Presentation III: Decoy state based QKD protocol

Just the first of the first

Presentation III: Decoy state based QKD protocol

Story of reducing (putting a bound on) false positives

Presentation III: Decoy state based QKD protocol

Story of reducing (putting a bound on) false positives

Based on

Decoy State Quantum Key Distribution

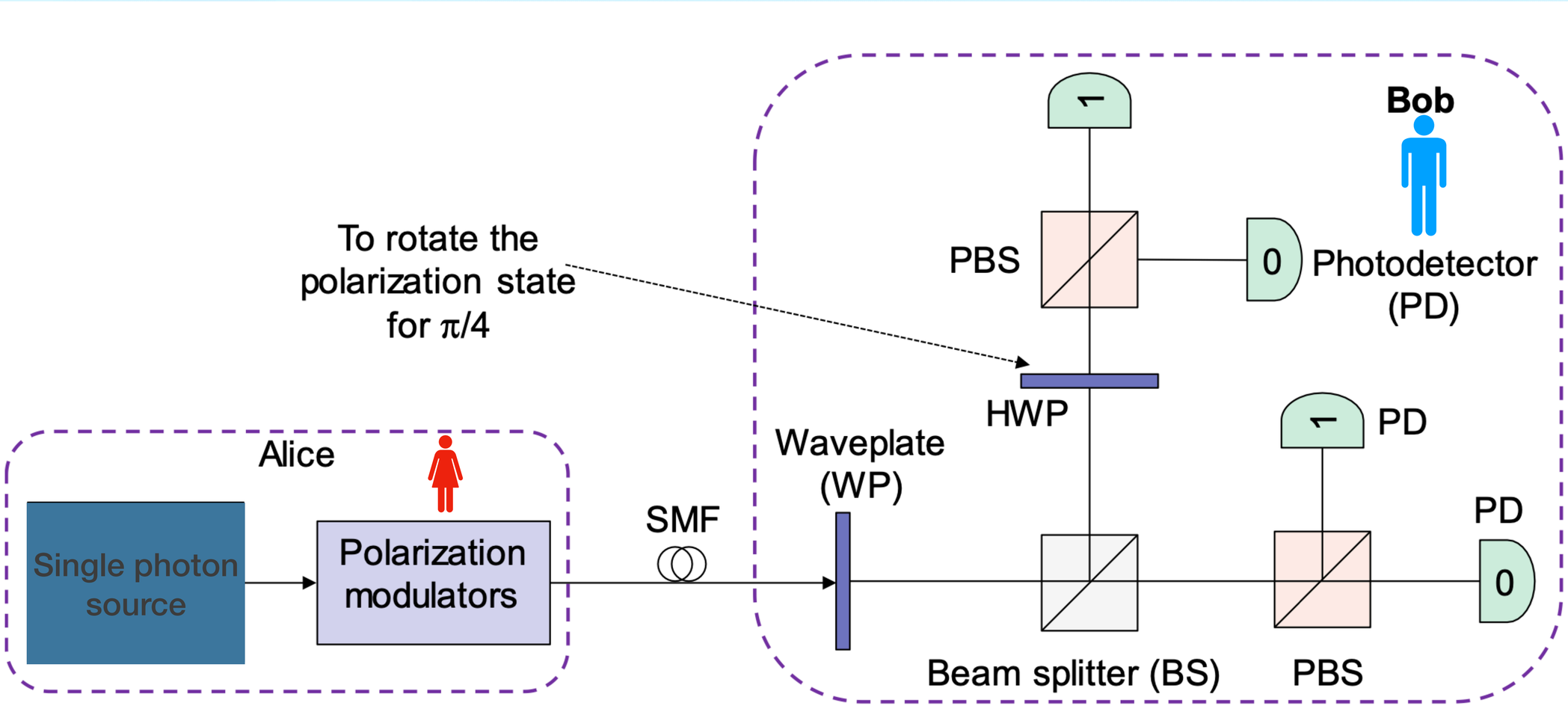
Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen

PRL **94,** 230504 (2005)

Why this presentation?

Last presentation: Heavy on notation and we could not explain some terms.

Schematic for experimental implementation
Polarisation based BB84 protocol



But, where are the single photon sources?

- Quantum dots

But, where are the single photon sources?

- Quantum dots

- Heralded single photon sources: from spontaneous parametric down conversion

But, where are the single photon sources?

- Quantum dots

- Heralded single photon sources: spontaneous parametric down conversion

  Second order non-linear process

  Costly

  Yield is very low (~mHz)

But, where are the single photon sources?

- Quantum dots

- Heralded single photon sources: from spontaneous parametric down conversion

  Second order non-linear process
  Costly
  Yield is very low (∼mHz)

- Resource friendly : weak coherent pulses (with small mean photon number μ)

$$|\,|\mu|\,e^{i\theta}\rangle$$

Weak coherent pulse

$$\frac{1}{2\pi}\int_0^{2\pi} d\theta\,|\mu\rangle\langle\mu| = \sum_{n=0}^{\infty} e^{-|\mu|^2}\frac{|\mu|^n}{n!}|n\rangle\langle n|$$

Multi-photon components

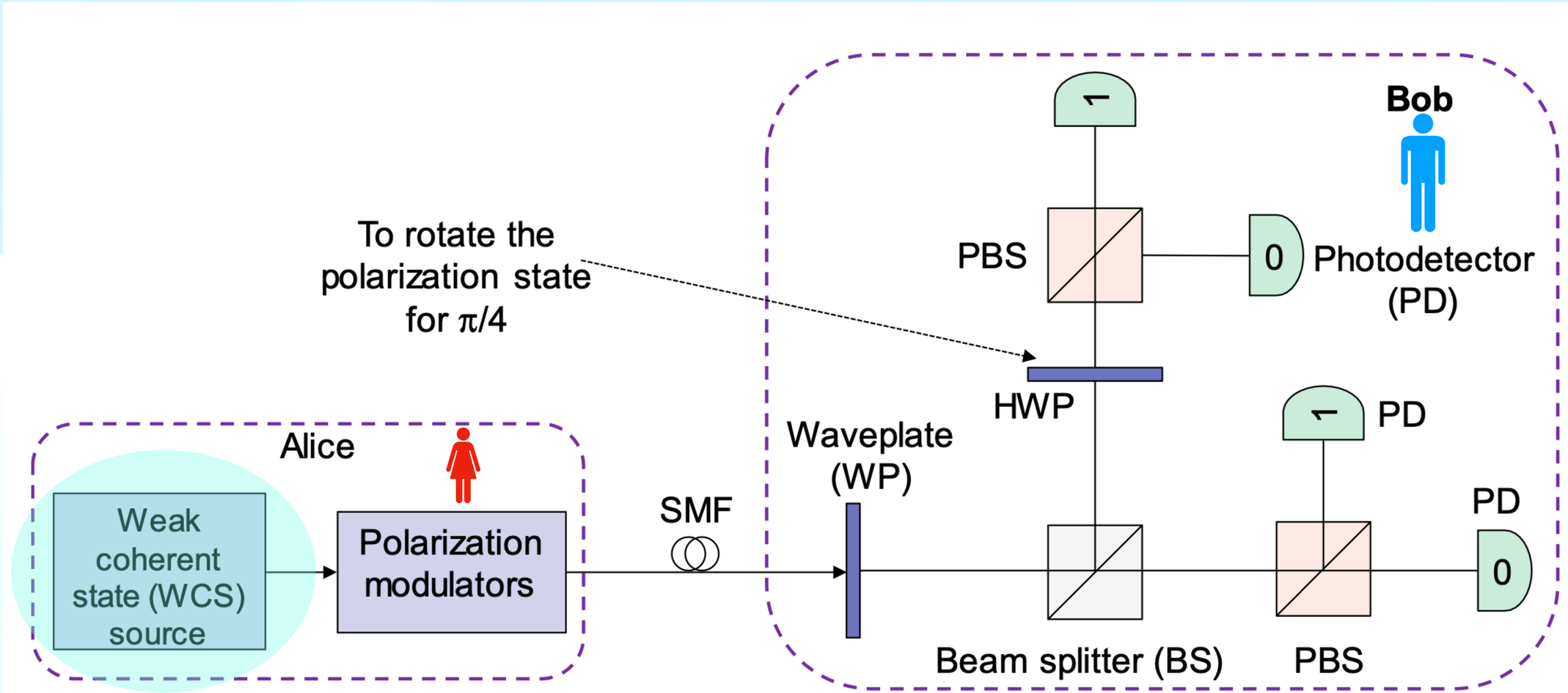
$$\mu = 0.1 \implies |0.1\rangle = \sqrt{0.90}\,|0\rangle + \sqrt{0.09}\,|1\rangle + \sqrt{0.002}\,|2\rangle + \cdots$$

No photon at all

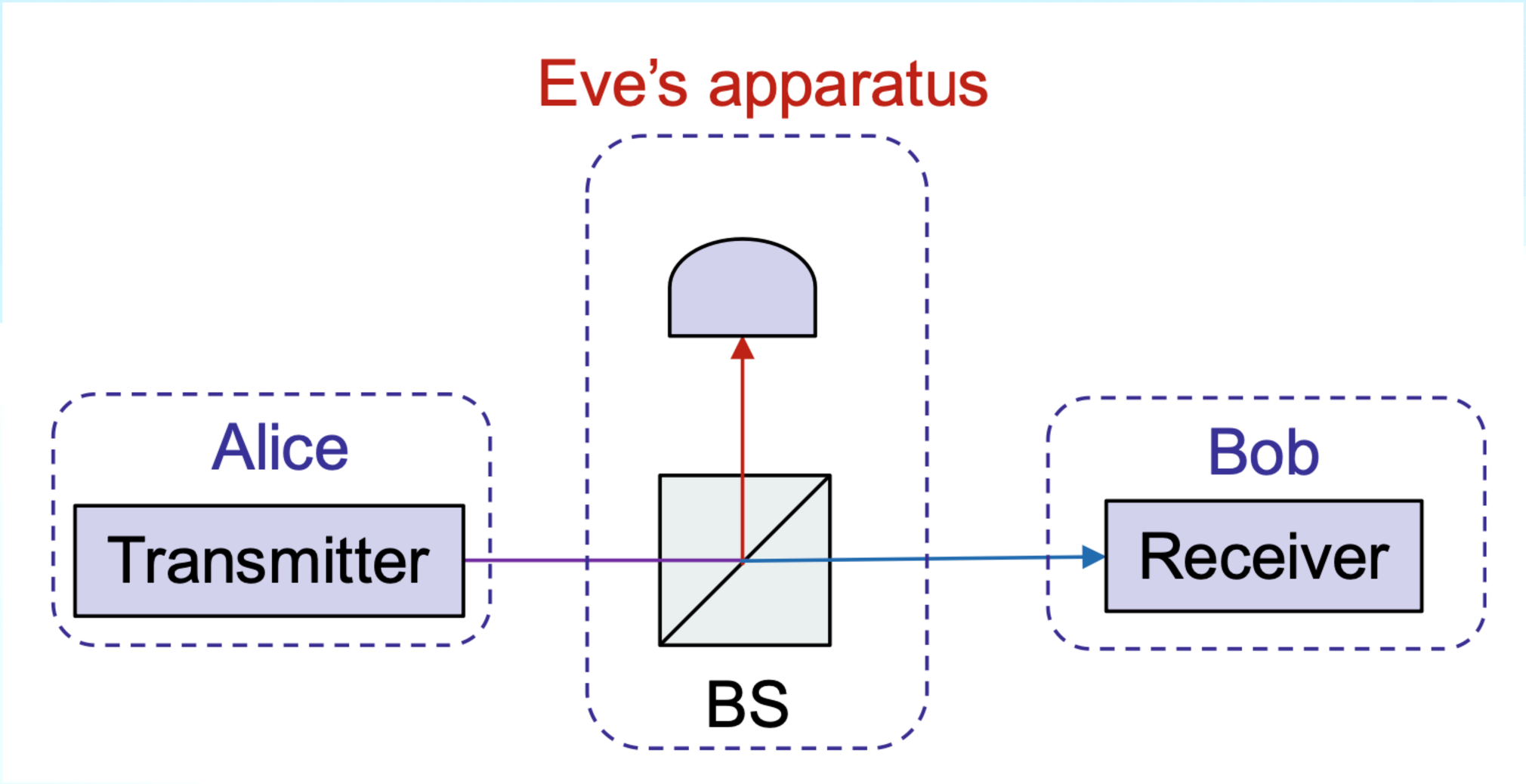
Single photon

Two photons

Schematic for experimental implementation
Polarisation based BB84 protocol



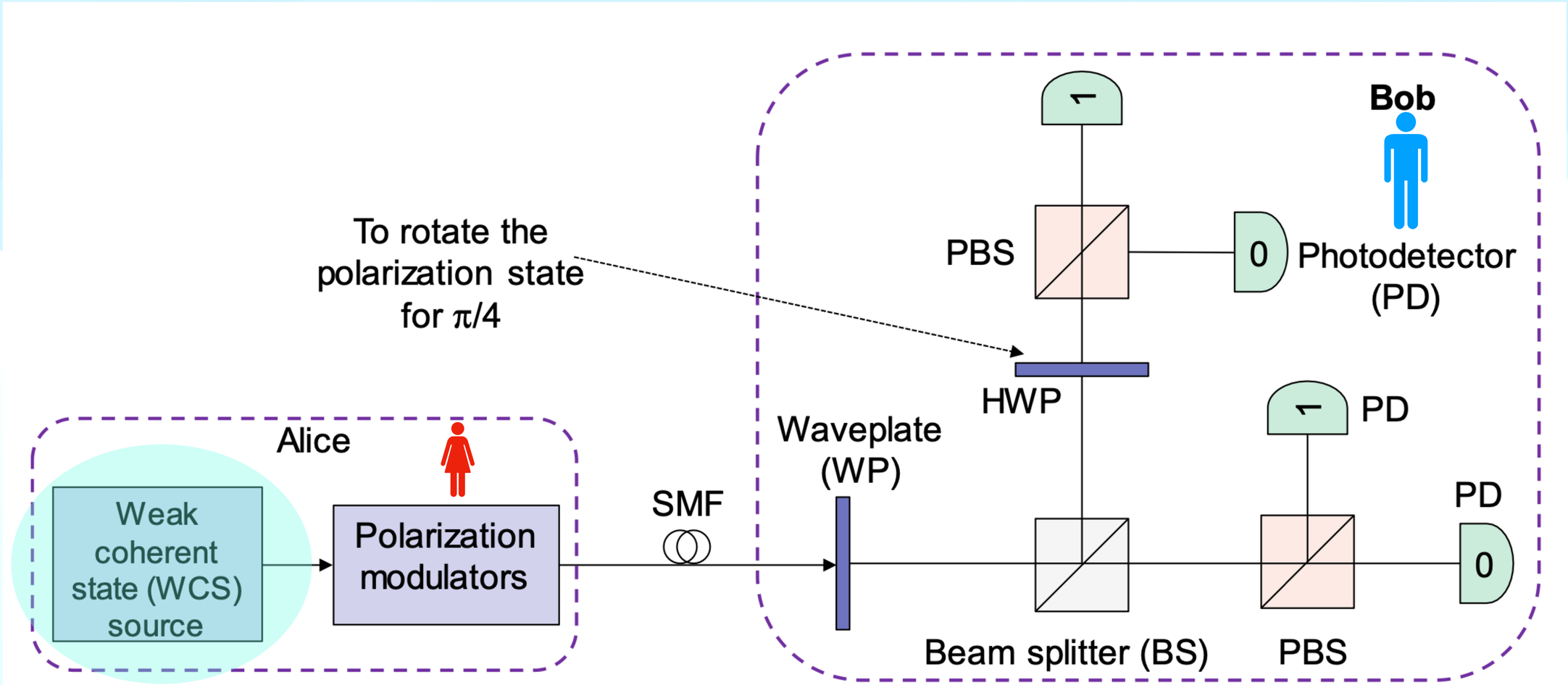
Photon-number-splitting attack



Why is it needed?

To counter photon-number-splitting attack.

Schematic for experimental implementation
Polarisation based BB84 protocol



Why is it needed?

To counter photon-number-splitting attack.

Why is it needed?

To counter photon-number-splitting attack. ?????

Decoy state based QKD protocol: Motivation

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n)\,|n\rangle\langle n| \qquad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}$$

Phase randomised coherent state: $\dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} d\theta\,|\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}|$

`Phase randomised' Weak Coherent pulse based QKD protocol

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n)\,|n\rangle\langle n| \qquad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}$$

$$\mu = \langle n \rangle$$
$$\Delta n^2 = \langle n \rangle = \mu$$

Weak Coherent pulse based QKD protocol

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n)\,|n\rangle\langle n| \qquad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}$$

$$\mu = \langle n \rangle$$
$$\Delta n^2 = \langle n \rangle = \mu$$

$$R^{re}_{BB84} = \frac{1}{2} Q_\mu \left\{ \Omega\left(1 - H_2(E_\mu \Omega^{-1})\right) - f(E_\mu) H_2(E_\mu) \right\}$$

Due to Gottesman-Lo-Lutkenhaus -Preskill

Weak Coherent pulse based QKD protocol

$$\rho_\mu = \sum_{n=0}^{\infty} P_\mu(n)\,|n\rangle\langle n| \qquad P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!}$$

$$\mu = \langle n \rangle$$
$$\Delta n^2 = \langle n \rangle = \mu$$

$$R^{re}_{BB84} = \frac{1}{2} Q_\mu \left\{ \Omega\left(1 - H_2(E_\mu \Omega^{-1})\right) - f(E_\mu) H_2(E_\mu) \right\}$$

Due to Gottesman-Lo-Lutkenhaus -Preskill

Two terms: The gain of the protocol Q_μ and QBER E_μ

A factor due to experimental losses

$$R^{re}_{BB84} = \frac{1}{2} Q_{\mu} \left\{ \Omega \left(1 - H_2(E_{\mu}\Omega^{-1}) \right) - f(E_{\mu}) H_2(E_{\mu}) \right\}$$

A factor due to experimental losses

$$R^{re}_{BB84} = \frac{1}{2} Q_\mu \left\{ \Omega \left(1 - H_2(E_\mu \Omega^{-1}) \right) - f(E_\mu) H_2(E_\mu) \right\}$$

Due to Gottesman-Lo-Lutkenhaus -Preskill

Have presented hand wavingly without the procedure for $f(E_\mu)$.

$Q_\mu f(E_\mu) H_2(E_\mu)$: **Number of bits sacrificed per use after applying error correction to the entire data (generated from both single- and multi photon pulses)**

EC efficiency

$$1 - \Omega = \frac{\sum_{n>1} P_\mu}{Q_\mu}$$

ΩQ_μ : A lower bound for the probability Q_1 that Bob's detector clicks when Alice sends a single-photon state

$\frac{E_\mu}{\Omega} \rightarrow$ An upper bound for the QBER e_1 associated with the detection of the single photon pulses.

Problem: Very hard to obtain a good lower bound on Ω and a good upper bound on e_1.

Problem: Very hard to obtain a good lower bound on Ω and a good upper bound on e_1.

One Solution: prior art methods (as in GLLP) make the most pessimistic assumption that all multiphoton signals emitted by Alice will be received by Bob.

Gottesman, Lo, Lutkenhaus, Preskill

Q_μ: Gain for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$

(The random mixture $|\sqrt{\mu}e^{i\theta}\rangle$ randomised over all values of θ.)

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}\frac{\mu^2}{2} + \cdots + Y_n e^{-\mu}\frac{\mu^n}{n!} + \cdots$$

The QBER E_μ for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$

$$Q_\mu E_\mu = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu}\mu e_1 + Y_2 e^{-\mu}(\mu^2/2) e_2 + \cdots + Y_n e^{-\mu}(\mu^n/n!) e_n + \cdots$$

Q_μ	success probability of click at Bob's detector when triggered by Alice's pulse. (For a given WCP of μ)	measured experimentally

Q_μ	success probability of click at Bob's detector when triggered by Alice's pulse. (For a given WCP of μ)	measured experimentally
E_μ	QBER overall error affecting the detection.	Calculated during the protocol

Q_μ	success probability of click at Bob's detector when triggered by Alice's pulse. (For a given WCP of μ)	measured experimentally
E_μ	QBER overall error affecting the detection.	Calculated during the protocol
e_n	the error rate of Bob's detection events for n photon pulse.	To be calculated theoretically

Q_μ	success probability of click at Bob's detector when triggered by Alice's pulse. (For a given WCP of μ)	measured experimentally
E_μ	QBER overall error affecting the detection.	Calculated during the protocol
e_n	the error rate of Bob's detection events for n photon pulse.	To be calculated theoretically
Y_n	the yield of n photon signal.	To be calculated theoretically
Y_0	detection events due to background including dark counts and stray light from timing pulses.	measured experimentally

Q_μ	success probability of click at Bob's detector when triggered by Alice's pulse. (For a given WCP of μ)	measured experimentally
E_μ	QBER overall error affecting the detection.	Calculated during the protocol
$\Omega \equiv \frac{Q_1}{Q_\mu}$	Fraction of Bob's detection events corresponding to single-photon pulses emitted by Alice.	To be bounded

Q_μ	success probability of click at Bob's detector when triggered by Alice's pulse. (For a given WCP of μ)	measured experimentally
E_μ	QBER overall error affecting the detection.	Calculated during the protocol
$\Omega \equiv \frac{Q_1}{Q_\mu}$	Fraction of Bob's detection events corresponding to single-photon pulses emitted by Alice. $Q_1 = Y_1 e^{-\mu} \mu$	To be bounded

Q_μ	success probability of click at Bob's detector when triggered by Alice's pulse. (For a given WCP of μ)	measured experimentally
E_μ	QBER overall error affecting the detection.	Calculated during the protocol
$\Omega \equiv \frac{Q_1}{Q_\mu}$	Fraction of Bob's detection events corresponding to single-photon pulses emitted by Alice. $Q_1 = Y_1 e^{-\mu}\mu$	To be bounded
$\frac{E_\mu}{\Omega}$	An upper bound for the QBER e_1 associated with the detection of the single photon pulses.	To be bounded

Q_μ: Gain for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$

(The random mixture $|\sqrt{\mu}e^{i\theta}\rangle$ randomised over all values of θ.)

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}\frac{\mu^2}{2} + \cdots + Y_n e^{-\mu}\frac{\mu^n}{n!} + \cdots$$

The QBER E_μ for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$

$$Q_\mu E_\mu = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu}\mu e_1 + Y_2 e^{-\mu}(\mu^2/2) e_2 + \cdots + Y_n e^{-\mu}(\mu^n/n!) e_n + \cdots$$

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n e^{-\mu}}{n!};$$

$$E_\mu = \frac{1}{Q_\mu}\sum_{n=0}^{\infty} e_n Q_n = \frac{1}{Q_\mu}\sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n e^{-\mu}}{n!}$$

Put a bound on e_n and Y_n

If Alice sends different values of light intensity μ,

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n e^{-\mu}}{n!};$$

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Q_n = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n e^{-\mu}}{n!}$$

Become linearly independent.

Put a bound on e_n and Y_n

If Alice sends different values of light intensity μ,

Control parameter: number of pulses with different μ

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n e^{-\mu}}{n!};$$

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Q_n = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n e^{-\mu}}{n!}$$

Become linearly independent.

Key point of the decoy state idea

- Alice prepares a set of additional states—decoy states, in addition to standard BB84 states.

Key point of the decoy state idea

- Alice prepares a set of additional states—decoy states, in addition to standard BB84 states.
- Those decoy states are used for the purpose of detecting eavesdropping attacks only, whereas the standard BB84 states are used for key generation only.

Key point of the decoy state idea

- Alice prepares a set of additional states—decoy states, in addition to standard BB84 states.
- Those decoy states are used for the purpose of detecting eavesdropping attacks only, whereas the standard BB84 states are used for key generation only.
- Only difference between the decoy state and the standard BB84 states: Their intensities (i.e., their photon number distributions).

Final result: **By measuring the yields and QBER of decoy states, Alice and Bob can obtain reliable bounds to Ω and e_1.**

Nitty gritty details

Assumptions on Alice's capability:

1. **Can prepare phase-randomized coherent states and can turn her power up and down for each signal.**

Tool: standard commercial variable optical attenuators (VOAs).

Question asked last time: variable optical attenuator??

THORLABS Products Rapid Order Services Company Contact Us

Overview | Specs | Power Lock | Pin Diagrams | Custom Capabilities | Feedback

Features

- Wavelength Range Options:
  - 780 nm to 980 nm
  - 1250 nm to 1625 nm
- Maximum Attenuation Greater than 25 dB Using MEMS-Based Approach
- Input Power up to 200 mW
- In-Line Fiber Optic Power Monitor with Calibrated Reading Displayed
- Power Lock Mode Stabilizes Output When Desired
- Li-Ion Rechargeable Battery with 300 hour Lifetime from Full Charge

Thorlabs' Electronic Variable Optical Attenuators (EVOAs) offer in-line tabletop control of the optical power in a single mode optical fiber, including the ability to lock the optical output power at a user-defined level. These EVOAs provide attenuation of up to at least 25 dB, which can be continuously tuned using either a rotary knob or an external control voltage applied via an SMA connector (maximum frequency of 1 kHz). To attenuate the light, an internal MEMS mirror adjusts the coupling ratio between the input and output fibers. The output power is displayed on the front in mW.

Click for Details

When Power Lock is active, the indicator LED next to the lock button blinks green.

EVOA Quick Links		
Item #	**Wavelength Range**	**Connector**
EVOA800A	780 - 980 nm	FC/APC
EVOA800F		FC/PC
EVOA1550A	1250 - 1625 nm	FC/APC
EVOA1550F		FC/PC

Fiber Optic Attenuator Selection Guide	
SM	Electronic VOAs for System Integration
	Tabletop EVOAs with Power Lock
	Manually Variable Attenuators
	Fixed-Value Attenuators
MM	Fixed-Value Attenuators
	Manually Variable Attenuators
PM	Electronic VOAs for System Integration
	Manually Variable Attenuators

The displayed output power is calculated from the signal read from a low-percentage internal optical tap and wavelength-specific calibration settings. The wavelength selector knob, shown in the photo to the right, is used to choose among one user-calibrated and two factory-calibrated settings. The factory-calibrated settings correspond to 785 nm and 852 nm for the EVOA800 models and 1310 nm and 1550 nm for the EVOA1550 models. The user can also calibrate for any wavelength within the operating range of the EVOA by using a single mode laser, an accurate power meter, and the trimpot on the side utility panel, shown in the photo below. The procedure is described in Section 4.4 of the manuals for the EVOA800 models and EVOA1550 models, and the user's custom calibration setting is accessed by turning the wavelength selector knob to USER.

These EVOAs are designed for use with optical fiber that is single mode within the operating range of the EVOA, and either FC/APC or FC/PC connectors are accepted. An example of single mode optical fiber that may be used with the EVOA800 models is 780HP, while SMF-28 is an option for the EVOA1550 models. For ease of operation, our EVOAs are powered by a Li-ion battery that typically lasts up to 300 hours from a full charge. This battery can be recharged using a USB mini-B connector or the included 5 V power adapter.

Nitty gritty details:

Assumptions on Alice's capability:

1. Can prepare phase-randomized coherent states and can turn her power up and down for each signal.

   Tool: standard commercial variable optical attenuators (VOAs).

2. Can prepare any Poissonian (with parameter μ) mixture of photon number states.

Nitty gritty details:

Assumptions on Alice's capability:

1. Can prepare phase-randomized coherent states and can turn her power up and down for each signal
   Tool: standard commercial variable optical attenuators (VOAs).

2. Can prepare any Poissonian (with parameter μ) mixture of photon number states.
3. Can vary the parameter, μ, for each individual signal.

Essence of the decoy state idea

***A* decoy and a signal**: have the same characteristics (wavelength, timing information, etc.).

Eve: cannot distinguish a decoy state from a signal state.

The only piece of information available to Eve: the number of photons in a signal.

The yield, Y_n, and QBER, e_n: can depend on only the photon number, n, but not which distribution (decoy or signal) the state is from.

Essence of the decoy state idea

$$Y_n(\text{signal}) = Y_n(\text{decoy}) = Y_n$$

$$e_n(\text{signal}) = e_n(\text{decoy}) = e_n$$

Detector’s behaviour does not depend on incident light’s mean photon number.

The protocol

Assumption: Alice will pick an infinite number of possible intensities (all non- negative values of μ) for decoy states.

Purpose served: Alice and Bob can experimentally measure the yield Q_μ and the QBER E_μ.

The protocol

Assumption: Alice will pick an infinite number of possible intensities (all non- negative values of μ) for decoy states.

Purpose served: Alice and Bob can experimentally measure the yield Q_μ and the QBER E_μ.

Relations between the variables $Q'_\mu s$ and $Y'_n s$ and between $E'_\mu s$ and $e'_n s$: linear.

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n e^{-\mu}}{n!};$$

$$E_\mu = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Q_n = \frac{1}{Q_\mu} \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n e^{-\mu}}{n!}$$

$\{Q'_\mu s\}$ and $\{E'_\mu s\}$ measured from their experiments $\Longrightarrow$ $\{Y'_n s\}$ and $\{e'_n s\}$.

Alice and Bob can constrain simultaneously the yields, Y_n, and QBER, e_n, simultaneously for *all* n.

Assumption: Alice will pick an infinite number of possible intensities (all non- negative values of μ) for decoy states.

Purpose served: Alice and Bob can experimentally measure the yield Q_μ and the QBER e_μ.

Relations between the variables $Q'_\mu s$ and $Y'_n s$ and between $E'_\mu s$ and $e'_n s$: linear.

$\{Q'_\mu s\}$ and $\{E'_\mu s\}$ measured from their experiments $\Longrightarrow$ $\{Y'_n s\}$ and $\{e'_n s\}$.

Alice and Bob can constrain simultaneously the yields, Y_n, and QBER, e_n, simultaneously for *all* n.

Suppose Alice and Bob know their channel property well (Well characterised channel).

Assumption: Alice will pick an infinite number of possible intensities (all non- negative values of μ) for decoy states.

Purpose served: Alice and Bob can experimentally measure the yield Q_μ and the QBER e_μ.

Relations between the variables $Q'_\mu s$ and $Y'_n s$ and between $E'_\mu s$ and $e'_n s$: linear.

$\{Q'_\mu s\}$ and $\{E'_\mu s\}$ measured from their experiments $\Longrightarrow$ $\{Y'_n s\}$ and $\{e'_n s\}$.

Alice and Bob can constrain simultaneously the yields, Y_n, and QBER, e_n, simultaneously for *all* n.

Assumption: Alice and Bob know their channel property well (Well characterised channel).

Acceptable range of values of Y_n's and e_n's: known.

Any attack by Eve that will change the value of any one of the Y_n's and e_n's substantially will, in principle, be caught with high probability by our decoy state method.

Therefore, in order to avoid being detected, the eavesdropper, Eve, has very limited options in her eavesdropping attack.

Yield

In the absence of eavesdropping

(a) $n = 0$: Y_0 : given by the background detection event rate p_{dark} of the system.

Yield

In the absence of eavesdropping

(a) $n = 0$: Y_0 : given by the background detection event rate p_{dark} of the system.

(b) $n \geq 1$. Y_n : Two sources — (i) the detection of signal photons η_n and (ii) the background event p_{dark}.

$$Y_n = \eta_n + p_{\text{dark}} - \eta_n p_{\text{dark}}$$

10^{-3} 10^{-5} 10^{-8}

η : overall transmission probability of each photon.

Yield

In the absence of eavesdropping

(a) $n = 0$: Y_0 : given by the background detection event rate p_{dark} of the system.

(b) $n \geq 1$. Y_n : Two sources — (i) the detection of signal photons η_n and (ii) the background event p_{dark}.

$$Y_n = \eta_n + p_{\text{dark}} - \eta_n p_{\text{dark}} \approx \eta_n + p_{\text{dark}}$$

10^{-3} 10^{-5}

η : overall transmission probability of each photon.

Yield

In the absence of eavesdropping

(a) $n = 0$: Y_0 : given by the background detection event rate p_{dark} of the system.

$$Y_n \approx \eta_n + p_{\text{dark}}$$

η : overall transmission probability of each photon.

Normal channel: independence between the behaviors of the *n photons*.

η_n : transmission efficiency for *n*-photon signals

$$\eta_n = 1 - (1 - \eta)^n$$

$1 - \eta$ Probability of no transmission

For a small η and ignore the dark count $Y_n = n\eta$.

QBER in a realistic experiment:

(a) For $n = 0$, Bob's detection is due to background including dark counts and stray light due to timing pulses.

Assumption: the two detectors have equal background event rates, then the output is totally random and the error rate is 50%.

That is, the QBER for the vacuum $e_0 = 1/2$.

QBER in a realistic experiment

(a) For $n = 0$, Bob's detection is due to background including dark counts and stray light due to timing pulses.

Assumption: that the two detectors have equal background event rates, then the output is totally random and the error rate is 50%.

That is, the QBER for the vacuum $e_0 = 1/2$.

(b) If the signal has $n \geq 1$ photons, it also has some error rate, say e_n.

e_n comes from two parts, erroneous detections and background contribution,

$$e_n = \frac{1}{Y_n}\left(e_{\text{detector}}\eta_n + \frac{1}{2}p_{\text{dark}} \right)$$

where e_{detector} is independent of n.

The values of Y_n and e_n can be experimentally verified by Alice and Bob using our decoy state method. Any attempt by Eve to change them significantly will almost always be caught.

Combining decoy state idea with GLLP

$|\sqrt{\mu}e^{i\theta}\rangle$: *signal state*

Ideal scenario: Alice and Bob can isolate the single-photon signals and apply privacy amplification to them only.

The gain of the signal state,

$$Q_\mu = \sum_{k=0}^{\infty} Y_k e^{-\mu} \frac{\mu^k}{k!}$$

The fraction of Bob's detection events that have originated from single-photon signals emitted by Alice is given by:

$$\Omega = \frac{Q_1}{Q_\mu}.$$

Where

$$Q_1 = Y_1 \mu e^{-\mu}.$$

Assumption: error correction protocols can achieve the fundamental (Shannon) limit. (Trying to understand!)

Just the first of the first

1. Various papers in JOSA on different platforms for QKD and corresponding simulation (graph) parameters.

2. **Control Parameters:** Number of decoy states, their mean photon number