussian channels for Gaussian inputs
  - Monogamy inequality for multipartite distributed Gaussian entanglement
  - Universal distortion-free entanglement concentration
  - Statistical analysis of testing of an entangled state based on the Poisson distribution framework
  - Irreversibility of entanglement loss
- On the minimum number of unitaries needed to describe a random-unitary channel
- Superbroadcasting and classical information
- Optimal Visible Compression Rate For Mixed States Is Determined By Entanglement Purification
- Properties of Conjugate Channels with Applications to Additivity and Multiplicativity
- Public and private communication with a quantum channel and a secret key

- Information-Disturbance Tradeoff in Quantum State Discrimination
  - A minimum-disturbing quantum state discriminator
  - Quantum Erasure of Decoherence
  - Entanglement measures and approximate quantum error correction
  - Global information balance in quantum measurements
  - Information extraction versus irreversibility in quantum measurement processes
  - Towards a unified approach to information-disturbance tradeoffs in quantum measurements

- (4,1)-Quantum Random Access Coding Does Not Exist--One qubit is not enough to recover one of four bits
- Prior entanglement between senders enables perfect quantum network coding with modification
- General Scheme for Perfect Quantum Network Coding with Free Classical Communication
Physical layer

• System
  – QKD

• Circuits over a network

• Entanglement generation/distribution

• Implementation
  – qubit/qudit
  – gate, memory
  – interface
Physical layer

- System
  - QKD
- Circuits over a network
- Entanglement generation/distribution
- Implementation
  - qubit/qudit
  - gate, memory
  - interface

• Practical quantum cryptosystem for metro area applications
• Experimental Decoy State Quantum Key Distribution with Unconditional Security incorporating Finite Statistics
• Ultra fast quantum key distribution over a 97-km installed telecom fibre with wavelength-division multiplexing clock synchronization
• Ensuring Quality of Shared Keys through Quantum Key Distribution for Practical Application
• High speed quantum key distribution system
• Quantum Key Distribution Over 50km with High-Performance Quantum dot Single Photon Source at 1.5-µm Wavelength
• Technologies for Quantum Key Distribution Networks Integrated With Optical Communication Networks

• Experimental demonstration of quantum leader election in linear optics
• Measurement of the off-diagonal geometric phase of a mixed-state photon via a Franson interferometer
• Asymptotic Quantum teleportation to enable universal quantum processor
• Quantum teleportation scheme by selecting one of multiple output ports

Generation/distribution

• Generation of Polarization-entangled Photom Pairs Using Periodically Poled Lithium Niobate Waveguides in a Fiver Loop
• Highly efficient polarization entangled-photon source from Periodically Poled Lithium Niobate waveguides
• Efficient generation of a photon pair in a bulk periodically poled potassium titanyl phosphate
• Efficient Photon Pair Generation Using Two-wavelength Spontaneous Parametric Down-conversion Module
• Performance of hybrid entanglement photon pair source for quantum key distribution
Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?*

Hirotada Kobayashi\textsuperscript{a,b,†} Keiji Matsumoto\textsuperscript{a,b,‡} Tomoyuki Yamakami\textsuperscript{c,§}
hirotada@nii.ac.jp keiji@nii.ac.jp yamakami@u-fukui.ac.jp

\textsuperscript{a}Principles of Informatics Research Division
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

\textsuperscript{b}Quantum Computation and Information Project
Solution Oriented Research for Science and Technology
Japan Science and Technology Agency
5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan

\textsuperscript{c}Department of Information Science
Graduate School of Engineering
University of Fukui
3-9-1 Bunkyo, Fukui City, Fukui 910-8507, Japan

Abstract

This paper introduces quantum “multiple-Merlin”-Arthur proof systems in which Arthur receives multiple quantum proofs that are unentangled with each other. Although classical multi-proof systems are obviously equivalent to classical single-proof systems (i.e., standard Merlin-Arthur proof systems), it is unclear whether or not quantum multi-proof systems collapse to quantum single-proof systems (i.e., standard quantum Merlin-Arthur proof systems). This paper presents a way of reducing the number of proofs to two while keeping the two-sided bounded-error property, which gives a necessary and sufficient condition under which the number of quantum proofs is reducible to two. It is also proved that, in the case of perfect soundness, using multiple quantum proofs does not increase the power of quantum Merlin-Arthur proof systems.
(Quantum) Interactive Proof System

- {Yes, No} question
- Prover: always tells “Answer is Yes.”
  - any Unitary operation allowed
- Verifier: checks P’s assertion with high probability through communication
  - quantum polynomial time computation

- Related to many problems:
  - Cryptography
  - Inapproximability of certain optimization problems (e.g. max-3sat, creek, etc)
  - Locally decodable/testable code
Quantum Merlin-Arthur Game

- Merlin sends a quantum proof.
- Characteristics:
  - Completeness: The verifier accepts a proof with probability at least $c$, if the answer is “Yes.”
  - Soundness: The verifier rejects any proofs with probability at least $1-s$, if the answer is “No.”
- It is interesting for physicists that calculating the ground state energy of a many body system is QMA.

Given Hamiltonian $\mathcal{H}$, Promise: $E_g(\mathcal{H}) < a$ or $E_g(\mathcal{H}) > b$ and Merlin says “$E_g(\mathcal{H}) < a$”!

accuracy $> 1/poly(N)$
Multiple-Merlin; QMA(k)

- Arthur receives $k$ quantum proofs.
- KMY shows $\text{QMA}(k) = \text{QMA}(2)$
  - iff ‘For any two-sided bounded error completeness-
soundness pair $(c, s)$, $\text{QMA}(2, c, s) = \text{QMA}(2, 2/3, 1/3)$’
- Aaronson, Beigi, Drucker, et al. (*) shows that the
  Additivity Conjecture implies that
  $\text{QMA}(k) = \text{QMA}(2)$, etc.

\[ f(X \otimes Y) = f(X) + f(Y) \, ? \]

(*) *Theory of Computing*, 5:1-42 (article 1) 2009
KMY ~ main result

• For any $k \in \text{poly}$ and any two-sided bounded error completeness-soundness pair $(c,s)[*]$, $QMA(k,c,s) \subseteq QMA(2,1-2^{-q},1-1/p)$ $p,q \in \text{poly}$

[*] $c-s \in \text{poly}^{-1}$ and $2^{-q} \leq s < c \leq 1-2^{-q}$

poly: set of all polynomially bounded function

• Proof: Applies Technique from Quantum Information

  – Construct 2-proof system for 3-proof system by 
    $(R_1,S_1)$ and $(R_2,S_2)$ expecting $
    |\psi_1\rangle = |\phi_1\rangle \otimes |\phi_3\rangle; |\psi_2\rangle = |\phi_2\rangle \otimes |\phi_3\rangle$

    and separability test & simulation test

  – $QMA(3,1-\varepsilon,1-\delta) \subseteq QMA(2,1-\varepsilon/2,1-\delta/20)$

  – $QMA(3k+r,1-\varepsilon,1-\delta) \subseteq QMA(2k+r,1-\varepsilon/2,1-\delta/20)$
Tests in two-proof system

• **Separability test** (control swap test)
  – Expecting $|\psi_1\rangle = |\phi_1\rangle \otimes |\phi_3\rangle; |\psi_2\rangle = |\phi_2\rangle \otimes |\phi_3\rangle$
  but $R_1$ and $S_1$ (or $R_2$ and $S_2$) may be entangled
  Test on $\rho = \text{Tr}_{R_1} |\psi'_1\rangle \langle \psi'_1|; \sigma = \text{Tr}_{R_2} |\psi'_2\rangle \langle \psi'_2|$, where $p_{sep} = (1 + \text{Tr}(\rho \sigma))/2$, and $\rho = \sigma$ if $R, S$ separable.

• **Simulation test**
  – will simulate the original verifier, if entanglement is small (pass the separability test)
  – Apply $V(x)$ to $(V, R_1, R_2, S_1)$.
  – $p_{sim}$ is given by **Fidelity** between the state to be tested $|\alpha\rangle$ and its projection $|\beta\rangle$ onto the accepting states:
    $$p_{sim} = F(V^+ |\beta\rangle \langle \beta| V, |\alpha\rangle \langle \alpha|)^2$$
  – $\text{Tr}(\rho \sigma) (> 1 - \delta/5)$ provides the bound to the fidelity and then desired soundness
Anonymous leader election

Select one leader from identical computers

- Classical
  - coin toss
  - finite probability of “even”
  - unsolved with finite communication

- Quantum
  - quantum communication
  - no probability of “even”
  - solved with finite communication
It is easy using pre-shared entanglement

• Suppose W state is shared by $N$-party.

\[ \left( |0\ldots01\rangle + |0\ldots010\rangle + \ldots |010\ldots0\rangle + |10\ldots0\rangle \right) / \sqrt{N} \]

• After measurement, the state is collapsed to one of $|0\ldots01\rangle, |0\ldots010\rangle, \ldots, |010\ldots0\rangle, |10\ldots0\rangle$

QLE (algorithm I)

\[
\begin{array}{cccc}
\text{status} & R0 & R1 & S \\
1 & 0\rangle + |1\rangle & 0 & |C\rangle \\
0 & |0\rangle & |0\rangle & |C\rangle \\
\end{array}
\]

\[k=n\]

* set

\[|\Psi\rangle\rightarrow |0\rangle\rightarrow |C\rangle\]

\[
\begin{array}{cccc}
\text{call SUB A} \\
\text{call SUB B} \\
superposition \\
\text{measure S} \\
\text{S}=C \& \text{status}=1 \\
\text{measure R0,R1} \\
\end{array}
\]

call SUB C

\[z=z_{\text{max}}\]

no

\[k=k-1\]

go to *

no

z

yes

put 0

\[k=2\]

until

\[S. Tani, H. Kobayashi, and K. Matsumoto , LNCS 3404, pp.581-592,2005\]
Two party QLE

• initial state: 
\[
\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)
\]

• SUB A
  – “copy” R0: 
  \[
  \left(\frac{|0\rangle_h |0\rangle_g + |1\rangle_h |1\rangle_g}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle_h |0\rangle_g + |1\rangle_h |1\rangle_g}{\sqrt{2}}\right)
  \]
  – quantum communication:
  \[
  |0\rangle_{1h} |0\rangle_{1g} |0\rangle_{2h} |0\rangle_{2g} + |1\rangle |0\rangle |1\rangle |0\rangle + |0\rangle |1\rangle |0\rangle + |1\rangle |1\rangle |1\rangle |1\rangle
  \]
  – inverse “copy”:
  \[
  S^2 \begin{pmatrix}
  |0\rangle_{1h} |0\rangle_{2h} + |1\rangle_{1h} |1\rangle_{2h} |0\rangle_{1g} |0\rangle_{2g} + |1\rangle_{1h} |0\rangle_{2h} + |0\rangle_{1h} |1\rangle_{2h} & |1\rangle_{1g} |1\rangle_{2g}
  \end{pmatrix}
  \]

• SUB B: erase amplitude of \(|0\rangle |0\rangle; |1\rangle |1\rangle\)
  – apply \(U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}\), if \(g=0\),
  \[
  \frac{|1\rangle_{1h} |0\rangle_{2h} + |0\rangle_{1h} |1\rangle_{2h}}{\sqrt{2}}
  \]
Quantum circuit for two-party QLE

Entangling feed forward

Q: So, how can we implement the circuit? – A: Photonics!
Quantum Information with photons

- pro & con -

• Good for Transmission (and Proof of Principle)
  – Low Loss Channel (fiber)
  – Weak Decoherence
  – Qubits by polarization, phase,…
  – Single Qubit Operation

• Bad for Processing
  – Weak Interaction
    ▶ Hard to make a Controlled-gate
  – NO Amplifiers
Single qubit gate for polarization

- **Waveplate**: birefringence
  - **HWP**: \[
  \begin{pmatrix}
  1 & 0 \\
  0 & -1
  \end{pmatrix}
  \]
  - **QWP**: \[
  \begin{pmatrix}
  1 & 0 \\
  0 & i
  \end{pmatrix}
  \]

- **Appropriate alignment of optical axes**
  - Any single qubit operation

\[
\begin{pmatrix}
  \cos\theta & -\sin\theta \\
  \sin\theta & \cos\theta
\end{pmatrix}
\begin{pmatrix}
  1 & 0 \\
  0 & -1
\end{pmatrix}
\begin{pmatrix}
  \cos\theta & \sin\theta \\
  -\sin\theta & \cos\theta
\end{pmatrix}
= \begin{pmatrix}
  \cos2\theta & \sin2\theta \\
  \sin2\theta & -\cos2\theta
\end{pmatrix}
\]

\[
\begin{pmatrix}
  \cos\theta & -\sin\theta \\
  \sin\theta & \cos\theta
\end{pmatrix}
\begin{pmatrix}
  1 & 0 \\
  0 & i
\end{pmatrix}
\begin{pmatrix}
  \cos\theta & \sin\theta \\
  -\sin\theta & \cos\theta
\end{pmatrix}
= \begin{pmatrix}
  \cos^2\theta + i\sin^2\theta & (1-i)\cos\theta\sin\theta \\
  (1-i)\cos\theta\sin\theta & i\cos^2\theta + \sin^2\theta
\end{pmatrix}
\]
Two-qubit gates

• Gate implementation with linear optics

entangler (photon number basis)

\[ |0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle|1\rangle + |1\rangle|0\rangle) \]

probabilistic CNOT (polarization basis)

Success Fail
C-NOT construction

\[ \phi^+ \]

control

\[ H \]

parity check

output

Prob. 1/4
w. feed forward

Polarization entangled photon generation by type I crystal

- **Spontaneous Parametric Down Conversion (SPDC)**
  - Nonlinear Crystal
  - \( (\omega_p, \vec{k}_p) \)
  - \( (\omega_i, \vec{k}_i) \)
  - \( (\omega_s, \vec{k}_s) \)

- **Two-crystal geometry**

\[ \omega_p = \omega_s + \omega_i \]
\[ \vec{k}_p = \vec{k}_s + \vec{k}_i \]
\[ \omega = \frac{ck}{n(\omega, \vec{k}/|\vec{k}|, \vec{e})} \]

No Which crystal information superposition = entanglement

\[ \frac{1}{\sqrt{2}} (|HH\rangle + |VV\rangle) \]
Entanglement in fiber-optics
Two color, hybrid entanglement

Alice

Z0 (X0)

PBS

λ/2

0°

(22.5°)

Z1 (X1)

OR

Bob

2.5ns

1550nm

2x4 PLC

Delay controller

Pulse generator

Photon-pair module

SMF

CW 532nm

2.5ns

X0

X1

Z0

Z1

time-polarization transformer

Lens

20 cm

H

V

Lens

2x4

PLC

λ/2

Trigger delay [ns]

C.C. [c/10s]

Visibility

X basis (D,A & phase)
Vis. 88%, 950c/s

Z basis (H,V & time)
Error 2.1%, 820c/s

PLC temp [℃]

delay length [mm]
Quantum circuit for two-party QLE

entangling

quantum comm.

feed forward

$|0\rangle_{\text{host}}$  H  $|0\rangle_{\text{guest}}$

Alice

$|0\rangle_{\text{guest}}$  U  $|0\rangle_{\text{host}}$

Bob

$|0\rangle_{\text{host}}$  H  $|0\rangle_{\text{guest}}$
Polarization-qubit implementation

entangled photon source

quantum comm.

feed forward

$|HH\rangle + |VV\rangle \over \sqrt{2}$

$|HH\rangle + |VV\rangle \over \sqrt{2}$

Alice

Bob

host

guest

guest

host
Polarization-qubit implementation

1. A, B create entangled photons
2. exchange one
3. PBS: H (1 to 3, 2 to 4), V (1 to 4, 2 to 3)
4. Hadamard (wave plate) to 4
5. measure 4, the outcome:
   (A, B) = {(H, H), (V, V), (H, V), (V, H),
            (0, HH), (0, VV), (HH, 0), (VV, 0)}
   the projected state
   \[
   \frac{1}{\sqrt{2}} (|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B ) \quad (H, H), (V, V)
   \frac{1}{\sqrt{2}} (|H\rangle_A |H\rangle_B - |V\rangle_A |V\rangle_B ) \quad (H, V), (V, H)
   \]
6. apply Unitary to 3 and measure

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}
\]
Photon number based implementation

1. entangling

2. quantum commun.

3. phase gate

4. measurement

State after phase gates

\[
\left( \frac{|0\rangle_h |1\rangle_g + |1\rangle_h |0\rangle_g}{\sqrt{2}} \right)_A \otimes \left( \frac{|0\rangle_h |1\rangle_g + |1\rangle_h |0\rangle_g}{\sqrt{2}} \right)_B
\]

\[
\rightarrow \left[ \begin{array}{cc}
\Psi^+ \rangle_A & \Psi^- \rangle_A \\
\Psi^- \rangle_B & \Psi^+ \rangle_B 
\end{array} \right]
\]

\[
+ \frac{1}{2} \left[ \begin{array}{cc}
|1\rangle_h |1\rangle_g \rangle_A |0\rangle_h |0\rangle_g \rangle_B \\
+ |0\rangle_h |0\rangle_g \rangle_A |1\rangle_h |1\rangle_g \rangle_B 
\end{array} \right]
\]

Distinguishable states appear from product of identical state
QLE is always successful, by defining the winner as \(|\Psi^+\rangle\) and \(|11\rangle\)
Measurement

\[
\left[ |\Psi^+\rangle_A |\Psi^-\rangle_B + |\Psi^-\rangle_A |\Psi^+\rangle_B \right] + \frac{1}{2} \left[ |1h1g\rangle_A |0h0g\rangle_B + |0h0g\rangle_A |1h1g\rangle_B \right]
\]

distinguishable

detection after two photon interference

input $|\Psi^+\rangle_A |\Psi^-\rangle_B$

Alice and Bob yield different detection pattern

A is leader

click A1, B2

detectors: A1 A2 B1 B2
**Expected Result**  
*(success with prob. 1)*

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
<th>Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>A2</td>
<td>B1</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

- **failure in usual setting**
- **one photon to each port**
- **two to one port**
Symmetric configuration
Two-photon interferometers

Experimental set-up

SPDC
pump pulse
(404 nm)

PMF

BBO

IF

S

H

G

Mode locked Ti:S

PZT

π/2

Bob

Alice

Two-photon interferometers

Symmetric configuration
### Result

#### Observed (Counts)

<table>
<thead>
<tr>
<th>A1</th>
<th>A2</th>
<th>B1</th>
<th>B2</th>
<th>Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>Alice</td>
</tr>
<tr>
<td>-</td>
<td>1</td>
<td>1</td>
<td>-</td>
<td>Bob</td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Alice</td>
</tr>
<tr>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>Alice</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>Bob</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>Bob</td>
</tr>
</tbody>
</table>

#### Theory

- $\frac{1}{4}$
- $\frac{1}{8}$
Two photon interference

\[ \nu \approx 0.83 < 1 \]

Piezo-Voltage (\(\sim\)Phase Difference)
\[ P_2 = \frac{1}{2} \]
\[ P_1 = \frac{1 + \nu}{4} \]
\[ P_f = \frac{1 - \nu}{4} \]

two photons detected
\[ P_{success} = \frac{3 + \nu}{4} \rightarrow 95.7\% \]

one photon each
Communication complexity in classical protocol

![Diagram showing a classical protocol between Alice and Bob]

- **Alice** and **Bob** exchange **2 bits**.
- **Expectation value of communication bits to success:**
- **Failure:** 50%

\[
\langle N^{\text{classical}} \rangle = \sum_{n=1}^{\infty} \frac{n}{2^{n-1}} = 4
\]
Communication complexity of QLE (with imperfect apparatus)

exchange guest qubits (QC)

2 bits

one photon each?

success (finish)

two photon detected
= protocol succeeded
= no CC required

2 bits in total

2 bits CC required to verify the results between Alice and Bob
Leader!!

4 bits in total

Leader!

Leader!

failure (try again!)
Communication complexity of QLE (with imperfect apparatus) cont.

\[
\langle N^{\text{quantum}} \rangle = \text{prob. to success at } k\text{-th round}
\]

\[
= \sum_{k=1}^{\infty} \left[ (4(k-1) + 2) \cdot \frac{1}{2} Q^{k-1} + (4(k-1) + 4) \cdot \frac{1 + \nu}{4} Q^{k-1} \right]
\]

\[
< N > \approx 3.13
\]

\[
< 4 = < N^{\text{classical}} >
\]
What’s interesting?

• Leader Election:
  – Create asymmetric states from a symmetric state only with symmetric operations.
  – Impossible! (as in classical protocols)
    So in quantum. But, because of non-locality in quantum state (entanglement), appropriate cut yields effective asymmetry.

• as a Practical photonic implementation
  – Appropriate definition on success events result in deterministic operation with linear optics
  – even loss helps the successful leader election!
Quantum Computing

Quantum Information

ex. 1: QMA

ex. 2: QLE

experiment

ex. 3: QKD
Secure key distribution with quantum communication

Application

Decoding

Privacy amp.

error correction

transmission

Coding

TX

RX

secure key

erase leakage info

common random numbers

key

estimate leakage information

Quant. Comm.

ex. 3

Alice

Bob

Eve
Assumptions on BB84 protocol

<table>
<thead>
<tr>
<th>ideal</th>
<th>practical</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. single photon source</td>
<td>1. weak coherent light</td>
</tr>
<tr>
<td>– one photon for one bit</td>
<td>– 0,1,2,.. photons for one bit</td>
</tr>
<tr>
<td>2. infinite computational resource</td>
<td>2. finite memory capacity, execution time</td>
</tr>
<tr>
<td>– infinite code length</td>
<td>– finite code length</td>
</tr>
<tr>
<td>(asymptotic)</td>
<td>– finite code length</td>
</tr>
<tr>
<td>3. infinite code length, infinite time to measure</td>
<td>3. finite code length, finite time</td>
</tr>
<tr>
<td>– no estimation error</td>
<td>– sampling error</td>
</tr>
<tr>
<td>– no fluctuation</td>
<td>– fluctuation</td>
</tr>
</tbody>
</table>

Can we extract secure keys under the practical assumptions? Yes, with **decoy** method (Hwang, Wang, Lo, *et al* for 1 and Hayashi, *et al* for 2,3.)
Estimation of sacrifice bits

• Estimation of channel (Eve’s strategy) from the transmission date
  – decoy method: improving the estimation by increasing the number of constraints

• Errors in estimation
  – fluctuation of data (environment, equipment)
  – estimation error from finite number of data
  – sampling error in finite-length code

\[ 2^{-\delta} \]
QKD transmitter/receiver

- including laser, encoder, modulator
- error detecting modulation
- 625MHz & 1.25GHz clock

Transmitter (Alice)

\[
E_{out} = E_{in} \cos \left( \frac{\phi_1 - \phi_2}{2} \right) \cdot \exp \left( i \frac{\phi_1 + \phi_2}{2} \right)
\]

PLC (Planer Lightwave Circuit) enables stable operation without active control

This board is developed by NEC under the contracted research with NICT
PLC-Interferometer

Telecom wavelength(1.55µm)
Optical delay: 2.5/0.8/0.4 ns
Low loss ≤ 1dB
Negligible PDL
Polarization insensitive

Nonlinear optimization of discontinuous functions under constraint

Key generation time

- Present (~15s in total)
- Future

- Code length: $n$
- $O(1)$
- $O(n)$
- $O(n^2)$
- $O(n^2)$

- Smaller error
- Longer code
- Less fluctuation

- Random permutation
- Leakage information estimation
- PA
- EC
- Q.C.
Fast key distillation

• Hardware logic for key distillation
  – Function: sift, error correction, privacy amplification
  – Form factor: Advanced TCA (PICMIG 3.0 Advanced TCA Base Specification)
Key distillation board

This board is developed by NEC under the contracted research with NICT.
Conclusions

• Three examples on cooperation between CS, IS, and PS;
  – East is East, and West is West, but **Quantum is also Quantum**

• These cooperation will be more important for Quantum Networks (Quantum Distributed ***)
  – The studies will include
    • What possible,
    • How efficient,
    • How it works,
    • How to make, …
Members (current)

• Head: Hiroshi Imai
• Quantum Computation Group
  – Leader: K. Matsumoto
  – Researcher: J. Hasegawa
  – Student members:
    • N. Fu
    • R. Aoshima
    • T. Sato
• Quantum Information Theory Group
  – Leader: T. Hiroshima
  – Researcher: M.-H. Hsieh
  – Student members:
    • Vorepong Suppakitpaisarn
• Quantum Information Experiment Group
  – Leader: A. Tomita
  – Researcher: K. Tsujino
• Staffs
  – T. Nagatsu (admin.)
    • H. Yokota
  – A. Tomita (tech.)
    • H. Takeshima
Members (past)

- M. Amaike (admin)
- T. Yamakami (researcher)
- Y. Kikuchi (researcher)
- X.-B. Wang (researcher)
- T. Ohno (admin)
- C. Matsumoto (admin)
- M. Yasuda (admin)
- Y. Iuni (student)
- J. Nishitoba (student)
- M. Hayashi (group leader)
- M. Asada (student)
- Y.-K. Jiang (researcher)
- S. Nagaoka (student)
- F. Buscemi (researcher)
- Ku. Kojima (researcher)
- Y. Tokuda (student)
- Ko. Kojima (student)
- S. Tani (researcher)
- F. Le Gall (researcher)
- H. Kobayashi (researcher)
- Y. Okubo (student)
- K. Yoshizoe (researcher)
- J. Sprojcar (researcher)
- K.-Y. Cheong (researcher)
- M. Kimura (admin)
Members (ERATO)

- **Quantum Computing (Tokyo)**
  - K. Tadaki
  - M. Hachimori
  - F. Yura
  - H. Fan
  - W.-Y. Hwang
  - A. Carlini
  - Y. Tokunaga
  - T. Yamazaki
  - M. Toda
  - S. Moriyama
  - T. Kawakami
  - A. Miyake
  - T. Ito
  - Y. Sasaki
  - S. Tokumoto
  - T. Yamada
  - M. Owari

- **Quantum Information (Tsukuba & Tokyo)**
  - M. Hamada
  - B.-S. Shi
  - Y. Tuda
  - Achanta V. Gopal
  - K. Kazui
  - S. Natori

- **Quantum Circuit Programming (Kyoto)**
  - K. Iwama
  - S. Yamashita
  - T. Koshiba
  - H. Nishimura
  - Chelliah Pethuru Raj
  - A. Kawachi
  - M. Amano
  - Y. Iio
  - Rudy Raymond Harry Putra
  - A. Matsuura
  - K. Kobayashi
  - R. Nishimaki
  - Y. Murakami
  - T. Inoue

- **Admin**
  - Y. Umezawa
  - T. Sakuragi
  - M. Inagaki
  - E. Bandai
  - M. Ohyama (Kyoto)
Thank you!