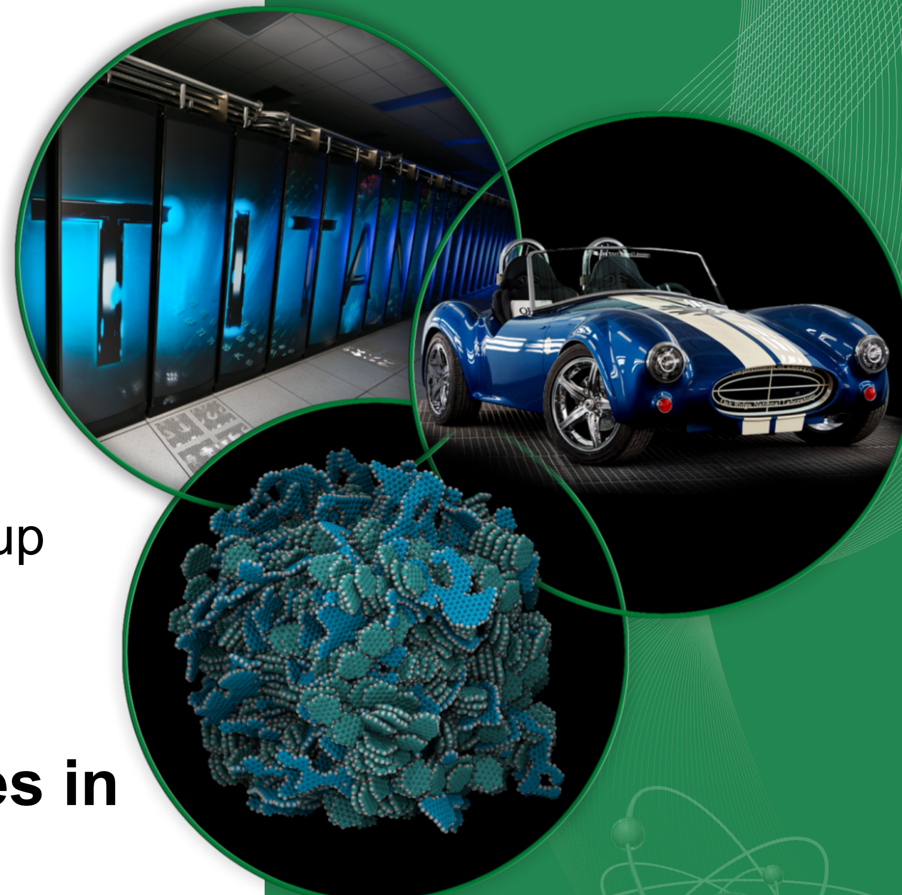
Quantum Technologies for Secure Wide-Area Time Distribution



Phil Evans, Ph.D.

evanspg@ornl.gov

Quantum Information Sciences Group

Oak Ridge National Laboratory

IEEE/NIST Timing Challenges in the Smart Grid Workshop

Gaithersburg MD

Oct 26th 2016

Outline

1. Motivation
2. The weird world of quantum mechanics
   - Uncertainty
   - Entanglement
3. Technologies
   - (Truly!) random numbers
   - Secure communications
4. Applications to time distribution
   - Over optical fiber
   - Over the wire
   - Over the air
5. Summary & Outlook

Motivation

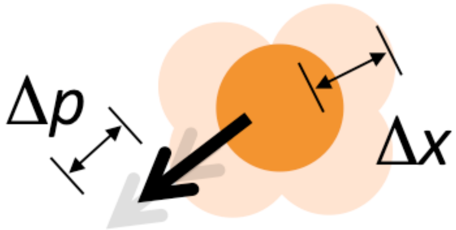
How can we distribute time from a trusted source in a secure, authenticated and resilient manner?

- Applications
  - Power & Energy
  - Transportation
  - Cyber security
  - Financial

Quantum Mechanics

- Physical laws describing behavior of ‘small’ things
  - Subatomic particles → clusters of atoms → MEMS devices
  - Photons (e.g. visible light, RF, X-rays)
  - Fields and vacuum
- Probabilities vs. absolutes
  - QM deals with *expectation values* & *probability functions*
  - The wavefunction Ψ completely describes the system
  - Want to calculate something? Apply the right operator!
- Consequences
  - Discrete states & energy levels (no continuums)
  - Uncertainty principles
  - Other ‘odd’ behaviors

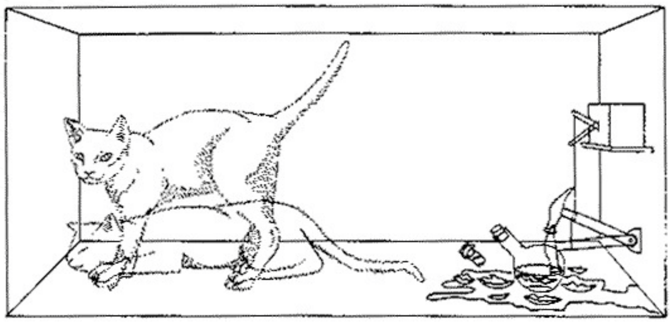
Quantum Mechanics (2)



$$\Delta p \Delta x \geq \frac{\hbar}{2}$$

Heisenberg's uncertainty relation

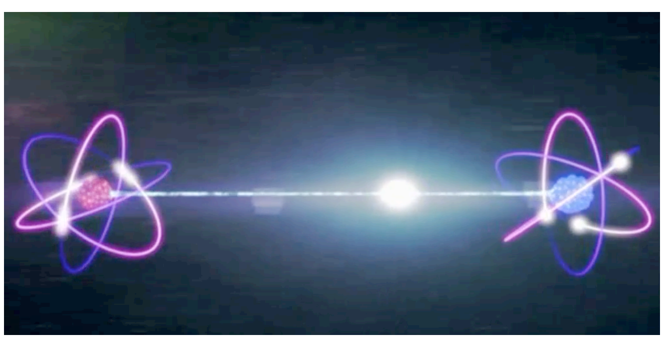
Increased measurement accuracy of one property implies less accuracy of the conjugate



Superposition

Quantum objects exist in a superposition of **ALL** allowed states….

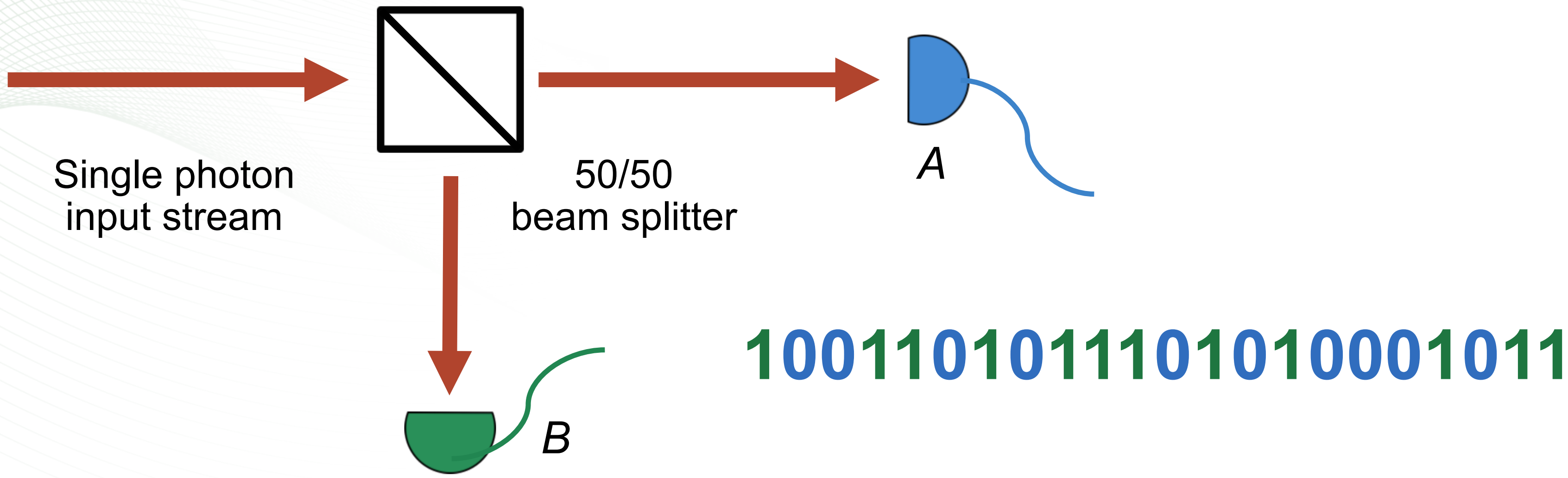
… until a measurement is made



Entanglement

"*Spooky action at a distance*"
Quantum systems with two (or more) particles are described with a single wavefunction.

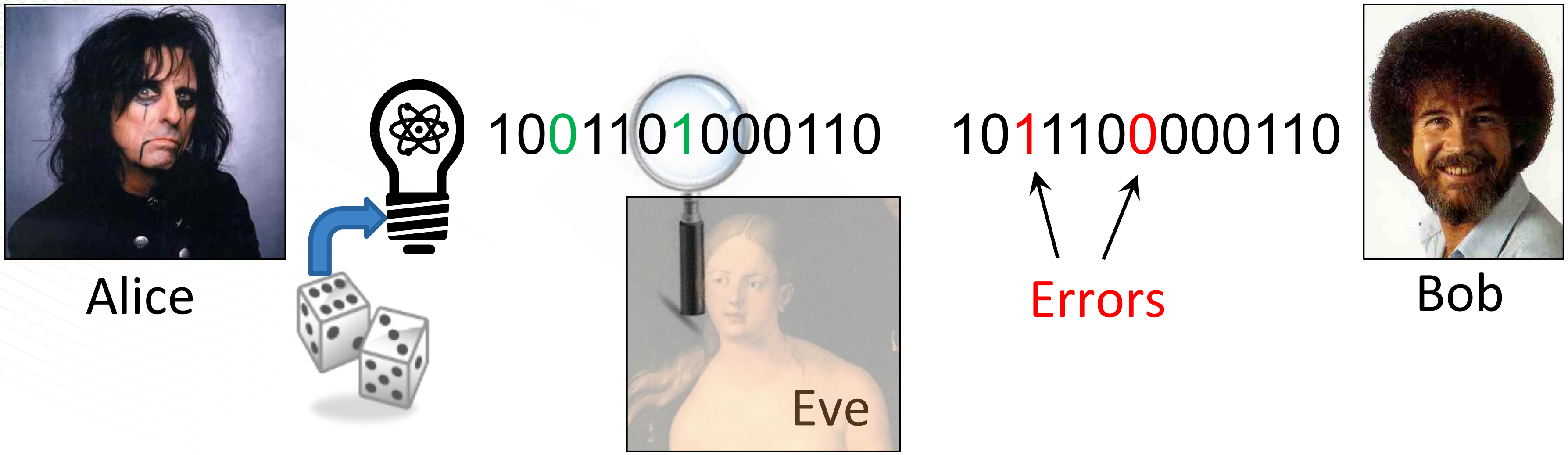
Truly Random Numbers



- Single photon source
  - Emission time of photons is **random**
- Reflection **OR** transmission at the beam splitter
- Detectors register single photon events
- Output is truly random bit stream
  - … except for biases

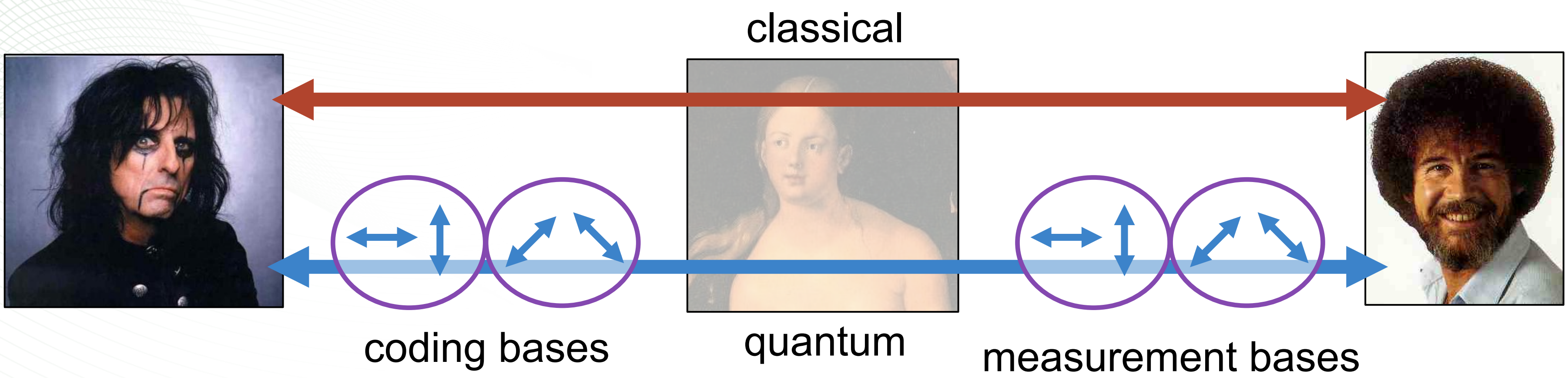
OAK RIDGE National Laboratory

Secure Communications



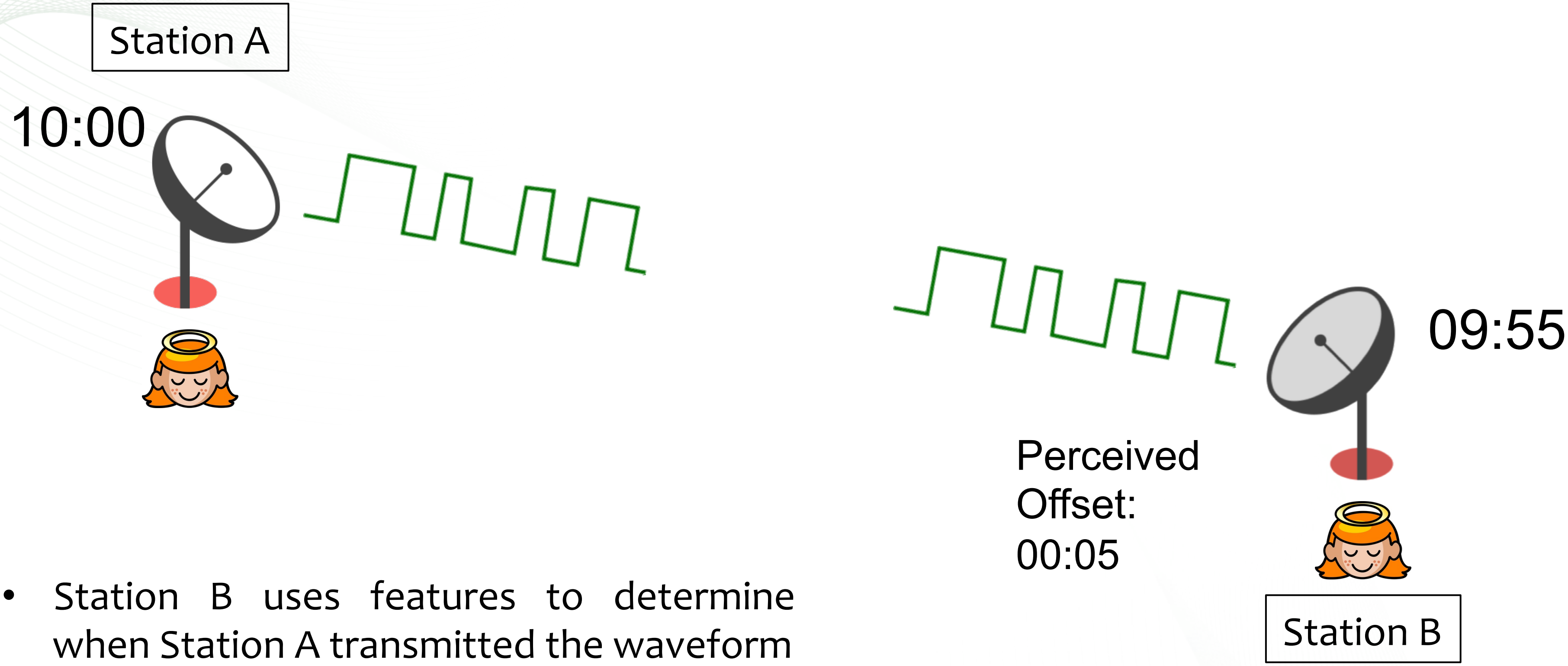
- *Alice* prepares single photon states
- *Bob* detects single photons
- *Eve* **cannot** measure and prepare Alice's state
  - No cloning allowed – the **uncertainty principle** in action
  - Introduces **errors** with her measurements

Secure Communications 2



- Quantum Key Distribution (QKD)
  - Quantum channel: Alice prepares, Bob measures
  - Classical channel: reconciliation, error correction
  - **BB84 protocol**
- Provably secure method of distributing keys
  - Passwords for symmetric key encryption
  - **Correlated** random numbers for one-time pad

One-Way Time Distribution is Insecure

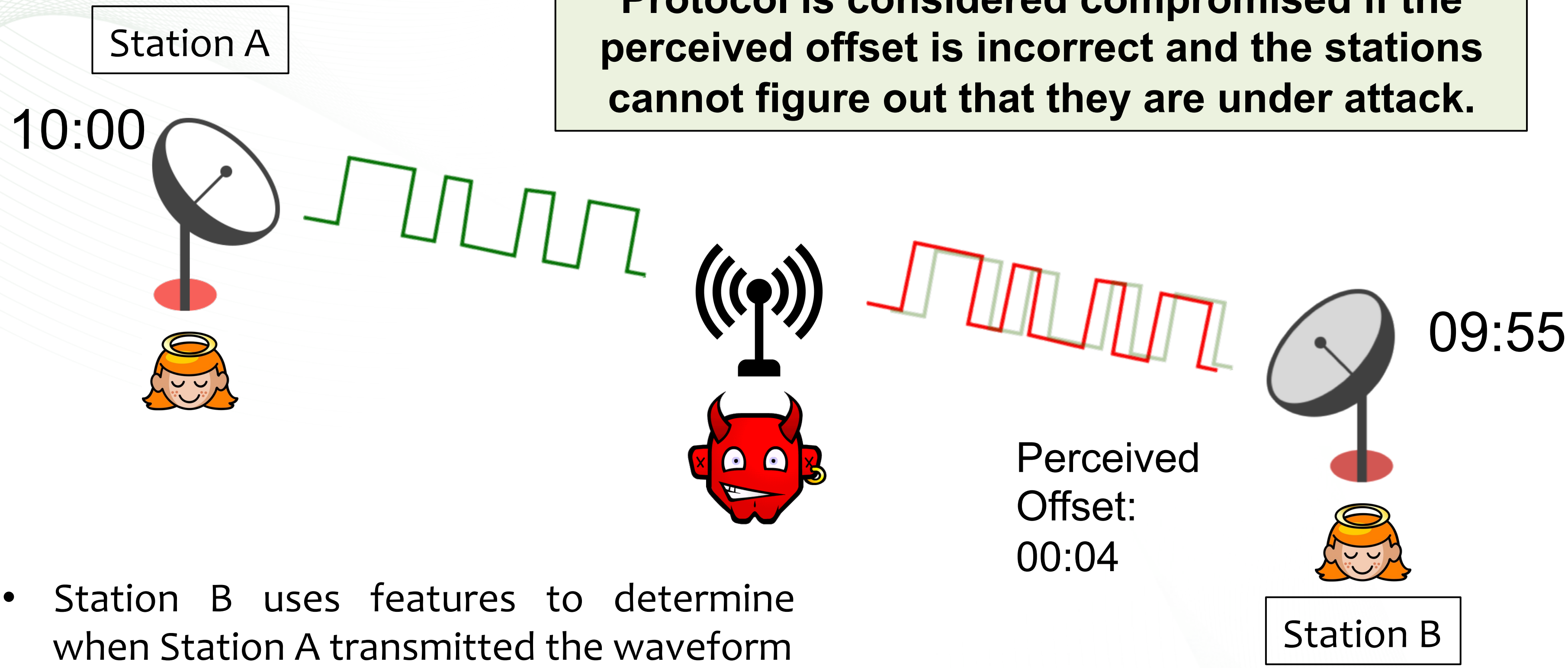


- Station B uses features to determine when Station A transmitted the waveform
- Station B takes the propagation delay into account

Oak Ridge National Laboratory

One-Way Time Distribution is Insecure 2

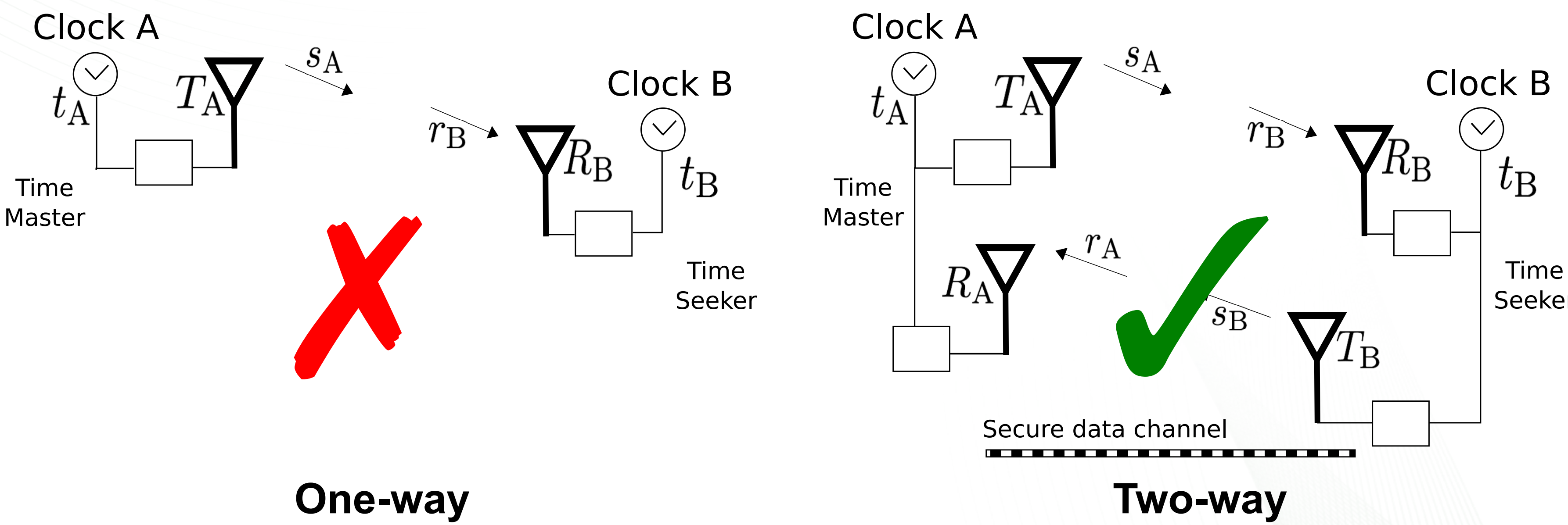
Protocol is considered compromised if the perceived offset is incorrect and the stations cannot figure out that they are under attack.



- Station B uses features to determine when Station A transmitted the waveform
- Station B takes the propagation delay into account

Conditions for Secure Time Distribution

1. Propagation delay between A and B must be known
2. The path taken by the timing signal must be irreducible.
3. Both A and B must inject **unpredictability** into their transmitted signals.
4. Time delay between B receiving message and replying must be known.



L. Narula & T. Humphreys, DOI: 10.1109/PLANS.2016.7479783

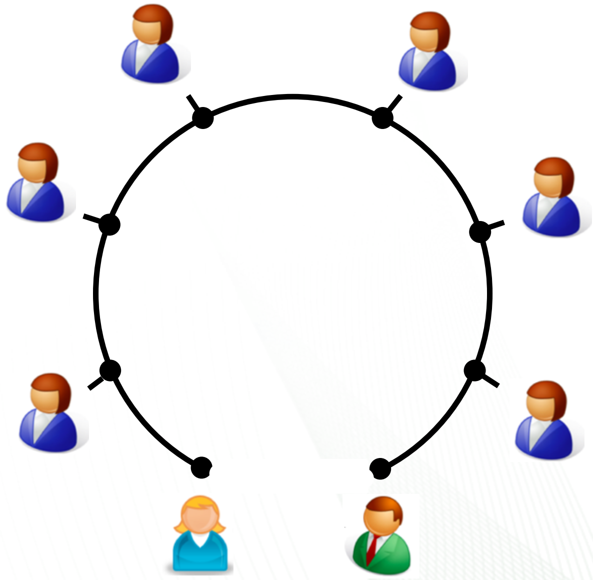
How Quantum Technologies Can Help

Use random numbers generated and distributed with QRNGs and QKD to encrypt time stamps with one-time pad

- Secure time distribution use cases:
  1. … over optical fiber
  2. … over the wire
  3. … over the air

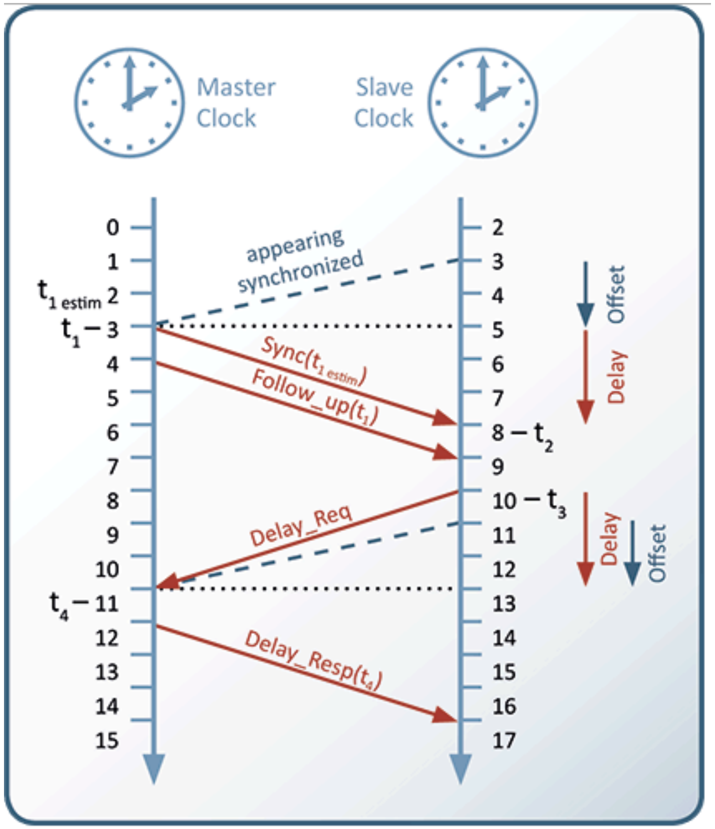
Secure Time Distribution over Optical Fiber

- Availability of fiber will allow full QKD solution
- Multi-party QKD network
  - Pairs of users establish key
  - Slaves establish their own keys with master
- Low cost – slave nodes are not full QKD stations
  - Photons not generated nor detected
- Funded by DOE CEDS
  - Lab research project recently concluded
  - Demonstrated with utility partner
  - Technology transition to industry
  - Industry project just started



Secure Time Distribution over the Wire

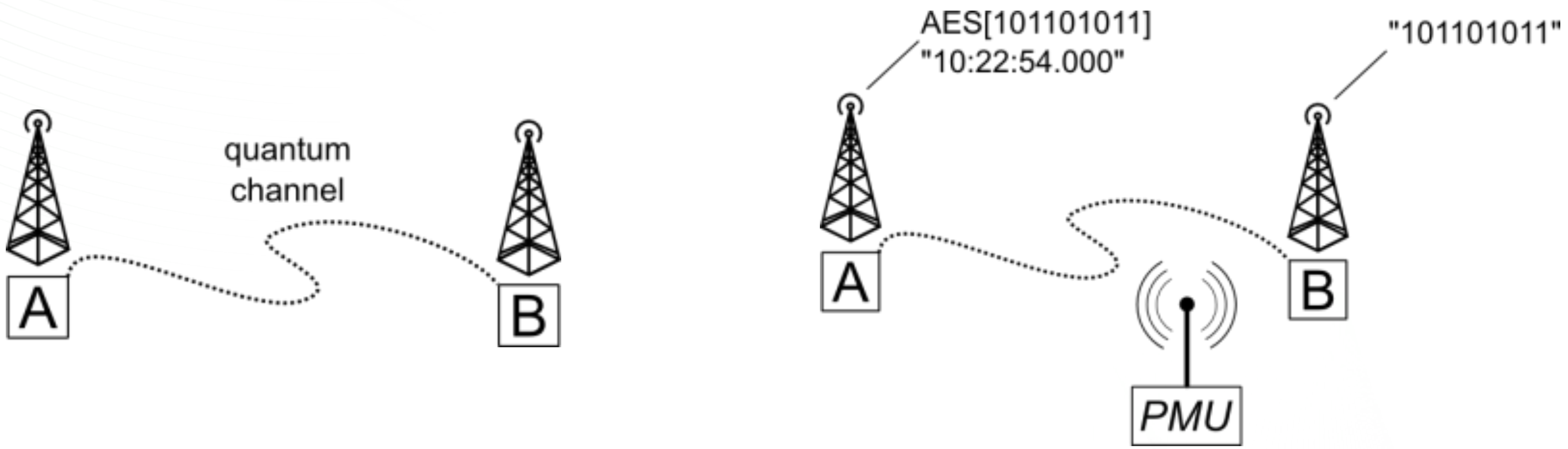
- Using IEEE 1588 (Precision Time Protocol)
- Authority generates key material using QRNGs
  - Pre-loaded onto devices
  - Distributes to users
- 1588 messaging uses key
  - All communications are secured
  - Minimize & account for overhead
- Modify to satisfy 2-way security
- *What happens when keys are used up or compromised?*



OAK RIDGE National Laboratory

Secure Time over the Air

- System of QKD-connected beacons
  - Key & time distributed to all beacons securely
  - Each beacon authenticates others' transmissions



- Timing Authentication Secured by Quantum Correlations (TASQC)
  - Currently funded by DOE CEDS
  - Proof of principle demo at PNNL Cyber-RF test bed
  - Utility demo coming in 2017

Secure Time over the Air

- Protocol:
  - Alice (master) encrypts and broadcasts time
  - Bob (verifier) receives & verifies Alice, broadcasts key
  - PMU (slave):
    - Encrypted time received at local clock t_1
    - Decryption key received at local clock t_2
    - Time message decryption, correction for TOF, local clock correction
    - PMU responds with quantum-seeded message
  - Alice & Bob receive acknowledgement and confirm
- Benefits:
  - **Full 2-way secure time distribution**
  - Utility / operator owns the system

Implemented with QKD systems & SDR

Summary & Outlook

- Secure time distribution
  - GPS is not enough
  - Terrestrial solutions – operated by stakeholders or trusted parties
  - Requires 2-way communication to prevent attacks
    - Master(s) to broadcast, slave(s) to acknowledge
    - Need store of shared unpredictability
- Quantum technologies
  - Leveraging true randomness for one-time pad
  - Leveraging provably secure communications
- Demonstrated use cases
- Increased quantum adoption in cyber systems
  - critical infrastructure to follow

Questions?