Keeping Secrets with Quantum Mechanics

Paul Townsend

Photonic Systems Group

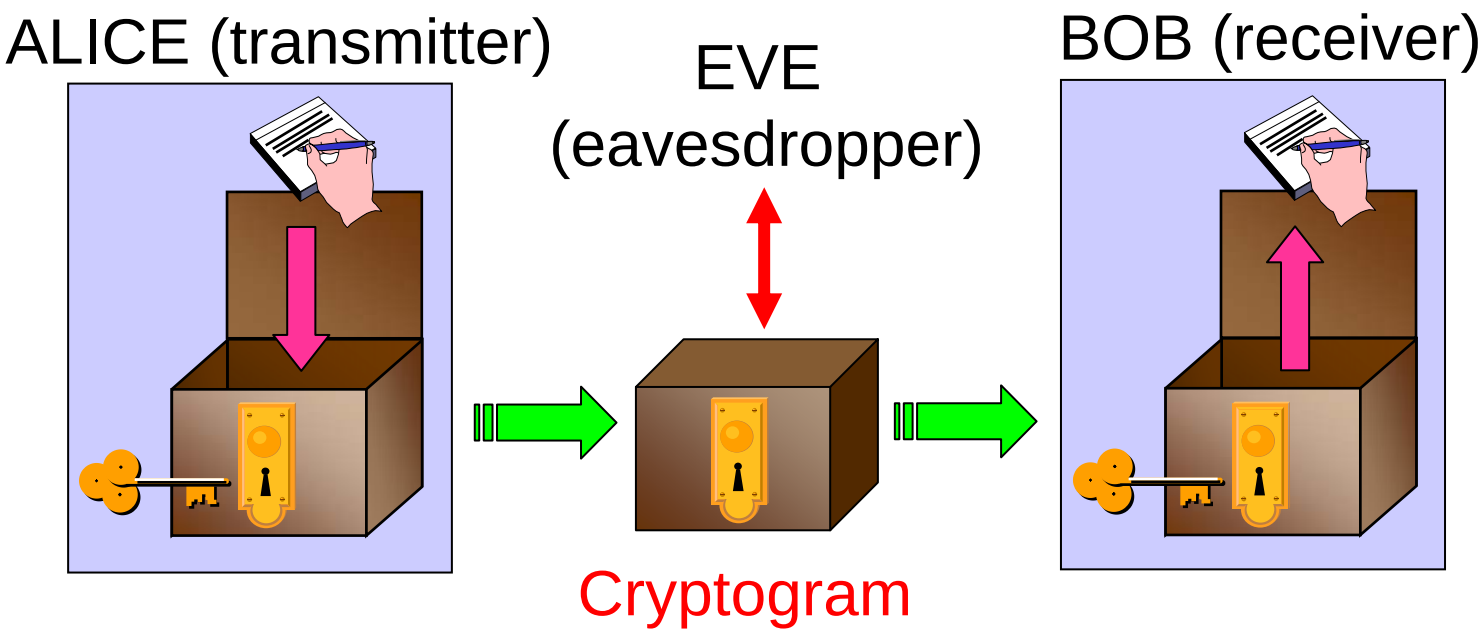
Department of Physics & Tyndall National Institute

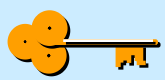
UCC

Access and Quantum Communications Group

- Access Networks
  - Dr Giuseppe Talli (Staff Researcher)
  - Dr Chi Wai Chow (Postdoc – now at Nat. Univ. Taiwan)
  - Eimear MacHale (PhD Student)
  - Cleitus Antony (PhD Student)
  - Paolo Leoni (Erasmus BEng Student – Univ. Padova)
- Quantum Communications
  - Dr Harendra Fernando (Postdoc)
  - Iris Choi (PhD Student)
  - Yiang Liu (visiting PhD Student – Chinese Univ. Hong Kong)
  - Alessandro Biavati (MEng Project Student)

Secret-Key Cryptography

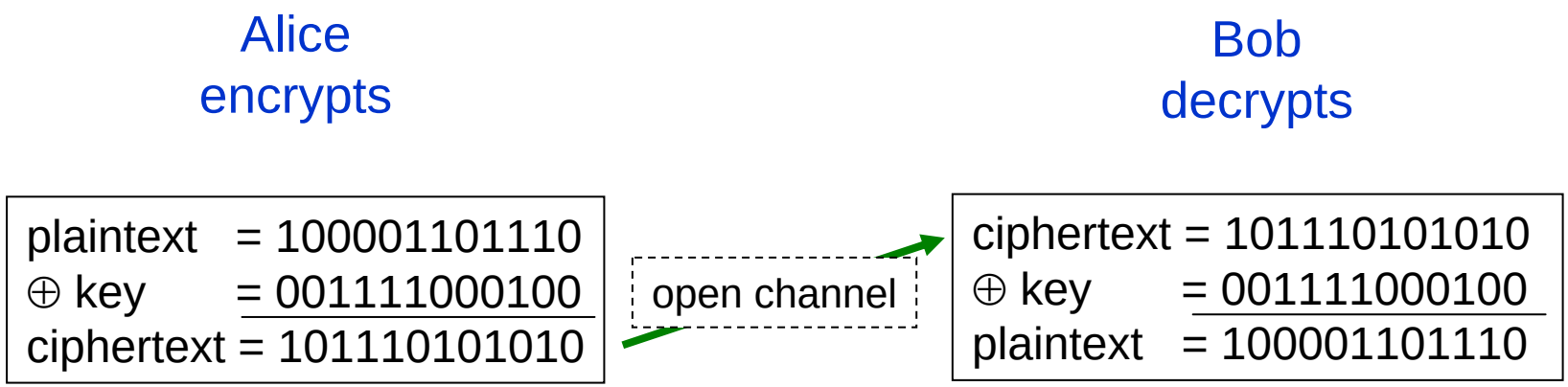


- Communications security is achieved using cryptography (classical)
- A cryptography system has two main elements: a key  & an algorithm 
- The algorithm is a public standard the key is a secret random bit sequence

Perfect secrecy: the “one time pad”

G.S. Vernam, Trans AIEE 45, 295 (1926)

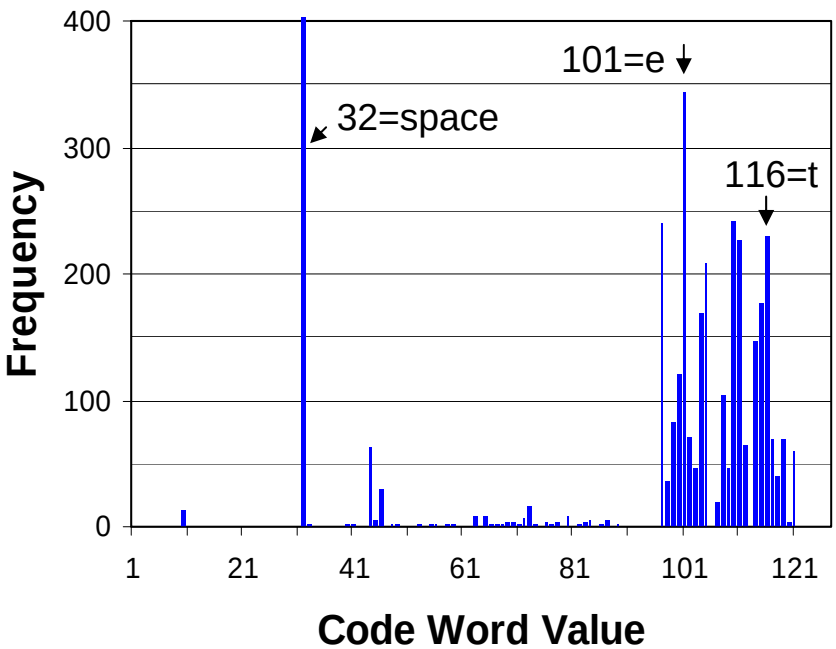
- Key material is a (truly) random bit sequence
- Algorithm is addition (mod 2) = XOR = $\oplus$
- Unconditionally secure provided key is not reused and is as long as the message



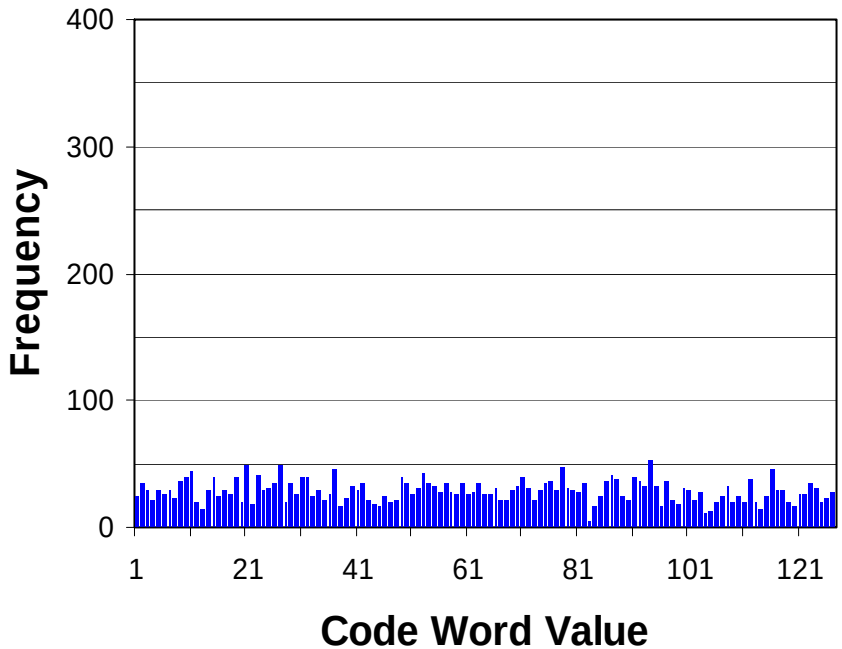
Coding Examples

- Excerpt from War and Peace (Leo Tolstoy)

ASCII Code



ASCII Code + One Time Pad

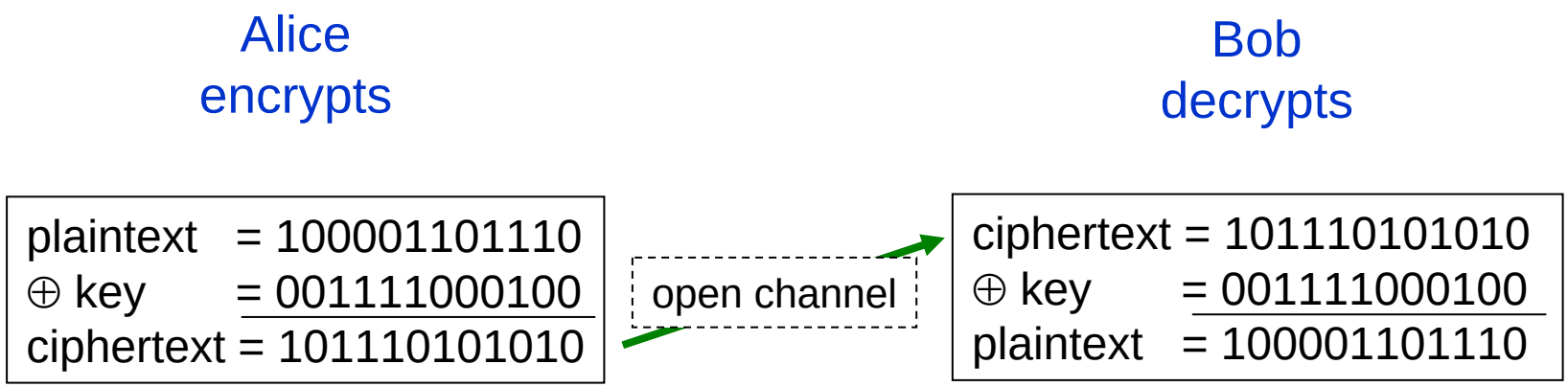


Key = quantum random number

Perfect secrecy: the “one time pad”

G.S. Vernam, Trans AIEE 45, 295 (1926)

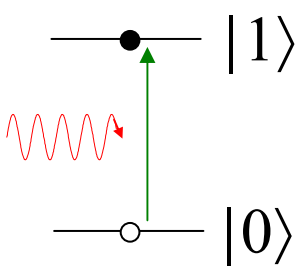
- Key material is a (truly) random bit sequence
- Algorithm is addition (mod 2) = XOR = ⊕
- Unconditionally secure provided key is not reused and is as long as the message

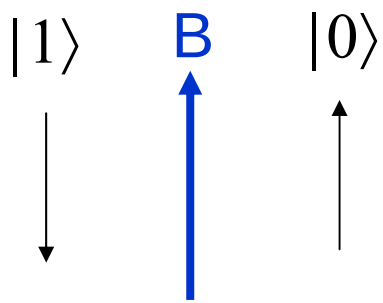


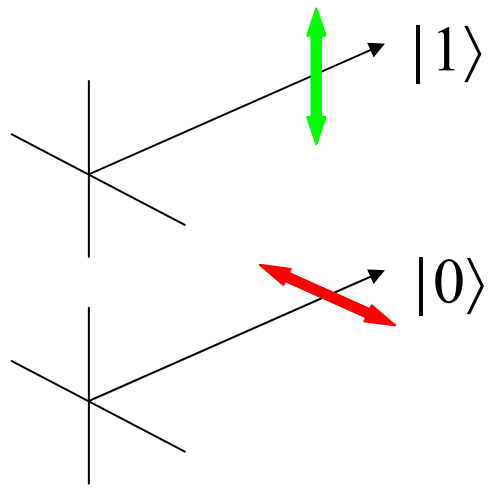
How do Alice and Bob share the key?

Quantum Bits or “qubits”

- A single bit of information can be represented by a two-state quantum system – a “qubit”

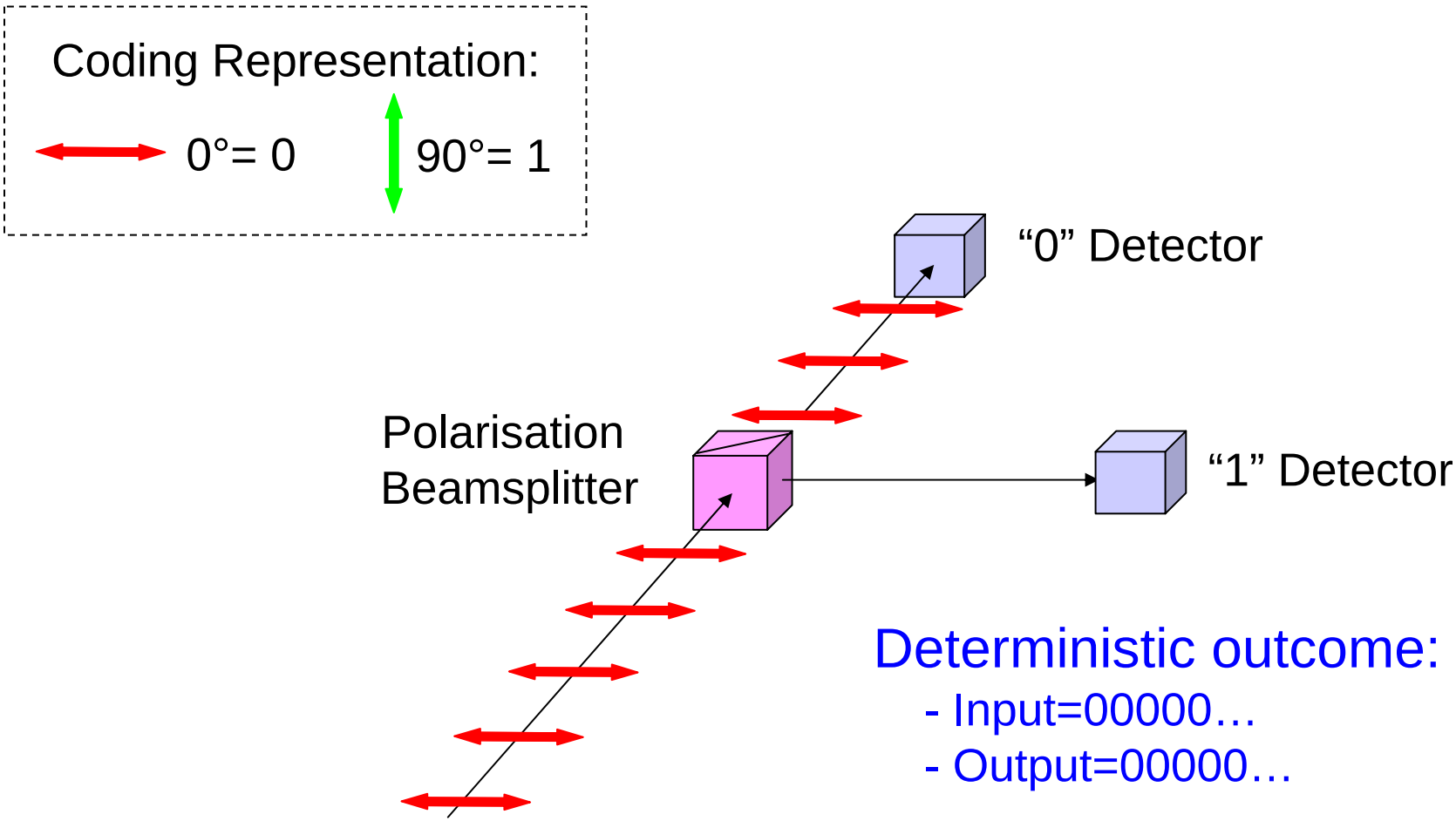






- an atomic electron
- a spin in a magnetic field (B)
- a polarised photon

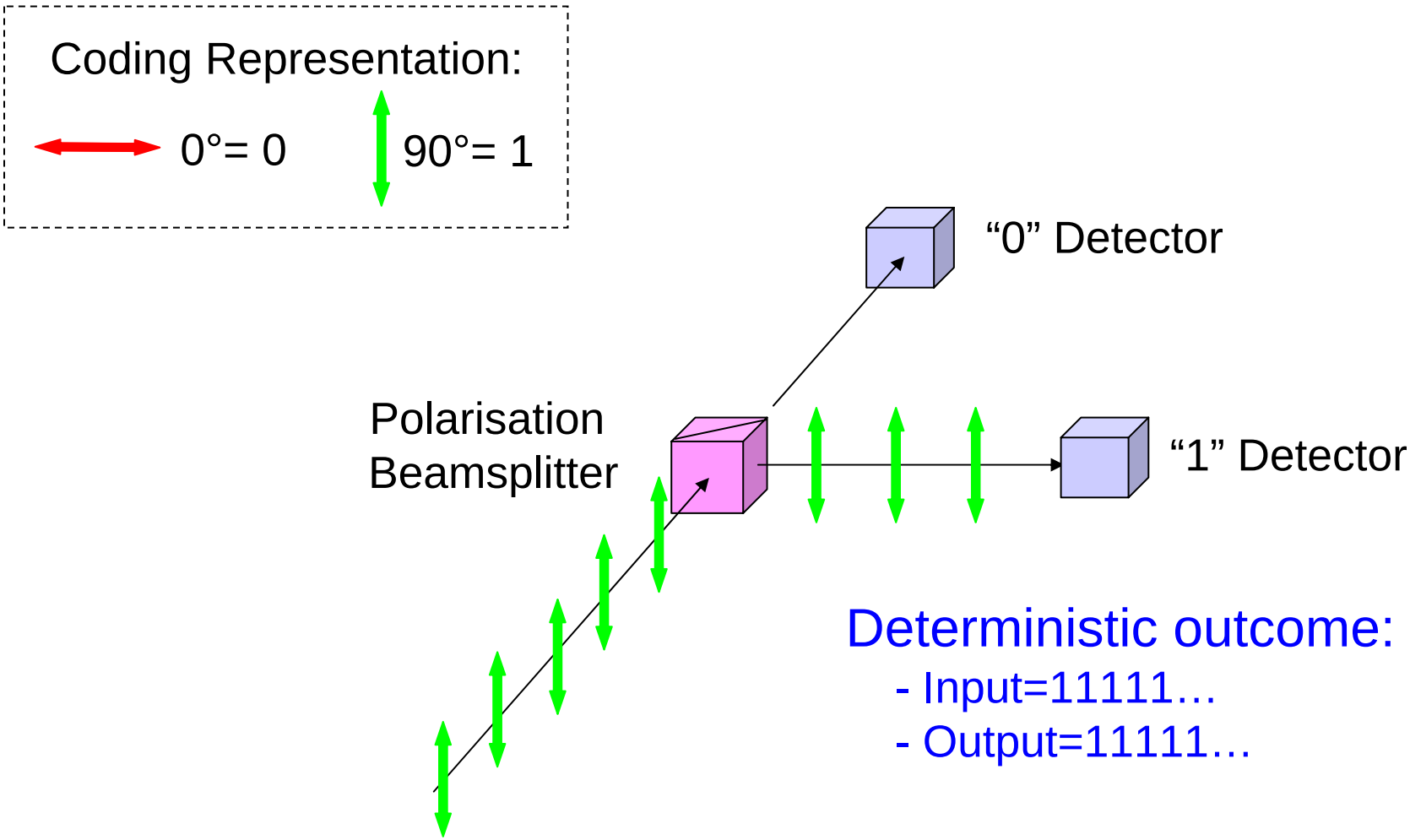
Photon Polarisation Coding and Measurement



Deterministic outcome:

- Input=00000…
- Output=00000…

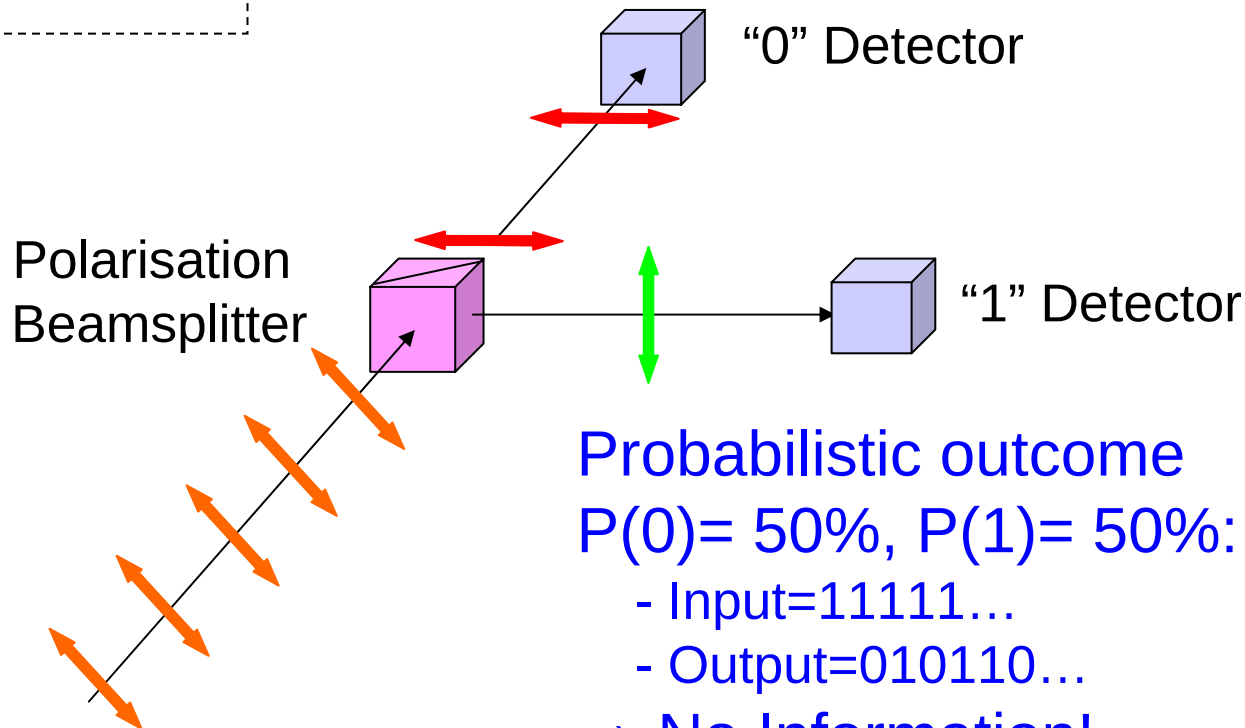
Photon Polarisation Coding and Measurement



Photon Polarisation Coding and Measurement

Coding Representation:

-45°= 0 +45°= 1



Probabilistic outcome

P(0)= 50%, P(1)= 50%:

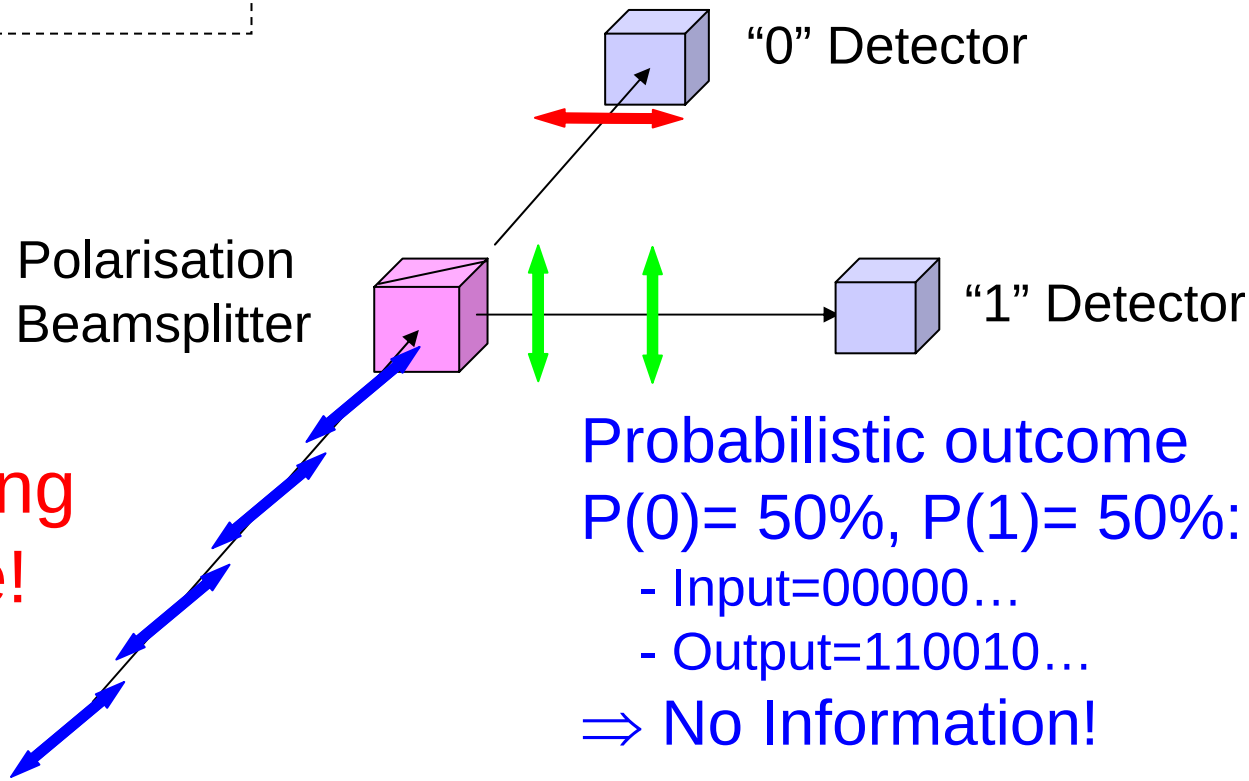
- Input=11111…
- Output=010110…

⇒ No Information!

Photon Polarisation Coding and Measurement

Coding Representation:

-45°= 0 +45°= 1



Perfect copying not possible!

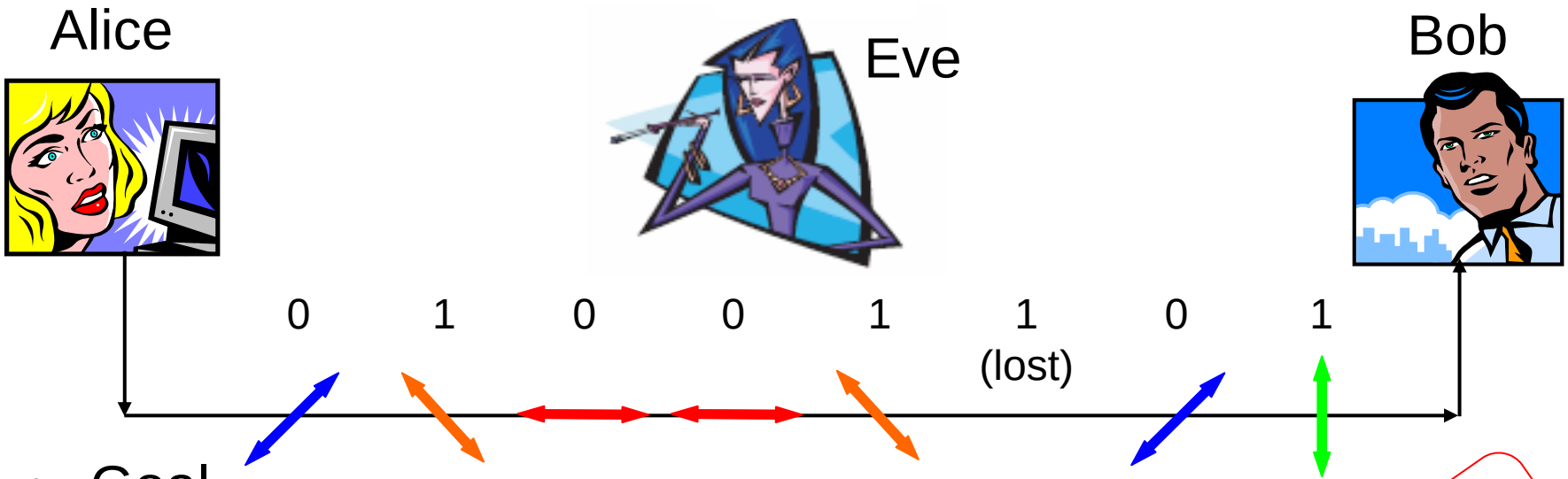
Probabilistic outcome

P(0)= 50%, P(1)= 50%:

- Input=00000…
- Output=110010…

⇒ No Information!

Quantum Cryptography or Quantum Key Distribution (QKD)[1]



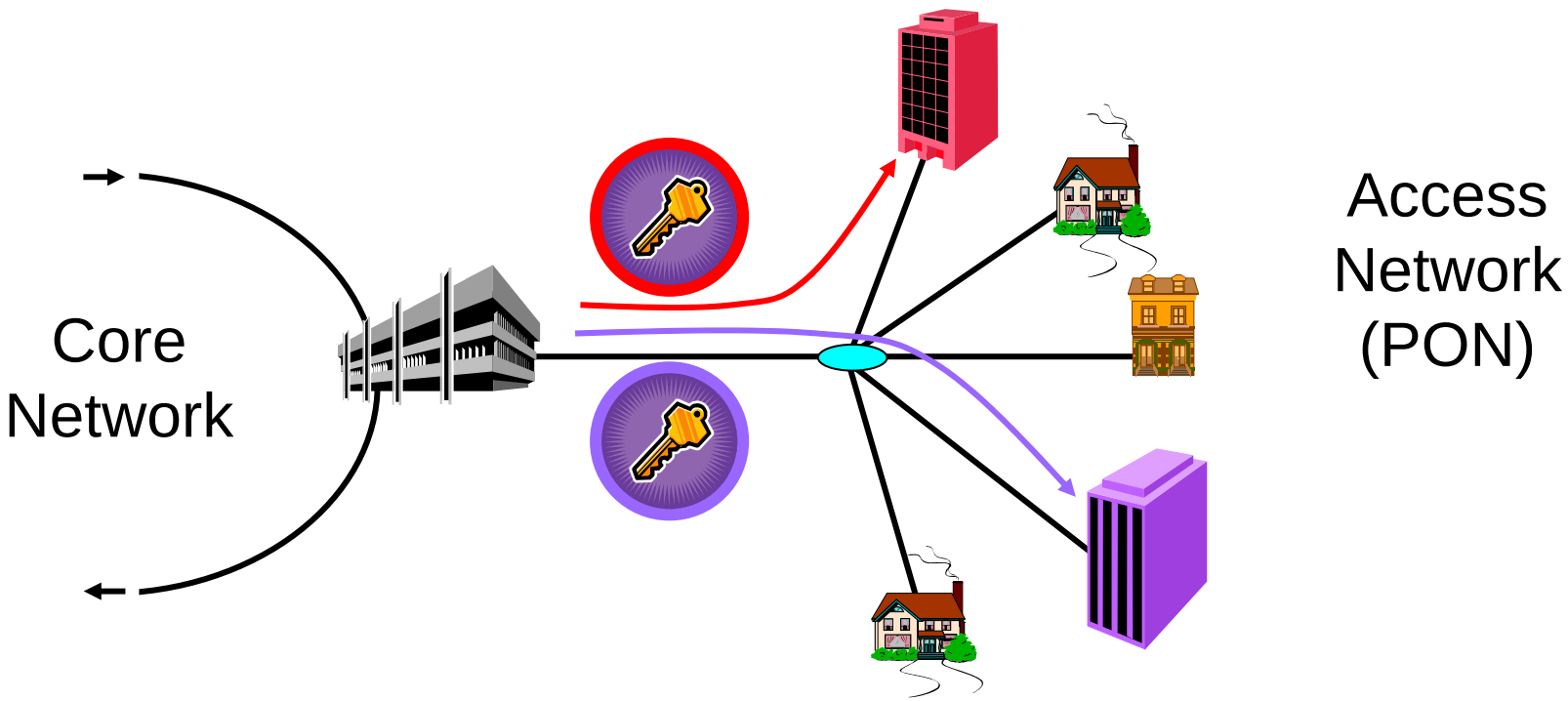
- Goal
  - Share a random bit sequence
  - Test secrecy
  - If secrecy confirmed use as an encryption key
- Method
  - Use non-orthogonal photon polarisation states as qubits
  - Post transmission test for errors = test for Eve
  - If error rate low (<11%) secret key can be generated

Guaranteed by quantum mechanics!

[1] C.H. Bennett and G. Brassard, *Int. Conf. on Comp. Syst. & Sig. Processing*, 175-179 (1984)

System Application: Security on Passive Optical Networks (PONs)

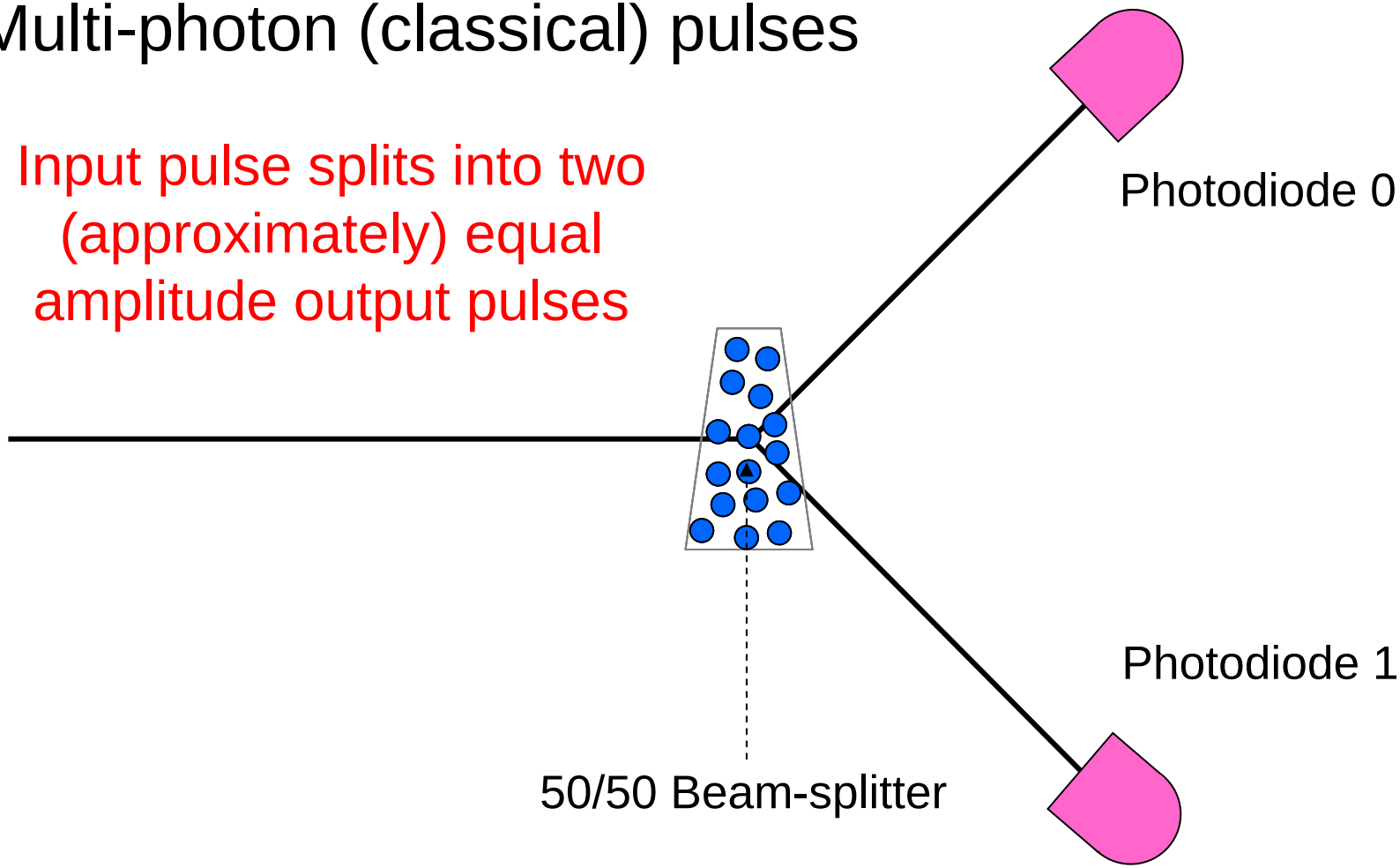
- Can we use QKD?
  - ‘QPON’ design and demonstration (Iris Choi PhD)



Photons and Beamsplitters

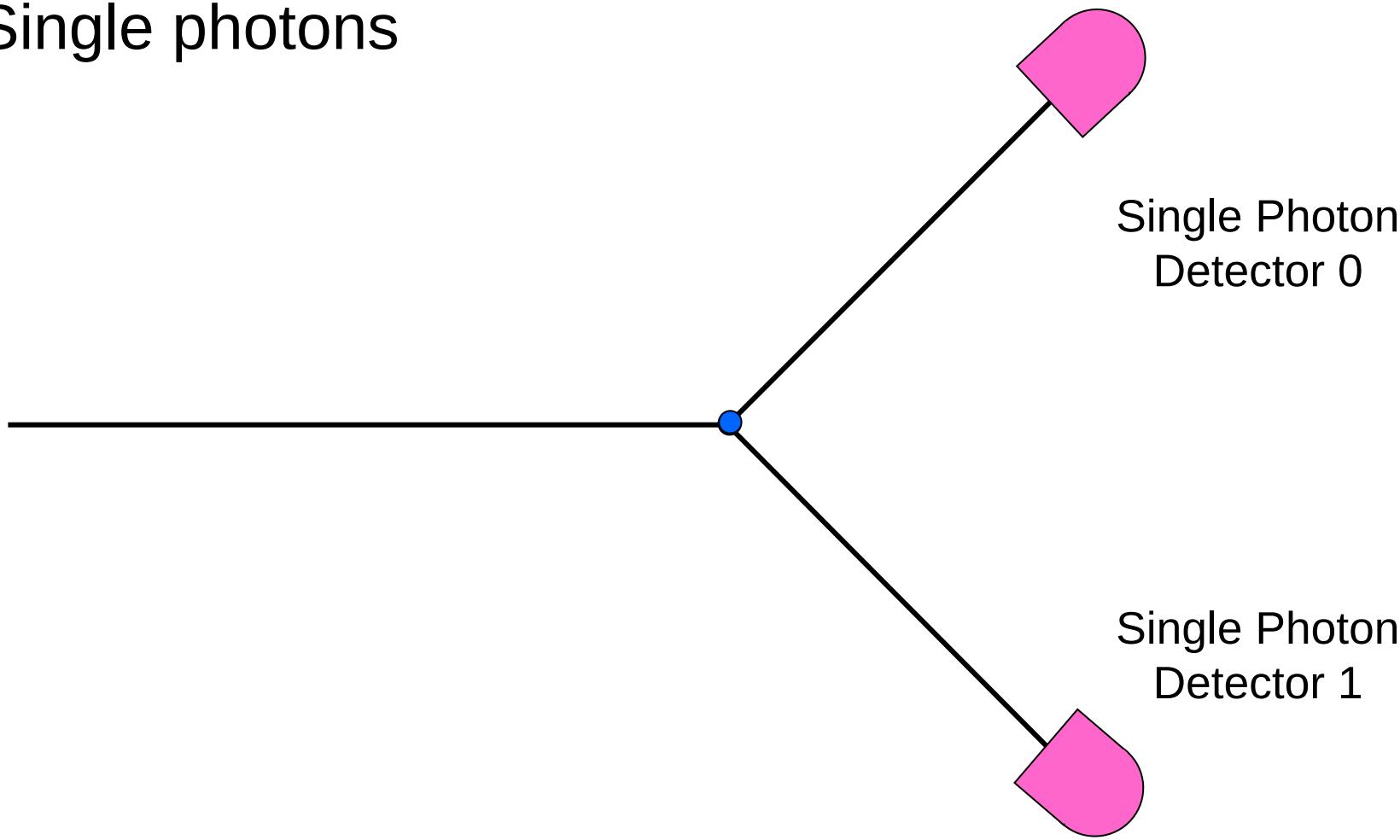
- Multi-photon (classical) pulses

Input pulse splits into two (approximately) equal amplitude output pulses



Photons and Beamsplitters

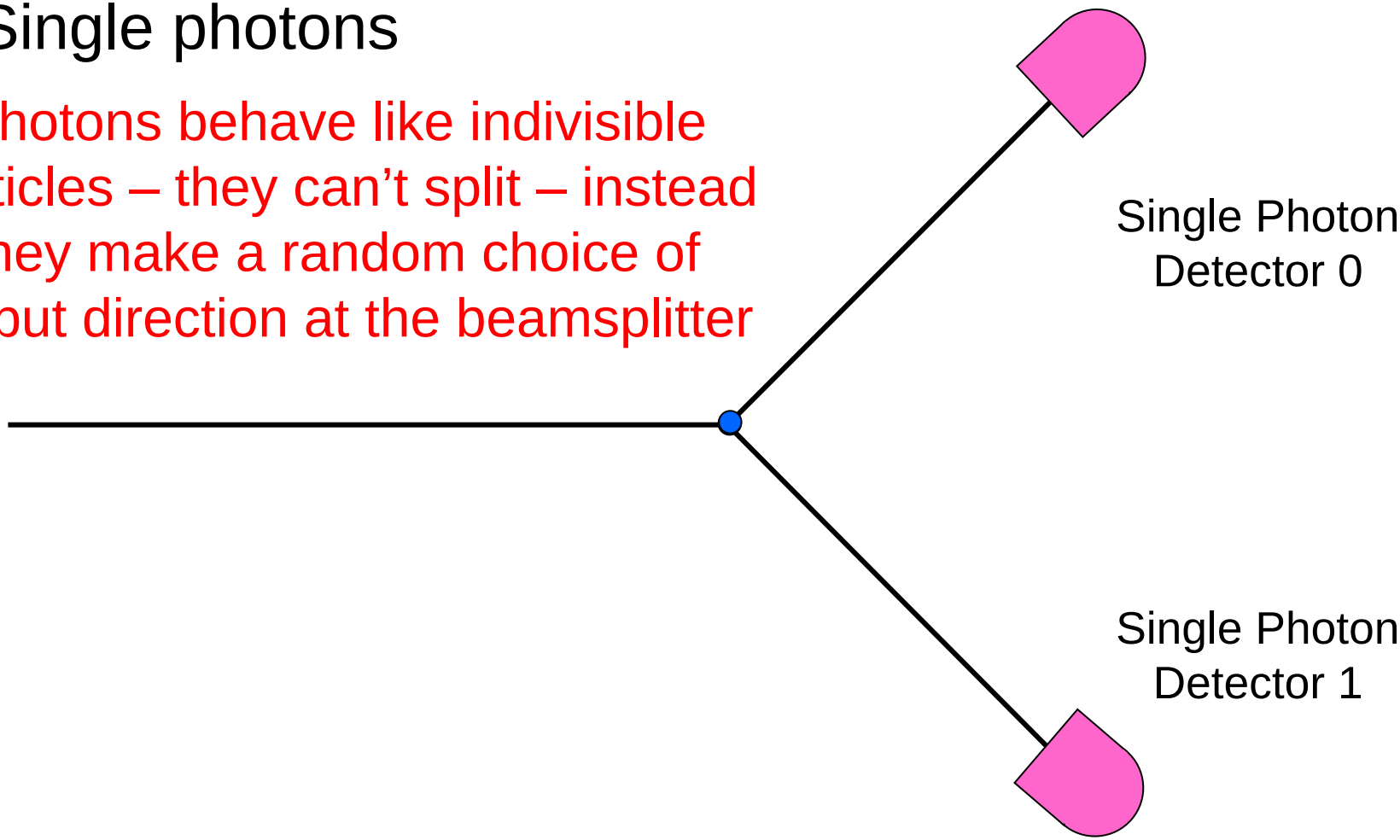
- Single photons



Photons and Beamsplitters

- Single photons

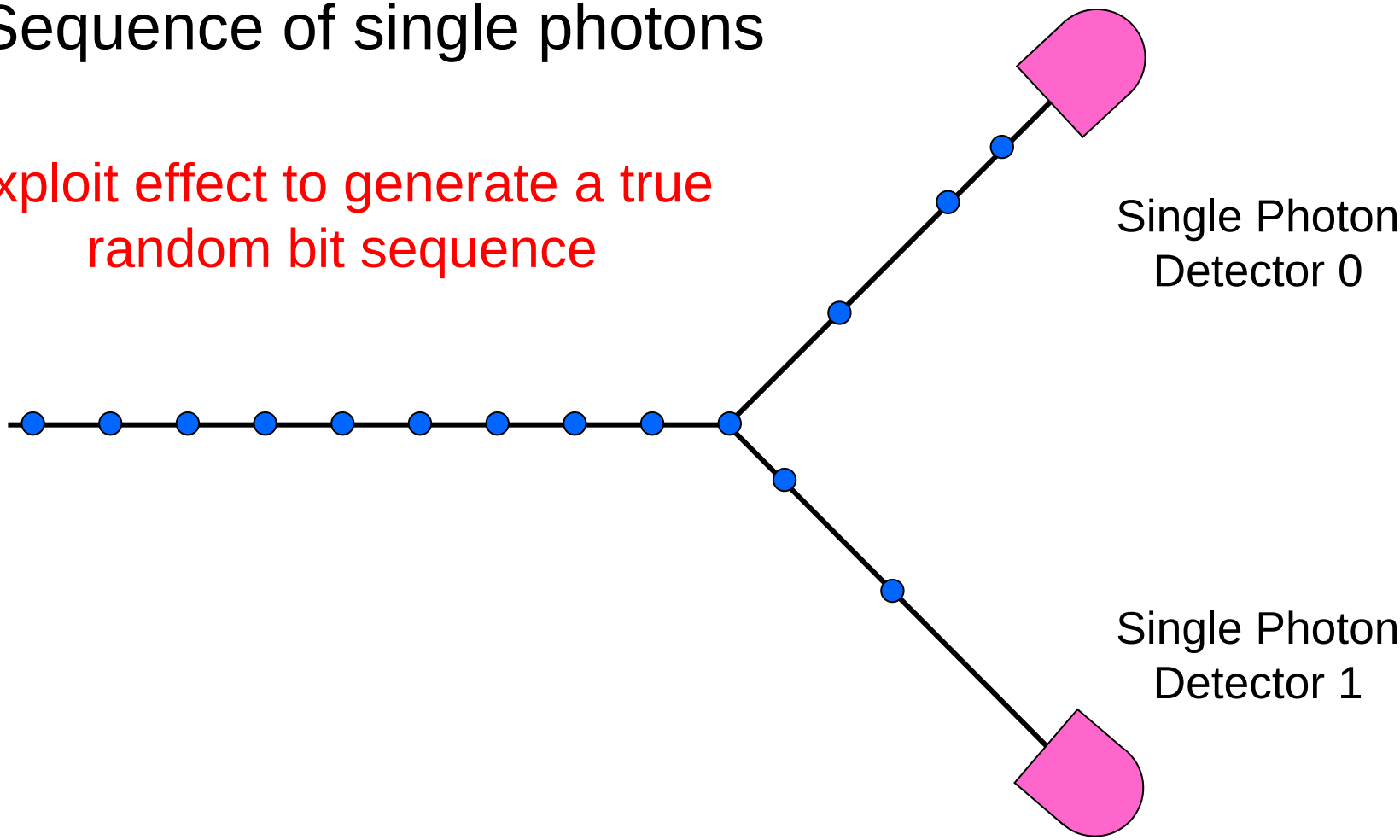
Photons behave like indivisible particles – they can't split – instead they make a random choice of output direction at the beamsplitter



Photons and Beamsplitters

- Sequence of single photons

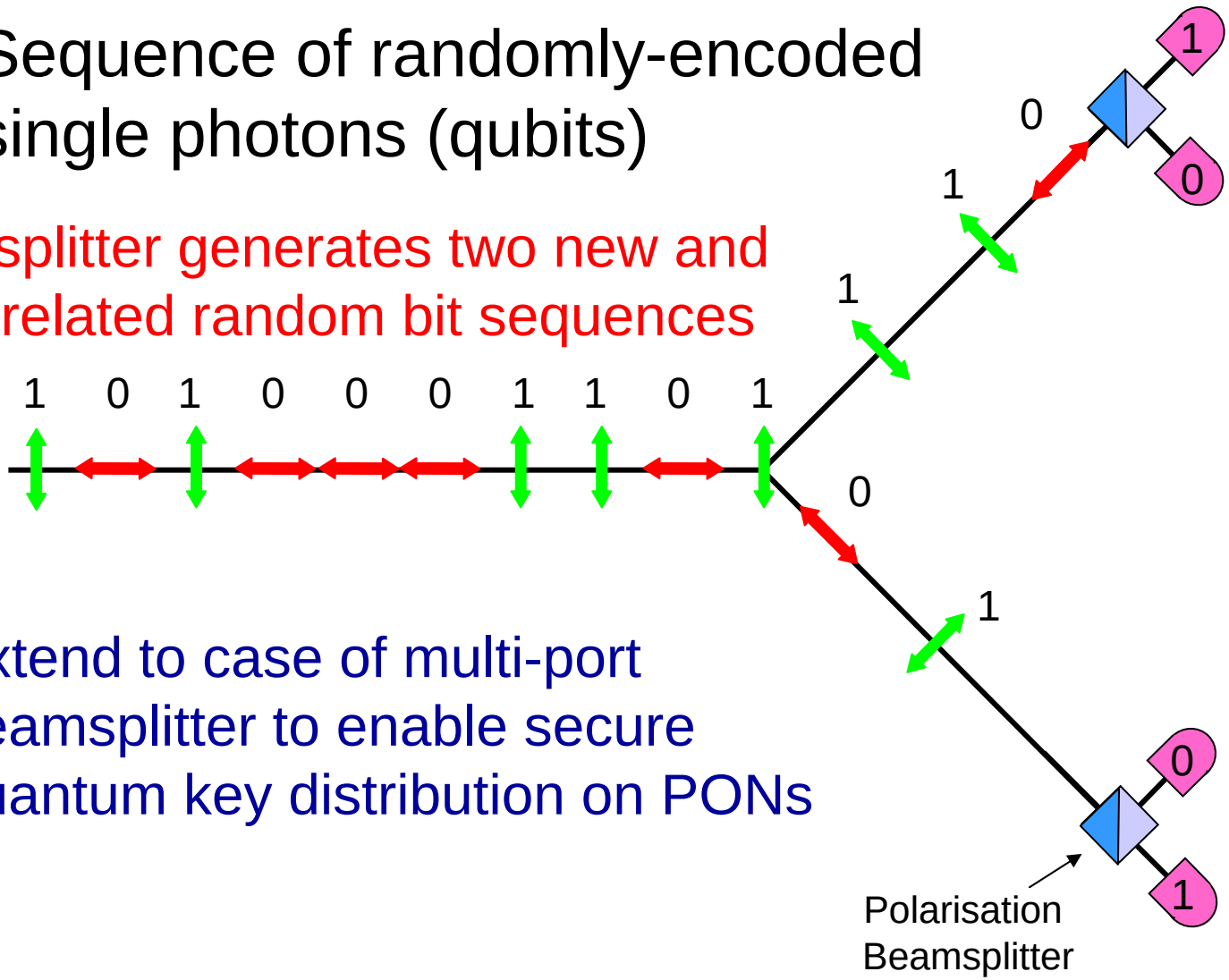
Exploit effect to generate a true random bit sequence



Photons and Beamsplitters

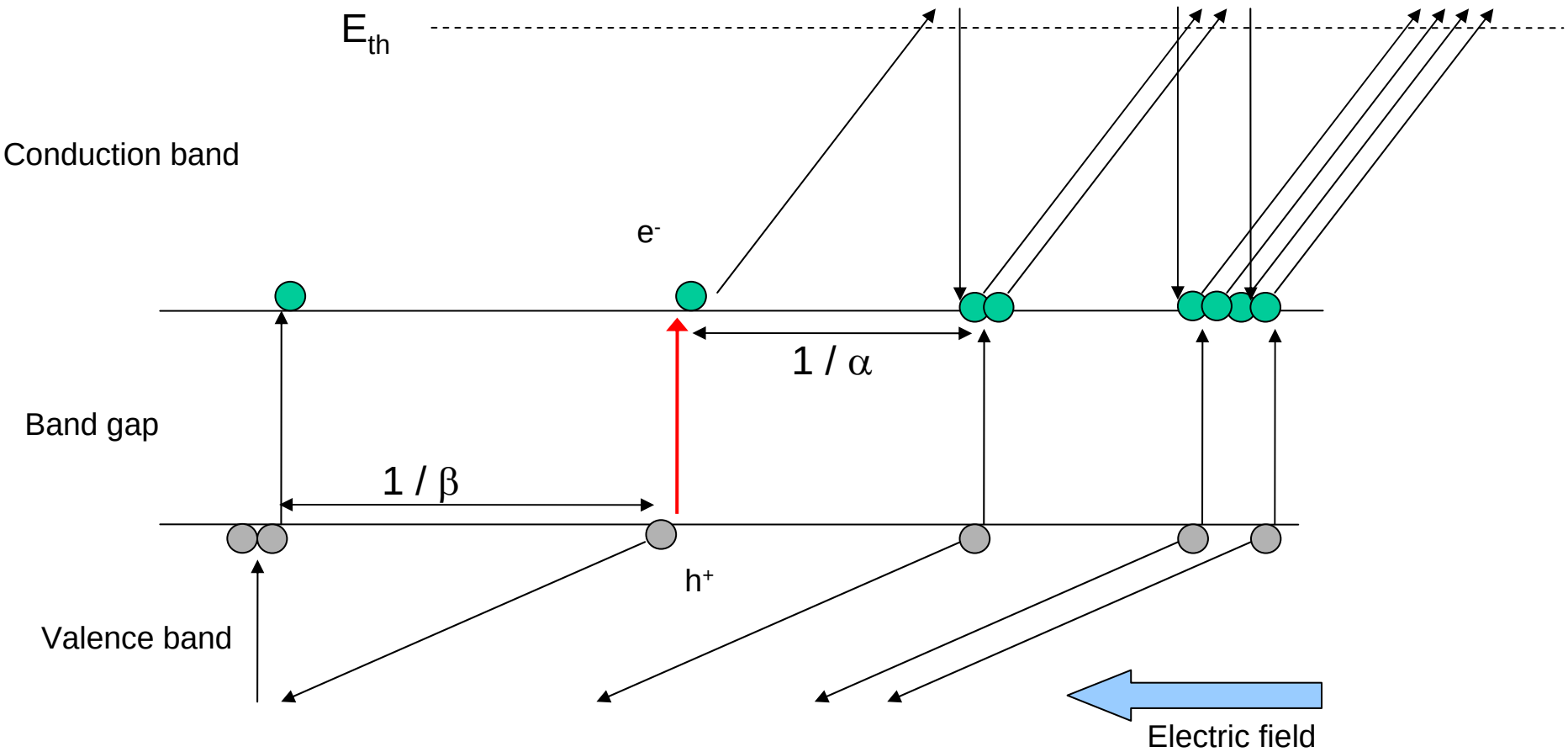
- Sequence of randomly-encoded single photons (qubits)

Beamsplitter generates two new and uncorrelated random bit sequences



- Extend to case of multi-port beamsplitter to enable secure quantum key distribution on PONs

Single Photon Detection



- Exploit impact ionisation in semiconductor Avalanche Photodiodes (APDs)
  - Generates multiplication gain in device
  - Used to enhance sensitivity of conventional optical receivers

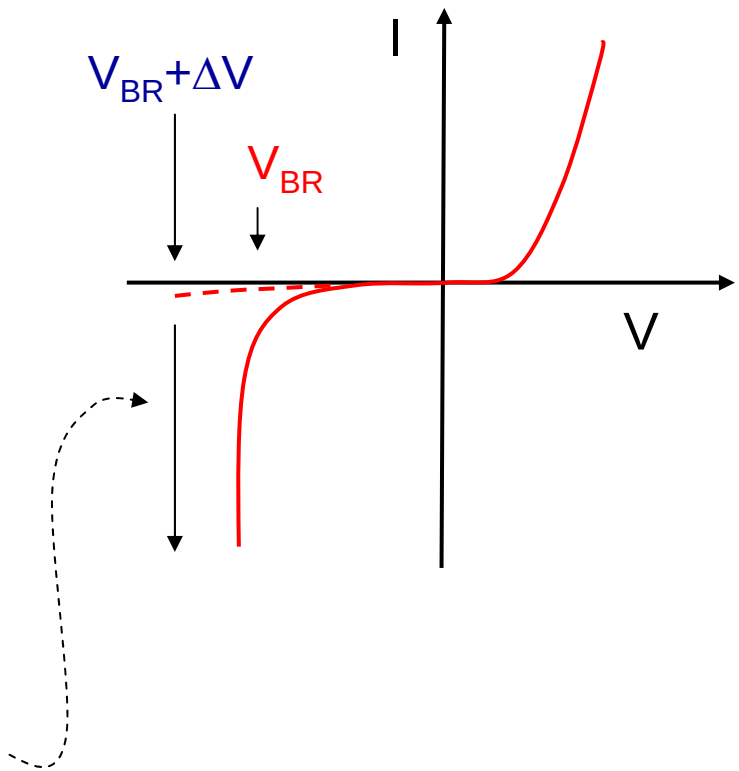
(Slide Courtesy: E. O'Reilly)

Single Photon Detection

- At APD reverse breakdown voltage $V=V_{BR}$ avalanche gain $\rightarrow \infty$

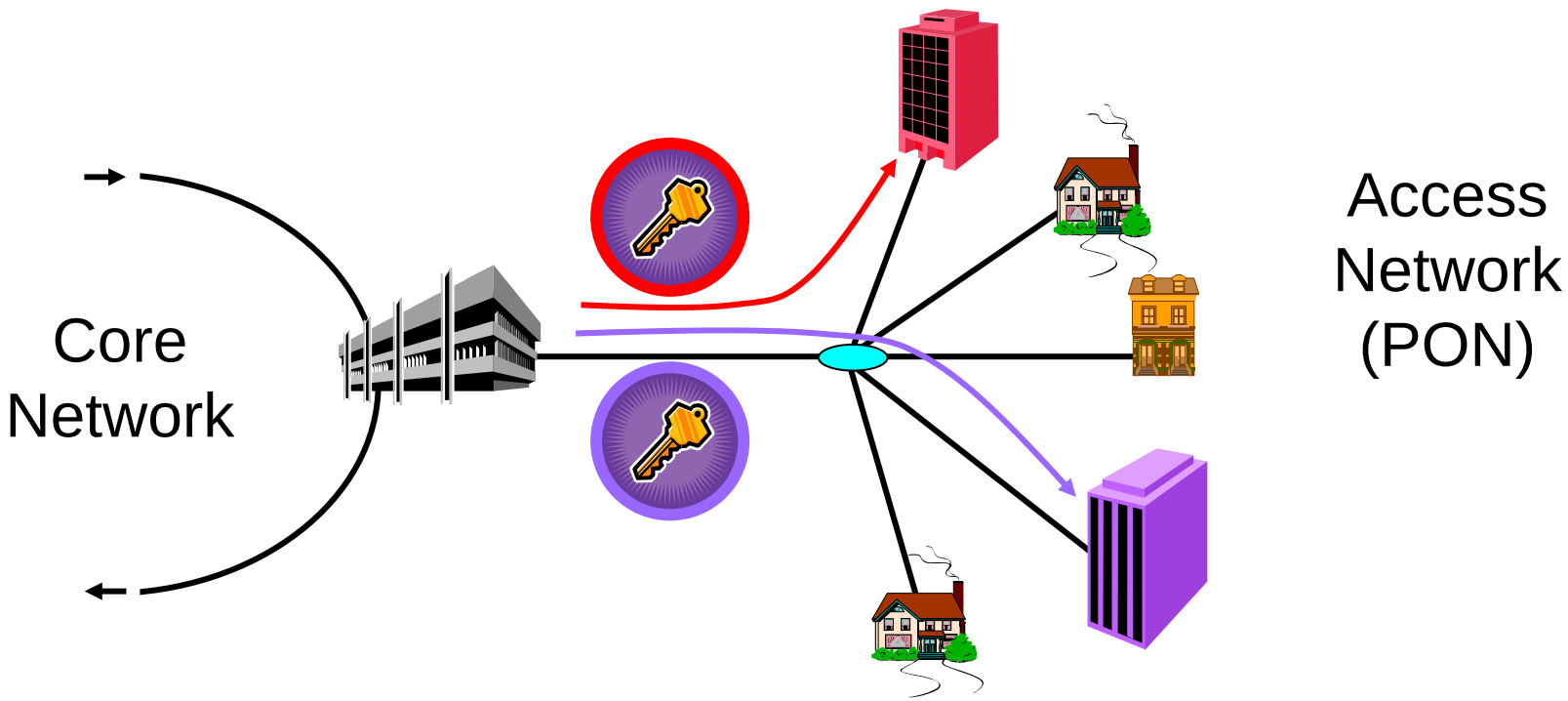
- To detect single photons:
  - Cool device to reduce dark carrier generation rate
  - Bias APD beyond breakdown
    - Device in quasi-stable state
    - Single photo-generated carrier generates self-sustaining avalanche
    - Results in large, detectable current pulse (Geiger Mode)

APD Dark Current vs. Bias Voltage



System Application: Security on Passive Optical Networks (PONs)

- What is the optimum detection scheme?



4th Year Project

- Title:
  - "Single Photon Detection for Quantum Cryptography"

- Method/Aims:
  - Experimental investigation of single photon detection in λ=1.3-1.55μm range using a variety of APD types
  - Investigate fundamental processes that determine device behaviour
  - Compare performance, assess suitability for use in quantum cryptography applications

If interested, contact me by e-mail at paul.townsend@tyndall.ie

Summary

- Quantum cryptography
  - Exploits fundamental quantum properties of photons
  - Enables secure transmission of information in optical networks
- Photonic Systems Group activity
  - Focused on developing and demonstrating practical applications
  - e.g. Quantum-encrypted optical access networks