

Two-Way QCP

Review

LM05 Protoc The Protocol Message Mode Control Mode

First Telecon Window

Experiment Incoherent Individu Attack Eavesdropping Simulation Imperfect Equipme

Third Telecom Window Phase Encoding

Summary



Bidirectional Quantum Channels Enter Quantum Security

Giovanni Di Giuseppe A. Ceré, R. Kumar, M. Lucamarini, S. Mancini and P. Tombesi

Quantum Optics & Quantum Information Group Department of Physics, University of Camerino

http://fisica.unicam.it/qog/



QUANTUM MECHANICS: FROM FUNDAMENTAL PROBLEMS TO APPLICATIONS Bertinoro (FC)- Italy. December 3rd - 8th, 2006



Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding
- Summary

1 Review

- LM05 Protoco
- The Protocol
- Message Mode
- Control Mode

First Telecom Window

- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation
 Imperfect Equipment
- Third Telecom Window
 Phase Encoding





Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Review

- 2 LM05 Protocol
 - The Protocol
 - Message Mode
 - Control Mode

First Telecom Window

- Experiment
- Incoherent Individual Attack
- Eavesdropping SimulationImperfect Equipment
- Third Telecom Window
 Phase Encoding





Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individu: Attack Eavesdropping
- Simulation Imperfect Equipme
- Third Telecom Window Phase Encoding
- Summarv

Review

- 2 LM05 Protocol
 - The Protocol
 - Message Mode
 - Control Mode

3 First Telecom Window

- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation
- Imperfect Equipment

Third Telecom Window



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping
- Imperfect Equipme
- Third Telecom Window
- Phase Encoding
- Summary

Review

- 2 LM05 Protocol
 - The Protocol
 - Message Mode
 - Control Mode

3 First Telecom Window

- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation
- Imperfect Equipment
- 4 Third Telecom WindowPhase Encoding
 - Summary



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping
- Imperfect Equipme

Third Telecom Window

- Phase Encoding
- Summary

Review

- 2 LM05 Protocol
 - The Protocol
 - Message Mode
 - Control Mode

3 First Telecom Window

- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation
- Imperfect Equipment
- 4 Third Telecom WindowPhase Encoding
- 5 Summary



Protocols

Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen

Third Telecom Window Phase Encoding

Summary

One-Way

▷ Bennett & Brassard, 1984 •••• ▷ Ekert (E91) and Bennett (B92)

vo-Way

- Dense Coding [Bennett & Wiesner, PRL 69, 2881 (1992)]
 Ping-Pong [Boström & Felbinger, PRL 89, 187902 (2002)]
 Protocols based on entanglement
 Li, quant-ph/0209050
 Long and Liu, PRA 65, 032302 (2002)
 Deng, Long and Liu, PRA 68, 042317 (2003)
 Cai and Li, PRA 69, 054301 (2004)
 [Degiovanni et al., PRA 69, 032310 (2004)]
 - ▷ Cai and Li, Chin. Phys. Lett. **21**, 601 (2004
 - ▷ A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, J. Phys. A 35 407



Protocols

Two-Way QCP

One-Way

Two-Way

Bennett & Brassard, 1984 •••• Ekert (E91) and Bennett (B92)

LM05 Protocol The Protocol Message Mode

Review

First Telecom Window

Experiment Incoherent Individua Attack Eavesdropping Simulation

Third Telecom Window

- ▷ Dense Coding [Bennett & Wiesner, PRL 69, 2881 (1992)] . Go
 ▷ Ping-Pong [Boström & Felbinger, PRL 89, 187902 (2002)] . Go
 ▷ Protocols based on entanglement
 - ▷ Li, quant-ph/0209050
 - ▷ Long and Liu, PRA **65**, 032302 (2002)
 - ▷ Deng, Long and Liu, PRA 68, 042317 (2003)
 - ▷ Cai and Li, PRA 69, 054301 (2004)
 - ▷ [Degiovanni et al., PRA 69, 032310 (2004)]
- ▷ Faint pulses based Protocol
 - ▷ Cai and Li, Chin. Phys. Lett. 21, 601 (2004)
 - ▷ A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, J. Phys. A 35 407



Two-Way QCP

The Protocol Lucamarini & Mancini, PRL 94, 140501 (2005)

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Single qubit (*no entanglement*)
- Two-Way Protocol



The Protocol Lucamarini & Mancini, PRL 94, 140501 (2005)

Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

Experiment Incoherent Individual Attack Eavesdropping Simulation

Imperfect Equipment

Third Telecom Window Phase Encoding

Summary

Single qubit (no entanglement)

Two-Way Protocol



Two-Way QCP

The Protocol Lucamarini & Mancini, PRL 94, 140501 (2005)

The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping
- Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Single qubit (no entanglement)
- Two-Way Protocol



Two-way QCP		
	BOB PREPARATION	ALICE
	(RND)	
LM05 Protocol The Protocol Message Mode Control Mode	0⟩ 1⟩ Z +⟩ -⟩ X	



Two-Way QCP



ENCODING $I \longrightarrow 0^{\circ}$ $iY \longrightarrow 1^{\circ}$



Two-Way QCP



LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

Experiment Incoherent Individu: Attack Eavesdropping Simulation Imperfect Equipment

Third Telecom Window Phase Encoding

Summary



Decoding

 $\begin{array}{l} \mathrm{I}|0,1\rangle = |0,1\rangle \\ \mathrm{i} Y|0,1\rangle = \mp |1,0\rangle \end{array}$

 $\begin{array}{l} \mathrm{I}|+,-\rangle = |-,+\rangle \\ \mathrm{i} \mathrm{Y}|+,-\rangle = \pm |-,+\rangle \end{array}$



Two-Way QCP



LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

Experiment Incoherent Individu: Attack Eavesdropping Simulation Imperfect Equipment

Third Telecom Window







Two-Way QCP



LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window
- Summary







Two-Way QCP

Poviow

LM05 Protocol The Protocol Message Mode

Control Mode

First Telecom Window

Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen

Third Telecom Window Phase Encoding

Summary

Alice does not need to know the incoming state to encode a bit using either identity or polarization-flip
 Bob decodes Alice's message measuring in the same basis he prepared the state

eatures

Actions

Deterministic protocol, i.e. the information is deterministically conveyed from one user to another! No qubits are discarded (wrong basis in BB84) No public discussion is necessary



Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding
- Summary

- Alice does not need to know the incoming state to encode a bit using either identity or polarization-flip
 - Bob decodes Alice's message measuring in the same basis he prepared the state

eatures

Actions

 Deterministic protocol, i.e. the information is deterministically conveyed from one user to another!
 No qubits are discarded (wrong basis in BB84)
 No public discussion is necessary



Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding
- Summary

 Alice does not need to know the incoming state to encode a bit using either identity or polarization-flip
 Bob decodes Alice's message measuring in the same basis he prepared the state

eatures

Actions

Deterministic protocol, i.e. the information is deterministically conveyed from one user to another! No qubits are discarded (wrong basis in BB84) No public discussion is necessary



Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- First Telecon
- Experiment Incoherent Individual Attack Eavesdropping Simulation
- Third Telecom Window Phase Encoding
- Summary

Alice does not need to know the incoming state to encode a bit using either identity or polarization-flip
 Bob decodes Alice's message measuring in the same basis he prepared the state

Features

Actions

Deterministic protocol, i.e. the information is *deterministically* conveyed from one user to another!
 No qubits are discarded (wrong basis in BB84)
 No public discussion is necessary



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding
- Summary

 Alice does not need to know the incoming state to encode a bit using either identity or polarization-flip
 Bob decodes Alice's message measuring in the same basis he prepared the state

Features

Actions

 Deterministic protocol, i.e. the information is deterministically conveyed from one user to another!
 No qubits are discarded (wrong basis in BB84)
 No public discussion is necessary



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding
- Summary

Alice does not need to know the incoming state to encode a bit using either identity or polarization-flip
 Bob decodes Alice's message measuring in the same basis he prepared the state

Features

Actions

 Deterministic protocol, i.e. the information is deterministically conveyed from one user to another!
 No qubits are discarded (wrong basis in BB84)
 No public discussion is necessary



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding
- Summary

 Alice does not need to know the incoming state to encode a bit using either identity or polarization-flip
 Bob decodes Alice's message measuring in the same basis he prepared the state

Features

Actions

- Deterministic protocol, i.e. the information is deterministically conveyed from one user to another!
- No qubits are discarded (wrong basis in BB84)
- No public discussion is necessary



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation
- Imperfect Equipment
- United Telecom Window Phase Encoding
- Summary

- Actions
 - Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
 - She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
 - Public debate on results

eatures



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
 - She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
 Public debate on results

eatures

Actions



Actions

Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individual Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
- She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state

Public debate on results

eatures



Actions

Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
- She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
- Public debate on results

eatures



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individual Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
- She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
- Public debate on results

Features

Actions



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individual Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summarv

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
- She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
- Public debate on results

Features

Actions



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individual Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summarv

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
- She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
- Public debate on results

Features

Actions



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
- She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
- Public debate on results

Features

Actions



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individual Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Alice performs a projective measurement on the qubit along a basis randomly chosen between Z and X
- She then sends the projected qubit to Bob, who measures it in the same basis he prepared the state
- Public debate on results

Features

Actions



Experiment Setup@810nm



Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window Experiment

Attack Eavesdropping Simulation Imperfect Equipme

Third Telecom Window Phase Encoding





Experiment Setup

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window

Experiment

Incoherent Individu Attack Eavesdropping Simulation Imperfect Equipme

Third Telecom Window Phase Encoding





Experiment Setup - Communication Tests

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window Experiment

Experiment

Attack Eavesdropping Simulation Imperfect Equipm

Third Telecon Window Phase Encoding









Experiment Setup - Communication Tests

Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecon Window Experiment

Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmer

Third Telecon Window

Summarv










Experiment Setup - Communication Tests

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window Experiment

Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmer

Third Telecon Window Phase Encoding

Summarv









Experiment Setup - Communication Tests

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window Experiment

Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmer

Third Telecon Window Phase Encoding

Summary





Faint-Pulses





Experiment Setup - Communication Tests

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window Experiment

Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmer

Third Telecon Window Phase Encoding

Summary









Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window Experiment

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

luantum Direct Communication

Can Alice send to Bob a meaningful string ?

Problems

・ロ・・ボー・オー・オー・オー・



Quantum Key Distribution

Two-Way QCP

Review

- LM05 Protocc The Protocol Message Mode Control Mode
- First Telecom Window
- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction
- Privacy Amplification sec

uantum Direct Communication

Can Alice send to Bob a meaningful string ??



Two-Way QCP

Quantum Key Distribution

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window Experiment

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation Error Correction — identical key

uantum Direct Communication

Can Alice send to Bob a meaningful string



Two-Way QCP

Quantum Key Distribution

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window Experiment

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation Error Correction — identical key

uantum Direct Communication

Can Alice send to Bob a meaningful string



Two-Way QCP

Quantum Key Distribution

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification

secure key

antum Direct Communication

Alice send to Bob a *meaningful* string



Two-Way QCP

Quantum Key Distribution

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification

secure key

antum Direct Communication

Alice send to Bob a *meaningful* string



Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summarv

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification → secure key

Quantum Direct Communication

- Can Alice send to Bob a *meaningful* string ?
 - Reliable (Error Correction)
 - Secure (Privacy Amplification)

- QBEF
- Losses



Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification → secure key

- Can Alice send to Bob a *meaningful* string ?
 - Reliable (Error Correction)
 - Secure (Privacy Amplification)
- Problems ...
 - QBEF
 - Losses



Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window

- Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification → secure key

Quantum Direct Communication

- Can Alice send to Bob a *meaningful* string ?
 - Reliable (Error Correction)
 - Secure (Privacy Amplification)

- QBEF
 - Losses



Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window Experiment

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification → secure key

Quantum Direct Communication

- Can Alice send to Bob a *meaningful* string ?
 - Reliable (Error Correction)
 - Secure (Privacy Amplification)

- OBER
 - Losses



Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification → secure key

- Can Alice send to Bob a *meaningful* string ?
 - Reliable (Error Correction)
 - Secure (Privacy Amplification)
- Problems ...
 - QBER
 - Losses



Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification → secure key

- Can Alice send to Bob a *meaningful* string ?
 - Reliable (Error Correction)
 - Secure (Privacy Amplification)
- Problems ...
 - QBER
 - Losses



Quantum Key Distribution

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

- Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Distribution of a key vs. generation

- Error Correction → identical keys
- Privacy Amplification → secure key

- Can Alice send to Bob a *meaningful* string ?
 - Reliable (Error Correction)
 - Secure (Privacy Amplification)
- Problems ...
 - QBER
 - Losses



Two-Way QCP

- LM05 Protocol The Protocol Message Mode Control Mode
- First Telecom Window
- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Individual attacks: a probe on each qubit and measuring the probe singularly
- Coherent attacks: Eve processes several qubits coherently
 - Collective attacks: a probe on each qubit but measuring several probes *collectively*
 - Joint attacks: a probe on several qubits and measure the probe



Two-Way QCP

- LM05 Protocol The Protocol Message Mode Control Mode
- First Telecon Window
- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Individual attacks: a probe on each qubit and measuring the probe singularly
- Coherent attacks: Eve processes several qubits coherently
 - Collective attacks: a probe on each qubit but measuring several probes *collectively*
 - Joint attacks: a probe on several qubits and measure the probe



Two-Way QCP

- LM05 Protocol The Protocol Message Mode Control Mode
- First Telecon Window
- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Individual attacks: a probe on each qubit and measuring the probe singularly
- Coherent attacks: Eve processes several qubits coherently
 - Collective attacks: a probe on each qubit but measuring several probes *collectively*
 - Joint attacks: a probe on several qubits and measure the probe



Two-Way QCP

- LM05 Protocol The Protocol Message Mode Control Mode
- First Telecom Window
- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding
- Summary

- Individual attacks: a probe on each qubit and measuring the probe singularly
- Coherent attacks: Eve processes several qubits coherently
 - Collective attacks: a probe on each qubit but measuring several probes *collectively*
 - Joint attacks: a probe on several qubits and measure the probe



Two-Way QCP

- LM05 Protocol The Protocol Message Mode Control Mode
- First Telecom Window
- Experiment
- Incoherent Individual Attack
- Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Individual attacks: a probe on each qubit and measuring the probe singularly
- Coherent attacks: Eve processes several qubits coherently
 - Collective attacks: a probe on each qubit but measuring several probes *collectively*
 - Joint attacks: a probe on several qubits and measure the probe



Incoherent Individual Attack Eve's probes

Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

Incoherent Individual Attack

Eavesdropping Simulation Imperfect Equipme

Third Telecom Window Phase Encoding

Summary



orthogonal Eve's probe (at most 4-dim)

 $\begin{array}{l} |0\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \\ |1\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle \end{array}$

 $\begin{array}{c} |+\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{++}\rangle + |-\rangle|\epsilon_{-+}\rangle \\ |-\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{+-}\rangle + |-\rangle|\epsilon_{--}\rangle \end{array}$



Incoherent Individual Attack





LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

Incoherent Individual Attack

Eavesdropping Simulation Imperfect Equipme

Third Telecom Window Phase Encoding

Summary



Non-orthogonal Eve's probe (at most 4-dim)

 $\begin{array}{l} |0\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \\ 1\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle \end{array}$

 $\begin{array}{l} |+\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{++}\rangle + |-\rangle|\epsilon_{-+}\rangle \\ |-\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{+-}\rangle + |-\rangle|\epsilon_{--}\rangle \end{array}$



Incoherent Individual Attack Eve's probes





Incoherent Individual Attack



Non-orthogonal Eve's probe (at most 4-dim)



Incoherent Individual Attack Eve's probes





Incoherent Individual Attack



Non-orthogonal Eve's probe (at most 4-dim)



Eavesdropping Simulation A. Ceré et. al, PRL 96, 200501 (2006)



Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

Experiment Incoherent Individ Attack

Eavesdropping Simulation

Third Telecom Window Phase Encoding

Summary



Same unitary operation on the forward and backward paths

- **・ ロ ・ ・ ヨ ・ ・ ヨ ・** ・ ヨ ・ の へ ()



Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode

First Telecom Window

Experiment Incoherent Individua Attack

Eavesdropping Simulation

Imperfect Equipment

Third Telecom Window Phase Encoding

Summary

The Shannon Mutual Information $I(\alpha, \beta)$ can be estimated from the QBER

 $I(A, B) \ge \min[I(A, E), I(B, E)]$



Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode

First Telecom Window

Experiment Incoherent Individu Attack

Eavesdropping Simulation

Imperfect Equipment

Third Telecom Window Phase Encoding

Summary

The Shannon Mutual Information $I(\alpha, \beta)$ can be estimated from the QBER

Condition for distillation of a secure key: $I(A, B) \ge \min[I(A, E), I(B, E)]$



Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

Experiment Incoherent Individu Attack

Eavesdropping Simulation

Imperfect Equipment

Third Telecom Window Phase Encoding

Summary

The Shannon Mutual Information $I(\alpha, \beta)$ can be estimated from the QBER

• Condition for distillation of a secure key: $I(A, B) \ge \min[I(A, E), I(B, E)]$





I(A, B) $\geq I(B, E)$ alway

If $I(A, B) \ge I(A, E)$ for $Q_{AB} \le ~ 19\%$ (~ 15% for BB84)





$I(A,B) \ge I(B,E) \text{ always}$

If $I(A, B) \ge I(A, E)$ for $Q_{AB} \le ~ 19\%$ (~ 15% for BB84)





 $I(A,B) \ge I(B,E) \text{ always}$

■ $I(A, B) \ge I(A, E)$ for $Q_{AB} \le ~ 19\%$ (~ 15% for BB84)



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individu: Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
 Detectors:
 - avalanche (click or no-click)
 quantum efficiency less than one
 dark counts
- Lossy channel: photons are lost in a double-trip





Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individu: Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
 Detectors:
 - avalanche (click or no-click) quantum efficiency less than one dark counts
 - Lossy channel: photons are lost in a double-trip





Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individu Attack Eavesdropping
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
 Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip





Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individu Attack Eavesdropping
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
 Datastance
- Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip




Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individu Attack Eavesdropping
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
- Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip





Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individe Attack Eavesdropping
- Simulation Imperfect Equipment
- Third Telecom Window
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
- Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip





Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individu Attack Eavesdropping
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
- Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip





Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individu Attack Eavesdropping
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
- Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip

lelevant Threat

PNS-attack



Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individu Attack Eavesdropping
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
- Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip

Relevant Threat

PNS-attack



Two-Way QCP

Review

- LM05 Protocol The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individu Attack Eavesdropping
- Imperfect Equipment

Third Telecom Window Phase Encoding

Summary

- Faint-Pulses: attenuated laser which accidentally/uncontrollably contains more than one photon
- Detectors:
 - avalanche (click or no-click)
 - quantum efficiency less than one
 - dark counts

Lossy channel: photons are lost in a double-trip

Relevant Threat

PNS-attack



Imperfect Equipment

Secure Rate [Following N. Lütkenhaus, PRA, 61, 052304 (2000)]

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

Experiment Incoherent Individual Attack Eavesdropping Simulation Imperfect Equipment

Third Telecom Window Phase Encoding

Summary

P. D. Townsend, IEEE Photonics Technol. Lett., 10, 1048 (1998)

 $\lambda = 830 \text{ nm}$ x = 2.5 dB/Km $f_c = 8 \text{ dB}$ $f_B = 0.5$





Imperfect Equipment

Secure Rate [Following N. Lütkenhaus, PRA, 61, 052304 (2000)]

P. D. Townsend, IEEE Photonics Technol. Lett., 10, 1048 (1998)

LM05 Protocol The Protocol Message Mode Control Mode

First Telecom Window

Experiment Incoherent Individu Attack Eavesdropping Simulation

Imperfect Equipment

Third Telecom Window Phase Encoding

Summary

 $\lambda = 830 \text{ nm}$ $\alpha = 2.5 \text{ dB/Km}$ $\Gamma_c = 8 \text{ dB}$ $d_B =$ $5 10^{-8} \text{ cnts/slot}$ $\eta_B = 0.5$





Imperfect Equipment

Secure Rate [Following N. Lütkenhaus, PRA, 61, 052304 (2000)]

P. D. Townsend, IEEE Photonics Technol. Lett., 10, 1048 (1998)

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individe Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

 $\lambda = 830 \text{ nm}$ $\alpha = 2.5 \text{ dB/Km}$ $\Gamma_c = 8 \text{ dB}$ $d_B =$ $5 10^{-8} \text{ cnts/slot}$ $\eta_B = 0.5$





Imperfect Equipment

Secure Rate [Following N. Lütkenhaus, PRA, 61, 052304 (2000)]

P. D. Townsend, IEEE Photonics Technol. Lett., 10, 1048 (1998)

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individe Attack Eavesdropping Simulation
- Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

 $\lambda = 830 \text{ nm}$ $\alpha = 2.5 \text{ dB/Km}$ $\Gamma_c = 8 \text{ dB}$ $d_B =$ $5 10^{-8} \text{ cnts/slot}$ $\eta_B = 0.5$





Phase Encoding Scheme





Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmer
- Third Telecom Window Phase Encoding
- Summary







Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode Control Mode

First Telecon Window

- Experiment Incoherent Individu: Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding

Summary







Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecon Window

- Experiment Incoherent Individu: Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding

Summary

Alice





・ロ・・ボー・ボー・ボー・



Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecon Window

- Experiment Incoherent Individu: Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding

Summary

Alice



Bob





Two-Way QCP

Review

LM05 Protocol The Protocol Message Mode Control Mode

First Telecon Window

- Experiment Incoherent Individu: Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding
- Summary

Alice



Bob





Results

Two-Way QCP

Review

- LM05 Protocol
- Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding

Summary

- We have shown an experimental test of LM0
- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
- Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

nprovements

No direct, contextual transmission of string of bits.

On the way



Results

Two-Way QCP

Review

- LM05 Protoco
- The Protocol
- Message Mod
- Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding

Summary

We have shown an experimental test of LM05.

- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
- Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

nprovements

No direct, contextual transmission of string of bits.

On the way



Results

Two-Way QCP

Review

- LM05 Protoco The Protocol Message Mode
- Control Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding

Summary

- We have shown an experimental test of LM05.
- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
 - Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

nprovements

No direct, contextual transmission of string of bits.

On the way



Results

Two-Way QCP

Review

- LM05 Protoco The Protocol Message Mode
- Control Mode

First Telecon Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding

Summary

We have shown an experimental test of LM05.

- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
- Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

provements

No direct, contextual transmission of string of bits.

On the way



Two-Way QCP

Review

- LM05 Protoco The Protocol Message Mode
- First Telecoi
- Window
- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipment
- Third Telecom Window Phase Encoding

Summary

Results

- We have shown an experimental test of LM05.
- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
- Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

Improvements

No direct, contextual transmission of string of bits.

On the way



Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode

First Telecom Window

Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen

Third Telecom Window Phase Encoding

Summary

Results

- We have shown an experimental test of LM05.
- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
- Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

Improvements

No direct, contextual transmission of string of bits.

On the way



Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding

Summary

Results

- We have shown an experimental test of LM05.
- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
- Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

Improvements

No direct, contextual transmission of string of bits.

On the way



Two-Way QCP

Review

LM05 Protoco The Protocol Message Mode

First Telecom Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding

Summary

Results

- We have shown an experimental test of LM05.
- Modulating the noise on the channel to simulate Eve's IIA disturbance, we have estimated the mutual informations and shown the range of security of the protocol for IIA on lossless channel.
- Higher secure rate even for lossy channel and imperfect devices on short-middle distances.

Improvements

No direct, contextual transmission of string of bits.

On the way



Founding

Two-Way QCP

Review

LM05 Protocol

- Message Mod
- Control Mode

First Telecon Window

- Experiment Incoherent Individua Attack Eavesdropping Simulation Imperfect Equipmen
- Third Telecom Window Phase Encoding

Summary

IST – Integrated Project 'Qubit Applications' (QAP)





MIUR - FIRB 2001 and PRIN 2005

・ロト・日本・日本・日本・日本・今日、