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 Optics & Quantum Information Group

Outline

Outline

Quantum Optics & Quantum Information Group

Outline

Outline

Outline

Protocols

One-Way

- Bennett & Brassard, 1984 Go
- Ekert (E91) and Bennett (B92)

Two-Way

- 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

Protocols

One-Way

- ▷ Bennett & Brassard, 1984 ▸ Go
- ▷ Ekert (E91) and Bennett (B92)

Two-Way

- ▷ 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

The Protocol

Lucamarini & Mancini, PRL **94**, 140501 (2005)

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

The Protocol

Lucamarini & Mancini, PRL **94**, 140501 (2005)

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

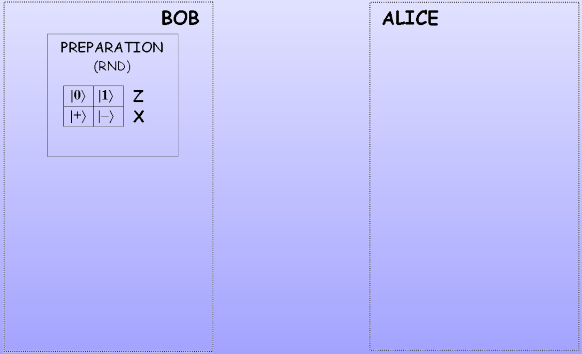
The Protocol

Lucamarini & Mancini, PRL **94**, 140501 (2005)

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

The Protocol

How it works!



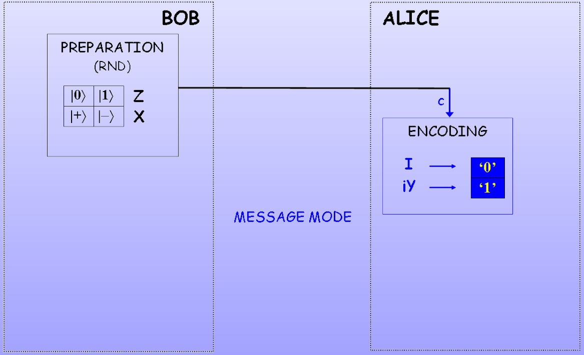
Decoding

$$\mathrm{I}|0,1\rangle = |0,1\rangle \qquad \mathrm{I}|+,-\rangle = |-,+\rangle$$

$$\mathrm{iY}|0,1\rangle = \mp|1,0\rangle \qquad \mathrm{iY}|+,-\rangle = \pm|-,+\rangle$$

The Protocol

How it works!

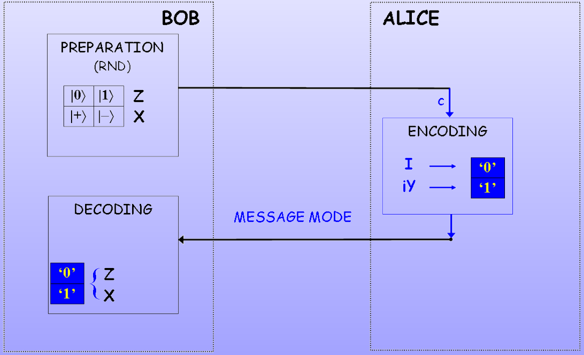


Decoding

$$\mathrm{I}|0,1\rangle = |0,1\rangle \qquad \mathrm{I}|+,-\rangle = |-,+\rangle$$
$$\mathrm{iY}|0,1\rangle = \mp|1,0\rangle \qquad \mathrm{iY}|+,-\rangle = \pm|-,+\rangle$$

The Protocol

How it works!



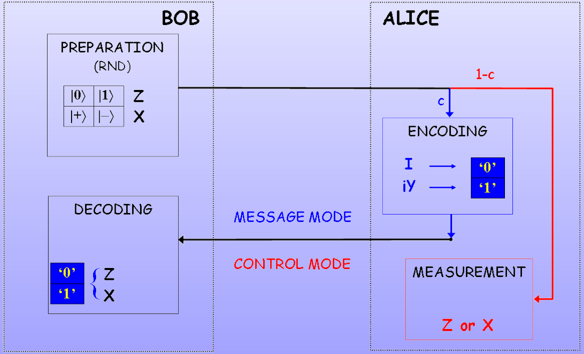
Decoding

$$\mathrm{I}|0,1\rangle = |0,1\rangle \qquad \mathrm{I}|+,-\rangle = |-,+\rangle$$

$$\mathrm{iY}|0,1\rangle = \mp|1,0\rangle \qquad \mathrm{iY}|+,-\rangle = \pm|-,+\rangle$$

The Protocol

How it works!

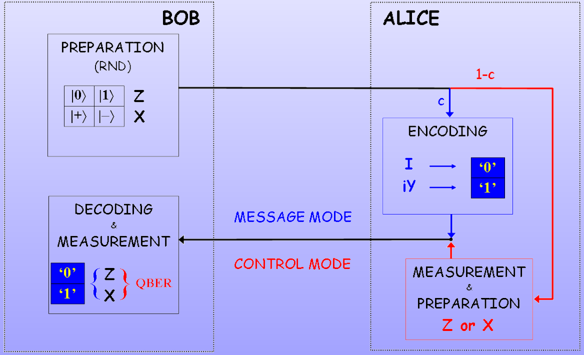


Decoding

$$I|0,1\rangle = |0,1\rangle \qquad I|+,-\rangle = |-,+\rangle$$
$$iY|0,1\rangle = \mp|1,0\rangle \qquad iY|+,-\rangle = \pm|-,+\rangle$$

The Protocol

How it works!



Decoding

$$I|0,1\rangle = |0,1\rangle \qquad I|+,-\rangle = |-,+\rangle$$

$$iY|0,1\rangle = \mp|1,0\rangle \qquad iY|+,-\rangle = \pm|-,+\rangle$$

Message Mode
Summary

Actions

- 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

- 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

Message Mode

Summary

Actions

- 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

- 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

Message Mode
Summary

Actions

- 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

- 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

Message Mode

Summary

Actions

- 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

- 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

Message Mode

Summary

Actions

- 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

- 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

Message Mode
Summary

Actions

- 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

- 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

Actions

- 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

- 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

Control Mode

Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel → (at least BB84) security

Control Mode

Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel → (at least BB84) security

Control Mode

Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel → (at least BB84) security

Control Mode
Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel → (at least BB84) security

Control Mode

Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel $\rightarrow$ (at least BB84) security

Control Mode
Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel $\rightarrow$ (at least BB84) security

Control Mode
Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel $\rightarrow$ (at least BB84) security

Control Mode
Security

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

Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel $\rightarrow$ (at least BB84) security

Control Mode
Security

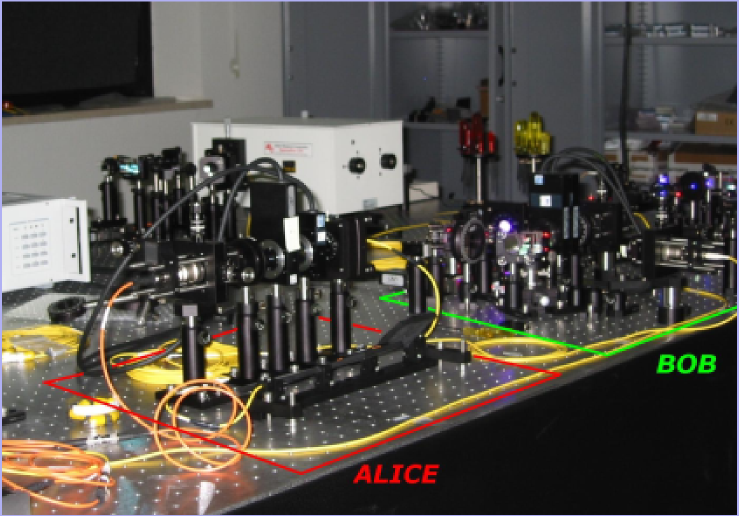
Actions

- 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

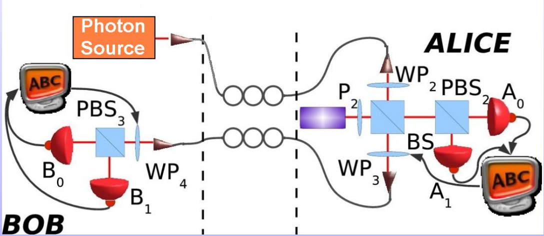
Features

- If Eve is not on the line, the users must find perfect *double correlation*: *Double* (BB84) check on the channel $\rightarrow$ (at least BB84) security

Experiment
Setup@810nm

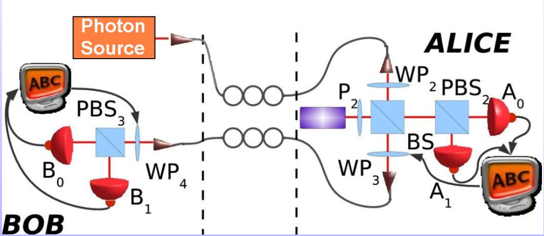


Experiment
Setup

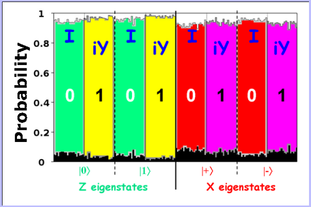


Experiment

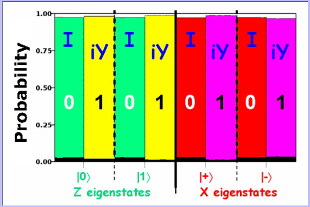
Setup - Communication Tests



SPDC

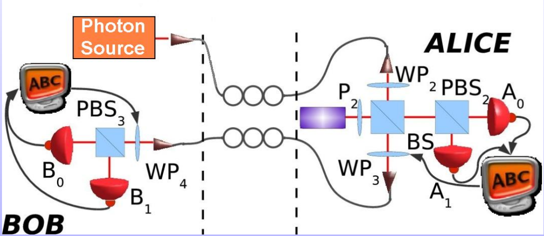


Faint-Pulses

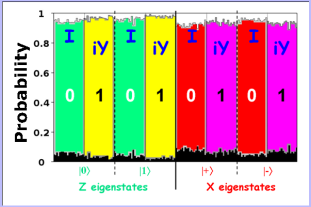


Experiment

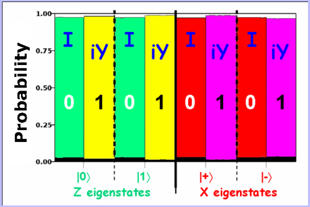
Setup - Communication Tests



SPDC

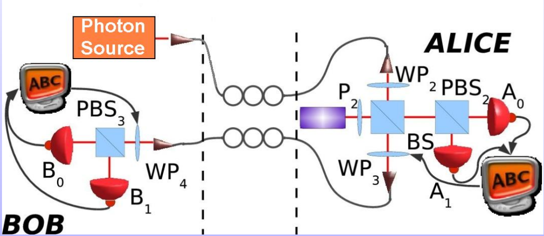


Faint-Pulses

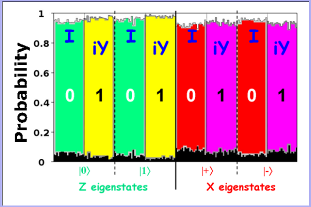


Experiment

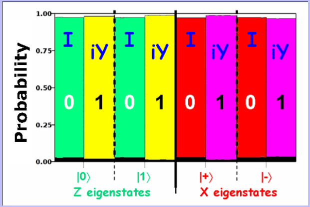
Setup - Communication Tests



SPDC

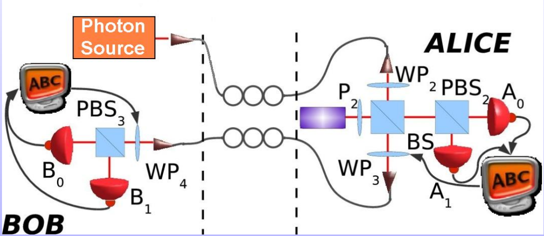


Faint-Pulses

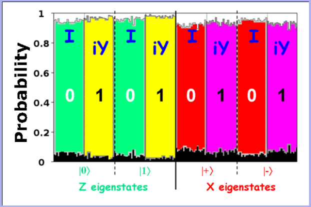


Experiment

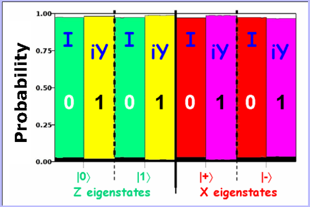
Setup - Communication Tests



SPDC

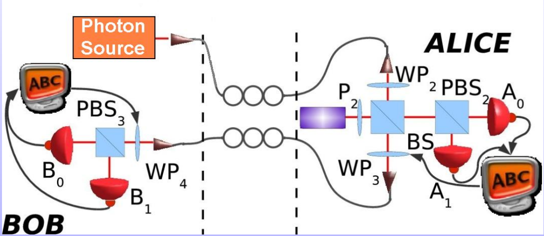


Faint-Pulses

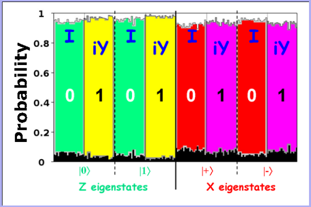


Experiment

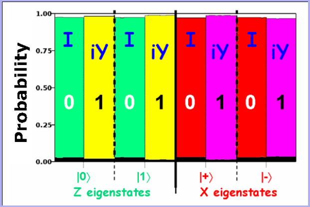
Setup - Communication Tests



SPDC



Faint-Pulses



Experiment

Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction

Quantum Direct Communication

Can Alice send to Bob a *meaningful* string ?

Problems ...

Experiment

Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

Can Alice send to Bob a *meaningful* string ?

Problems ...

Experiment

Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

Can Alice send to Bob a meaningful string ?

Problems ...

Experiment
Discussion on the Message Mode

Quantum Key Distribution

- *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 ?

Problems ...

Experiment

Discussion on the Message Mode

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

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

Can Alice send to Bob a meaningful string ?

Problems ...

Experiment

Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

Can Alice send to Bob a *meaningful* string ?

Problems ...

Experiment
Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

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

Experiment

Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

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

Experiment
Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

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

Experiment

Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

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

Experiment

Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

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

Experiment
Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

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

Experiment
Discussion on the Message Mode

Quantum Key Distribution

- *Distribution* of a key vs. *generation*
  - Error Correction $\longrightarrow$ identical keys
  - Privacy Amplification $\longrightarrow$ secure key

Quantum Direct Communication

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

Eve's attacks

noisy lossless channel

- 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

Eve's attacks
noisy lossless channel

- **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

Eve’s attacks
noisy lossless channel

- 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

Eve's attacks
noisy lossless channel

- **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

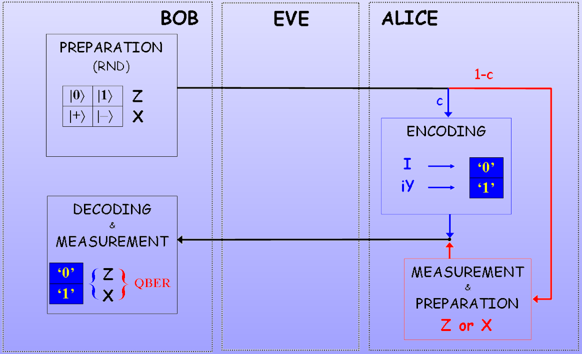
Eve’s attacks

noisy lossless channel

- **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

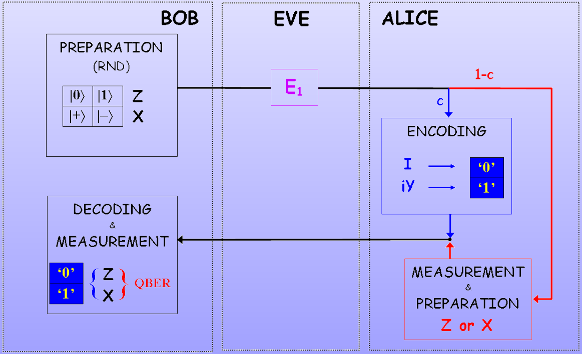


Non-orthogonal Eve's probe (at most 4-dim)

$$|0\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \qquad |+\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{++}\rangle + |-\rangle|\epsilon_{-+}\rangle$$
$$|1\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle \qquad |-\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{+-}\rangle + |-\rangle|\epsilon_{--}\rangle$$

Incoherent Individual Attack

Eve's probes



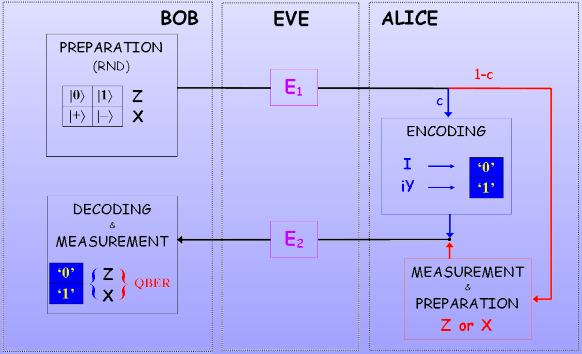
Non-orthogonal Eve's probe (at most 4-dim)

$$|0\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \qquad |+\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{++}\rangle + |-\rangle|\epsilon_{-+}\rangle$$

$$|1\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle \qquad |-\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{+-}\rangle + |-\rangle|\epsilon_{--}\rangle$$

Incoherent Individual Attack

Eve's probes



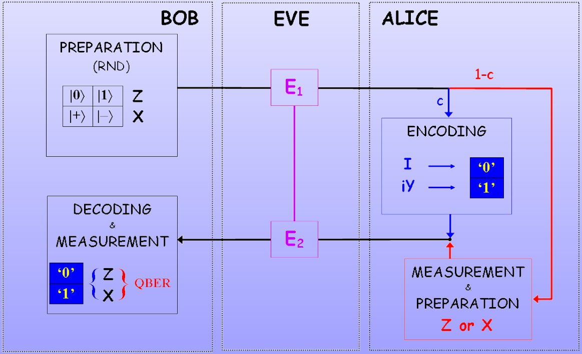
Non-orthogonal Eve's probe (at most 4-dim)

$$|0\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \qquad |+\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{++}\rangle + |-\rangle|\epsilon_{-+}\rangle$$

$$|1\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle \qquad |-\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{+-}\rangle + |-\rangle|\epsilon_{--}\rangle$$

Incoherent Individual Attack

Eve's probes



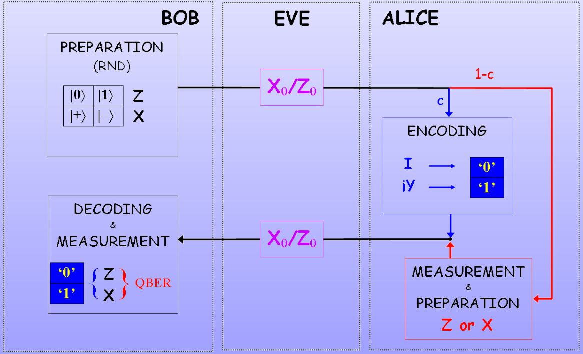
Non-orthogonal Eve's probe (at most 4-dim)

$$|0\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{00}\rangle + |1\rangle|\epsilon_{01}\rangle \qquad |+\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{++}\rangle + |-\rangle|\epsilon_{-+}\rangle$$

$$|1\rangle|\epsilon\rangle \longrightarrow |0\rangle|\epsilon_{10}\rangle + |1\rangle|\epsilon_{11}\rangle \qquad |-\rangle|\epsilon\rangle \longrightarrow |+\rangle|\epsilon_{+-}\rangle + |-\rangle|\epsilon_{--}\rangle$$

Eavesdropping Simulation

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



Same unitary operation on the forward and backward paths

Eavesdropping Simulation

Mutual Information

- The Shannon Mutual Information $I(\alpha, \beta)$ can be estimated from the QBER
- Condition for distillation of a secure key: $I(A, B) \geq \min[I(A, E), I(B, E)]$

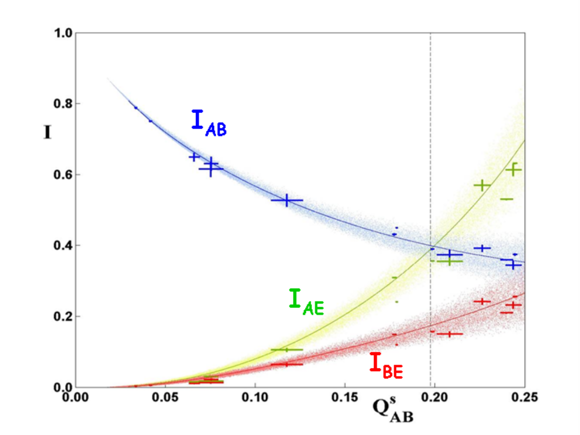
Eavesdropping Simulation
Mutual Information

- The Shannon Mutual Information $I(\alpha, \beta)$ can be estimated from the QBER
- Condition for distillation of a secure key: $I(A, B) \geq \min[I(A, E), I(B, E)]$

Eavesdropping Simulation
Mutual Information

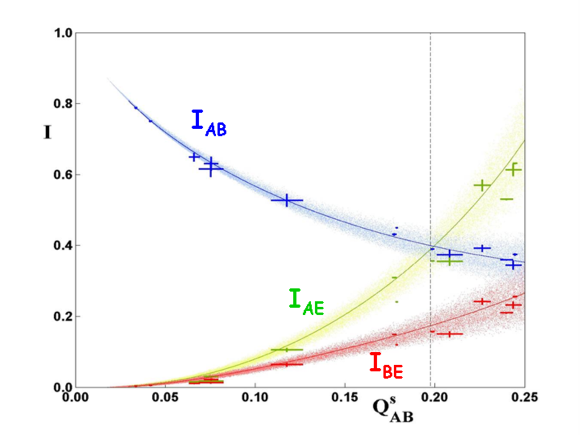
- The Shannon Mutual Information $I(\alpha, \beta)$ can be estimated from the QBER
- Condition for distillation of a secure key: $I(A, B) \geq \min[I(A, E), I(B, E)]$

Eavesdropping Simulation
Mutual Information



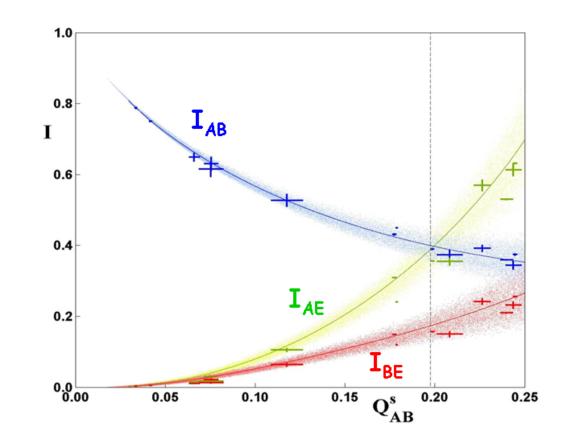
- $I(A,B) \geq I(B,E)$ always
- $I(A,B) \geq I(A,E)$ for $Q_{AB} \leq\sim 19\%$ ($\sim 15\%$ for BB84)

Eavesdropping Simulation
Mutual Information



- $I(A, B) \geq I(B, E)$ always
- $I(A, B) \geq I(A, E)$ for $Q_{AB} \leq \sim 19\%$ ($\sim 15\%$ for BB84)

Eavesdropping Simulation
Mutual Information



- $I(A,B) \geq I(B,E)$ always
- $I(A,B) \geq I(A,E)$ for $Q_{AB} \leq\sim 19\%$ ($\sim 15\%$ for BB84)

Imperfect Equipment
Losses

- 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

Quantum Optics & Quantum Information Group

Imperfect Equipment

Losses

- **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

Imperfect Equipment
Losses

- **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

Imperfect Equipment
Losses

- **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

Imperfect Equipment

Losses

- **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

Imperfect Equipment

Losses

- **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

Imperfect Equipment
Losses

- **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

Imperfect Equipment
Losses

- **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
Losses

- **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

Losses

- 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

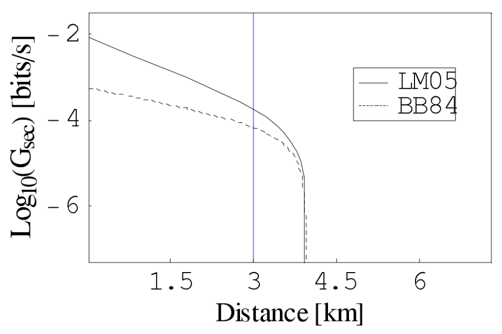
PNS-attack

Imperfect Equipment

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

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

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

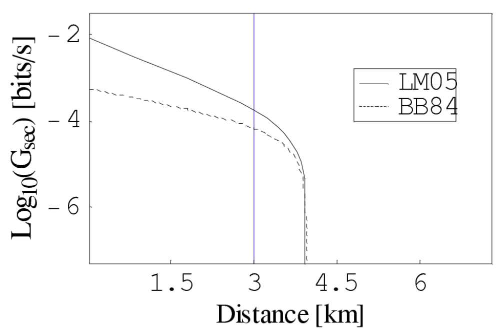


Imperfect Equipment

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

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

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

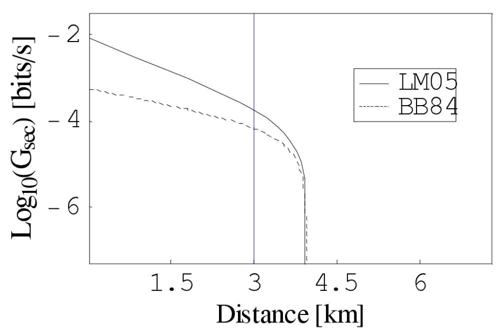


Imperfect Equipment

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

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

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

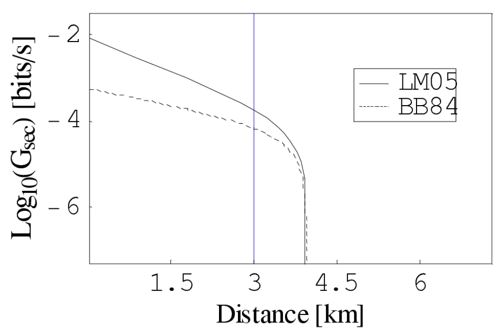


Imperfect Equipment

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

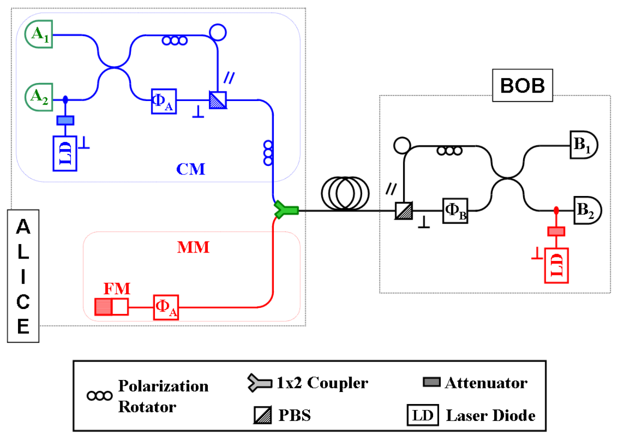
P. D. Townsend, IEEE Photonics Technol. Lett., **10**, 1048 (1998)

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



Phase Encoding

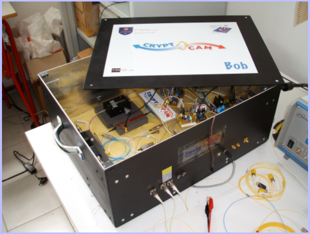
Scheme



Phase Encoding
Implementation

Alice

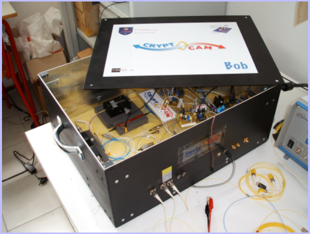
Bob



Phase Encoding
Implementation

Alice

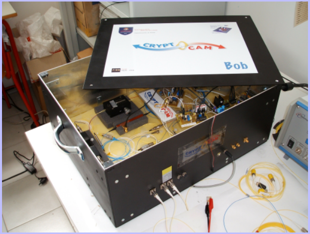
Bob



Phase Encoding
Implementation

Alice

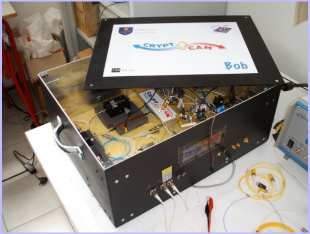
Bob



Phase Encoding
Implementation

Alice

Bob

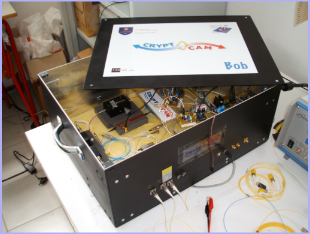


Quantum Optics & Quantum Information Group

Phase Encoding
Implementation

Alice

Bob



Conclusion

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

- real-time running two-way protocol @1550nm.

Conclusion

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

- real-time running two-way protocol @1550nm.

Conclusion

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

- real-time running two-way protocol @1550nm.

Conclusion

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

- real-time running two-way protocol @1550nm.

Conclusion

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

- real-time running two-way protocol @1550nm.

Conclusion

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

- real-time running two-way protocol @1550nm.

Conclusion

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

- real-time running two-way protocol @1550nm.

Quantum Optics & Quantum Information Group

Conclusion

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

- real-time running two-way protocol @1550nm.

Founding

IST – Integrated Project ‘Qubit Applications’ (QAP)

MIUR – FIRB 2001 and PRIN 2005