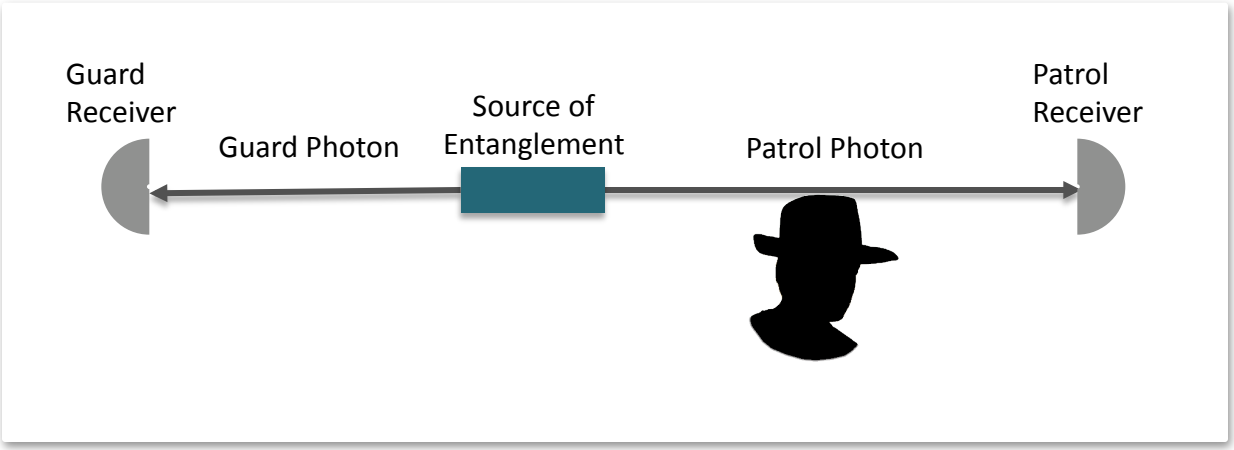
Sensing Intruders Using Entanglement: A Photonic Quantum Fence

Travis Humble, Ryan Bennink, Warren Grice
Oak Ridge National Laboratory

Israel Owens
Los Alamos National Laboratory

We describe the use of quantum-mechanically entangled photons to sense both intrusions and attempts to spoof sensor receivers. We present theoretical arguments and experimental results that demonstrate the principle of entanglement-based detection for a sensor derived from polarization-entangled photon pairs.



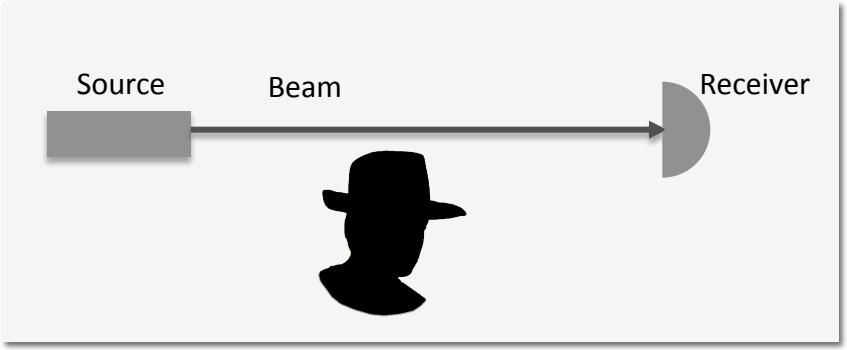
Presented at SPIE Defense Security and Sensing 2009:
Quantum Information and Computation VII

Managed by UT-Battelle
for the Department of Energy

Intercept-resend Attack (Classical)

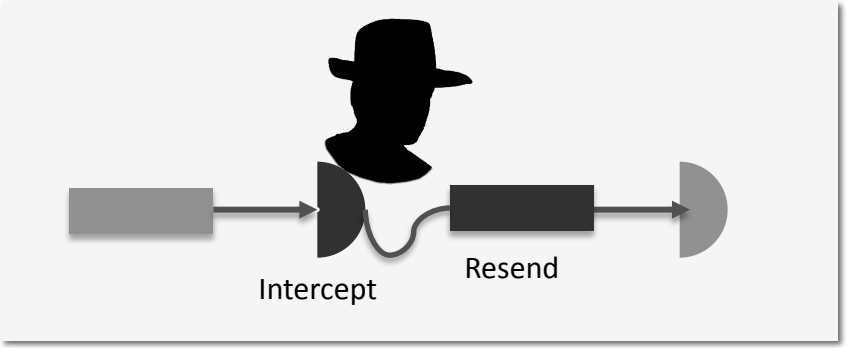
Motivation: A laser tripwire

- *Transmit a beam across a protected boundary*
- *Measure the state of transmitted beam*
  - Classically defined EM field
- *Changes in beam properties signal intrusion*



Problem: Classical information cloned.

- *Measure the state of transmitted beam*
  - Classically defined EM field
- *Resend a perfect replica.*
- *How do you tell the difference?*



Similar situations:

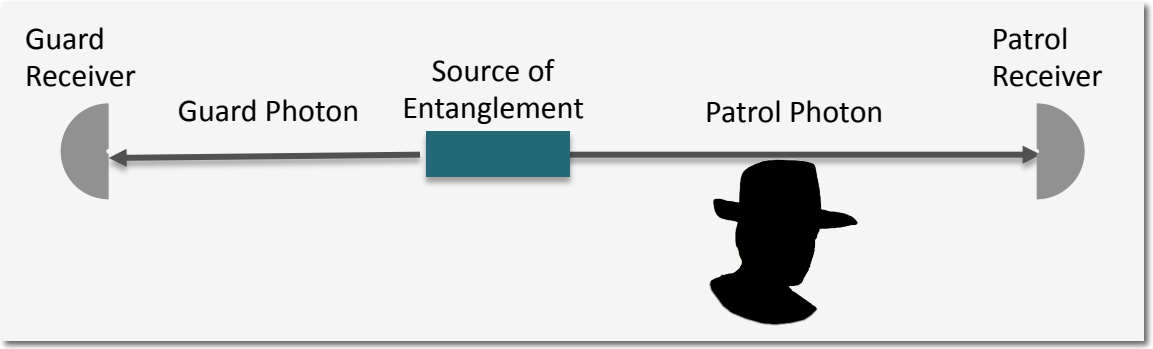
- Fiber communication, containment and surveillance, locks, seals.

Oak Ridge National Laboratory

Entanglement-based Detection

Solution: The no-cloning principle and entanglement

- *No cloning: An arbitrary quantum of information cannot be reliably copied.*
- *Entanglement: Non-local correlations exist between measurement outcomes.*



Transmit, but verify

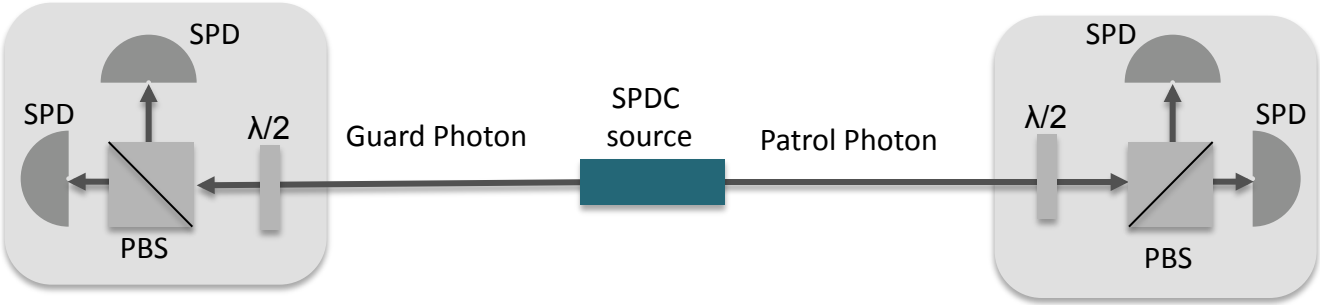
- *Entangled photon pair source distributes patrol and guard photons:*
  - Patrol photon traverses boundary; Guard photon remains secured.
- *Receivers measure local observables, communicate outcome to monitor (alarm)*
- *Monitor validates transmission of entangled photons*
  - Monitor quantifies entanglement

Oak Ridge National Laboratory

Polarization-entangled Photon Pairs

Polarization correlations

- *Local measurements made at patrol and guard receivers, polarization analyzers.*



- *Basis-dependent results – basis choice coordinated by the monitor*

State Prepared

$$|\varphi_{PG}\rangle = \frac{1}{\sqrt{2}}\left(|h_P, v_G\rangle + |v_P, h_G\rangle\right)$$

Statistics Observed

h / v basis: $R_C^{h/v}(\theta_P, \theta_G) = \sin^2(\theta_G + \theta_P)$

+ / – basis: $R_C^{+/-}(\theta_P, \theta_G) = \sin^2(\theta_G + \theta_P + \pi/2)$

Visibility quantifies entanglement $V = \dfrac{R_C^{MAX} - R_C^{MIN}}{R_C^{MAX} + R_C^{MIN}}$

h / v basis: $V^{h/v} = 1$

+ / – basis: $V^{+/-} = 1$

Oak Ridge National Laboratory

Quantifying Sensor Performance

Binary Decision Problem

- *Discriminate between two hypotheses*

Unentangled $V_0 = 0 \quad H_0 : s_i = V_0 + n$ Entangled $V_1 = 1 \quad H_1 : s_i = V_1 + n$

Gaussian random noise with zero mean and variance σ^2

- *Probability for detection and false alarm*

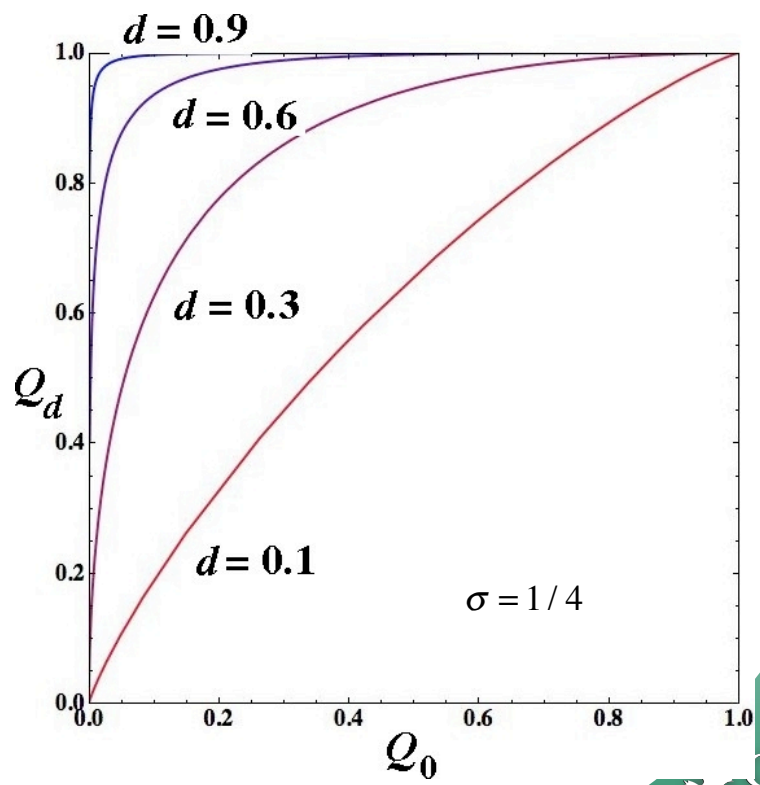
$$Q_d = erfc(x_1) \quad \text{vs.} \quad Q_0 = erfc(x_0)$$

$$erfc(y) \equiv (2\pi)^{-1/2} \int_y^\infty \exp\left[-x^2/2\right] dx$$

$$x_1 = \frac{\ln \lambda}{2} - \frac{d}{2} \qquad x_0 = \frac{\ln \lambda}{d} + \frac{d}{2}$$

Displacement $d = M^{1/2}\left(V_1 - V_0\right)/\sigma$

For threshold λ and M measurements



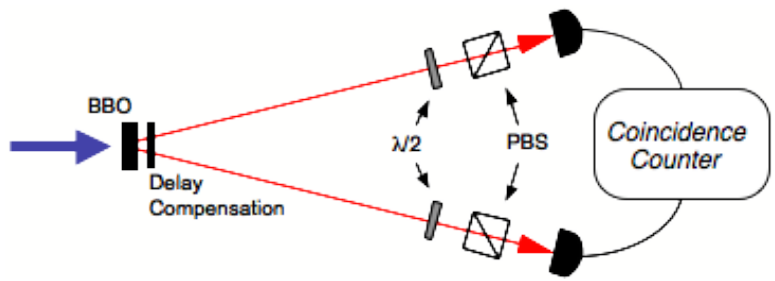
Experiment to Simulate Intrusion

Setup

- *Entanglement source: type-II SPDC cross-ring configuration*

  1-mm BBO cw-pumped at 351.1 nm, degenerate down conversion at 702 nm

  Patrol and guard photons travel 60 cm to polarization analyzers



BBO Beta Barium Borate
PBS Polarization Beam Splitter
λ/2 Half-wave plate

- *Entanglement detection: polarization-correlation visibility*

  Polarization analyzers for h/v and +/– bases, half-wave plate fixes basis

  Single-photon detectors collect transmitted photons

  Coincidence counter monitors statistics, 1-s collection windows

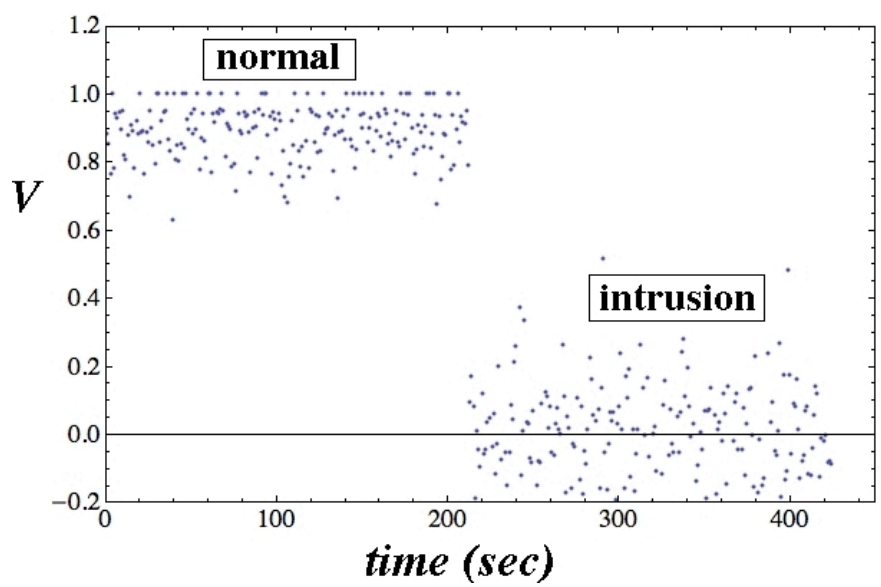
basis	count rate	visibility
h / v	188 pairs/sec	0.98±0.02
+ / –	35 pairs/sec	0.91±0.08

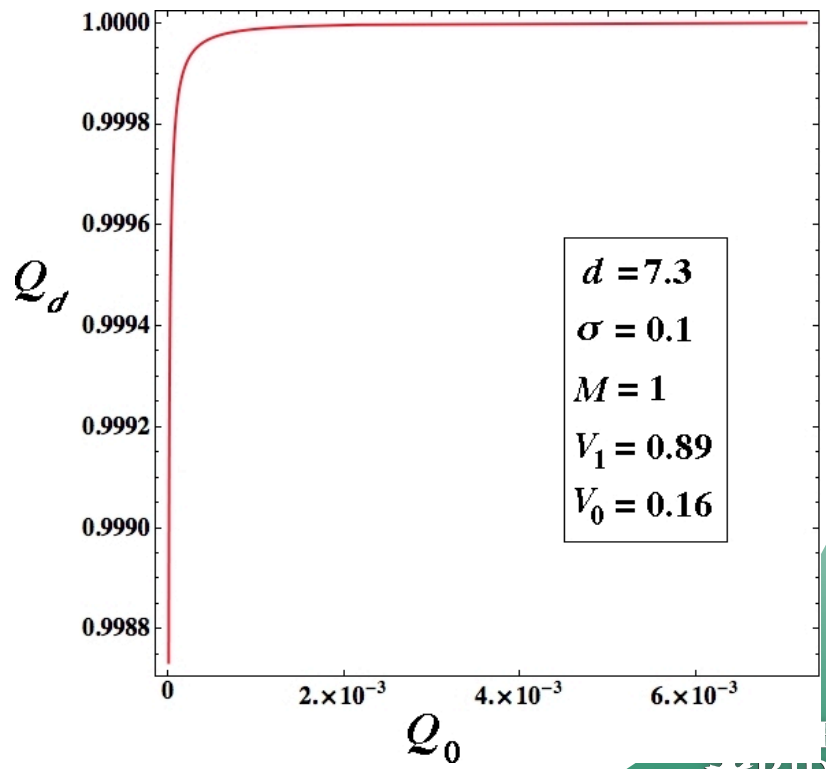
Oak Ridge National Laboratory

Experiment to Simulate Intrusion

Results

- *Acquired two time-series to simulate an intrusion*
  1. Visibility of entangled photons in +/– basis (normal)
  2. Visibility of unentanlged photons in +/– basis (intrusion)
- *Concatenated the times series to simulate an intrusion*





Long-range Performance

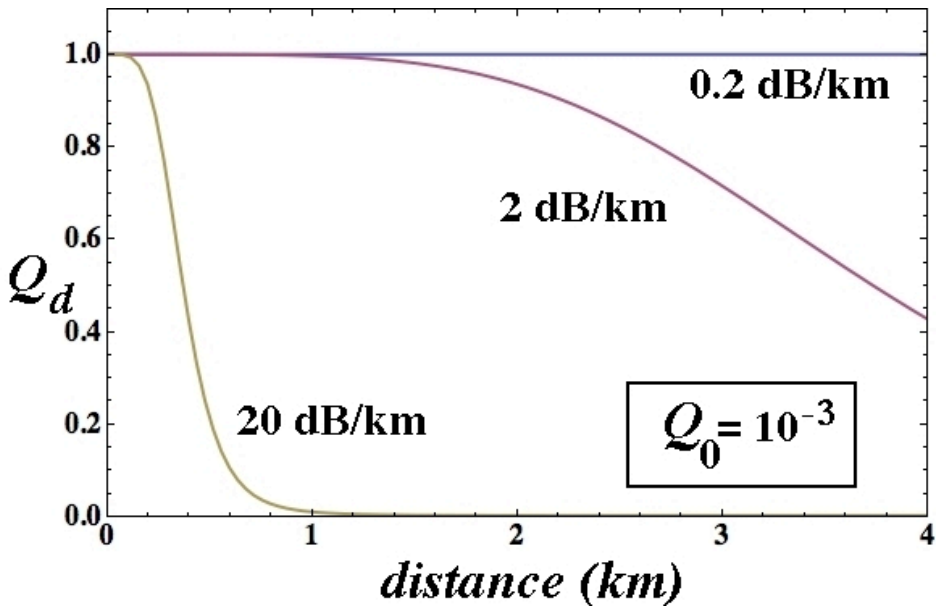
Extrapolate the results

- *Losses from atmospheric attenuation*

  Assume error scales as (count rate)$^{-1/2}$ and count rate scales with range

  Attenuation rates from 0.2 dB/km (clear) to 20 dB/km (fog) at 800 nm

- *Detection probability Q_d for fixed false-alarm rate $Q_0 = 10^{-3}$*



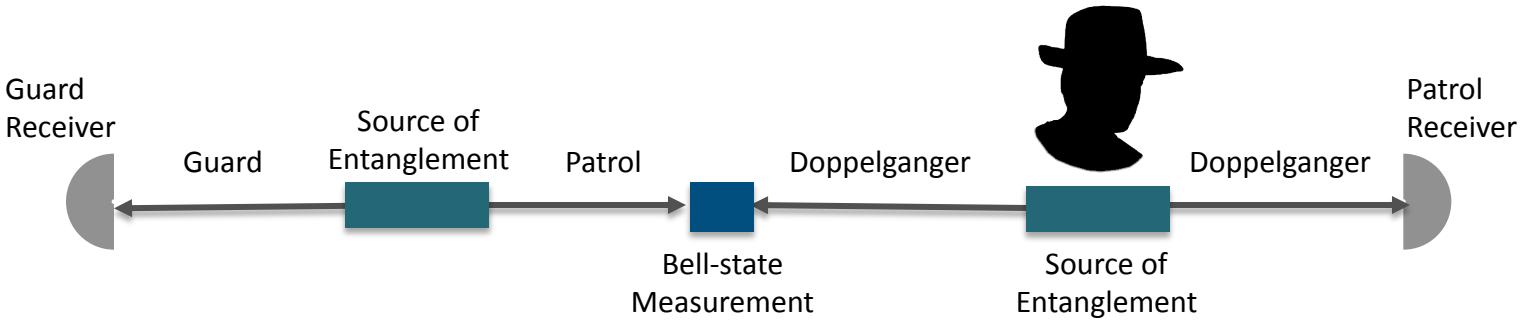
- 0.2 dB/km loss, Q_d > 0.9999 to 3 km.
- 20 dB/km loss, Q_d > 0.999 to 120 m.

Intercept-resend Attack (Quantum)

Quantum teleportation avoids cloning, preserves entanglement

- *Intruder can employ quantum techniques to avoid (classical) information*

  Quantum teleportation of patrol photon state transferred to doppelganger photon.



- *Two caveats*
  1. Required Bell-state measurement has probabilistic success, probabilistic outcome.
  2. Required local corrective action delays transmitted doppelganger

Intercept-resend Counterattack (Quantum)

Impair the quantum teleportation attack

- *Engineer patrol-guard state to exhibit good visibility but to teleport poorly*

  Spectrally multimode, polarization-entangled photons

$$|\varphi_{PG}\rangle = \frac{1}{\sqrt{2}}\int d\omega \int d\omega' \left[f(\omega,\omega')\left|h_P(\omega), v_G(\omega')\right\rangle + g(\omega,\omega')\left|v_P(\omega), h_G(\omega')\right\rangle \right]$$

  Joint spectral probability amplitudes are highly entangled (Schmidt modes)

$$f(\omega,\omega') = \sum_n \lambda_n^{1/2} u_n(\omega) v_n(\omega') \qquad K^{-1} = \sum_n \lambda_n^2$$

  K measures entanglement

- *Polarization-correlation visibility*

Before teleportation attack	$V = 1$
After teleportation attack	$V = K^{-1}$

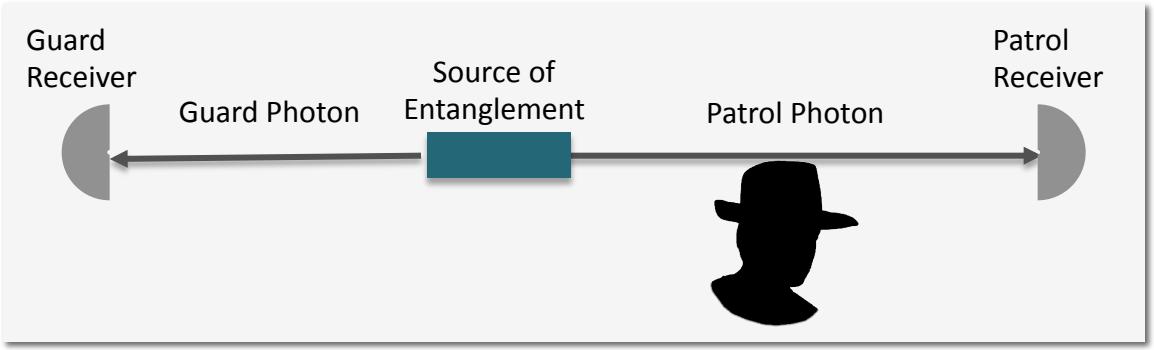
For very large *K*, the visibility vanishes after the intruder attempts teleportation.

Oak Ridge National Laboratory

Concluding Remarks

- A Quantum Fence
  - *Detects intruders and their attempts to spoof the sensor*
  - *Monitors the non-local correlations measured by patrol and guard receivers*
  - *Theoretical and experimental demonstrations of sensor performance*

    High probability of detection at low false-alarm rate for a very modest experiment
  - *Exploits the larger biphoton Hilbert space to 'impair' teleportation*



  - *Does not need to be free space; fiber-based applications also possible.*
  - *Other degrees of freedom of interest.*

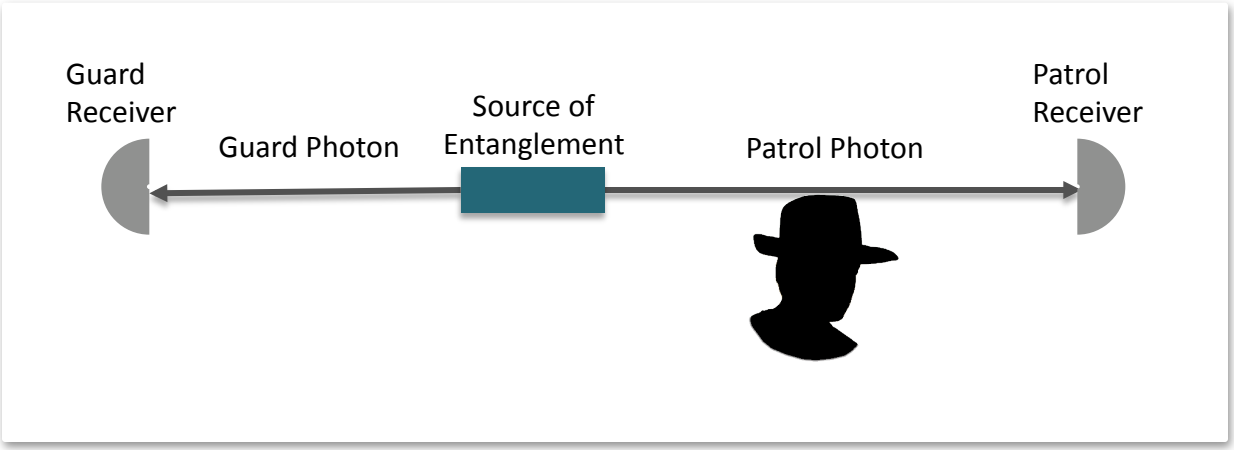
OAK RIDGE National Laboratory

Sensing Intruders Using Entanglement: A Photonic Quantum Fence

Travis Humble, Ryan Bennink, Warren Grice
Oak Ridge National Laboratory

Israel Owens
Los Alamos National Laboratory

We describe the use of quantum-mechanically entangled photons to sense both intrusions and attempts to spoof sensor receivers. We present theoretical arguments and experimental results that demonstrate the principle of entanglement-based detection for a sensor derived from polarization-entangled photon pairs.



Presented at SPIE Defense Security and Sensing 2009:
Quantum Information and Computation VII

Managed by UT-Battelle
for the Department of Energy