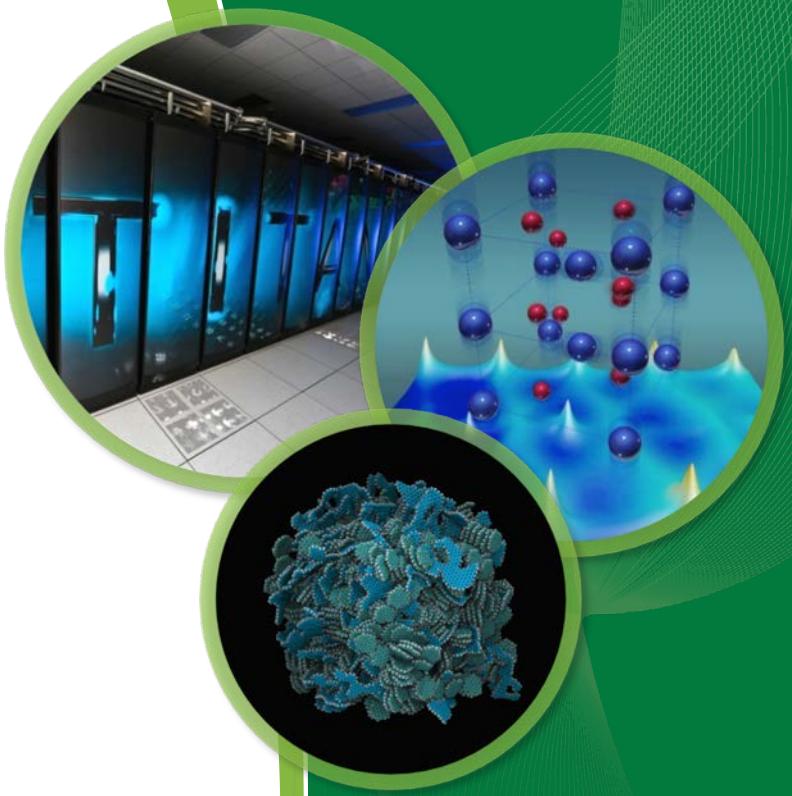
Quantum Communication Techniques for Time Authentication and Distribution



Phil Evans, Ph.D.

evanspg@ornl.gov

Oak Ridge National Laboratory

NASPI Work Group Meeting

March 22-23 2017

Gaithersburg MD

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 – The TASQC Project**
5. Summary & Outlook

Motivation

Why is GPS vulnerable?

- GPS signals are broadcast in a well-known format
- The system has no way of checking the authenticity of GPS signals

Spoofing GPS matters today

- Corruption of local time
- Failures damage equipment, outages, economic loss

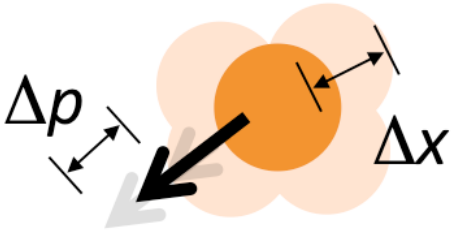
→ Loss of confidence in energy delivery system

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

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

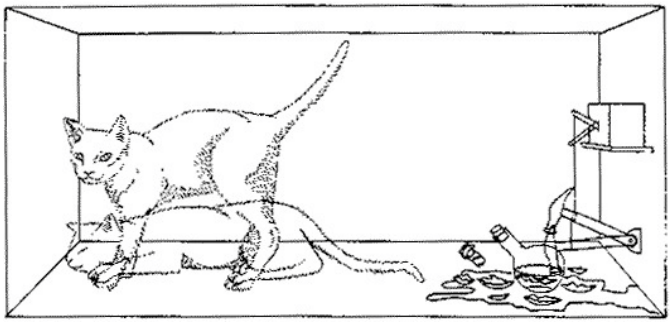
Quantum Mechanics



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

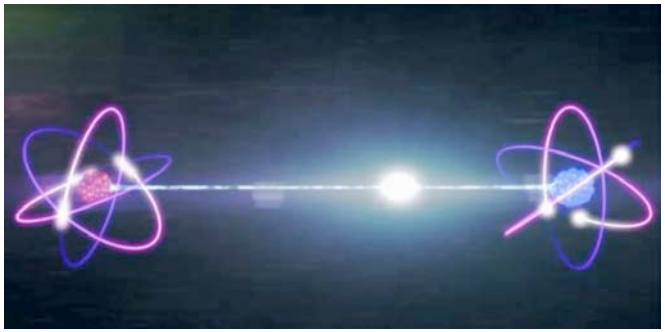
Heisenberg's uncertainty relation

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



Superposition

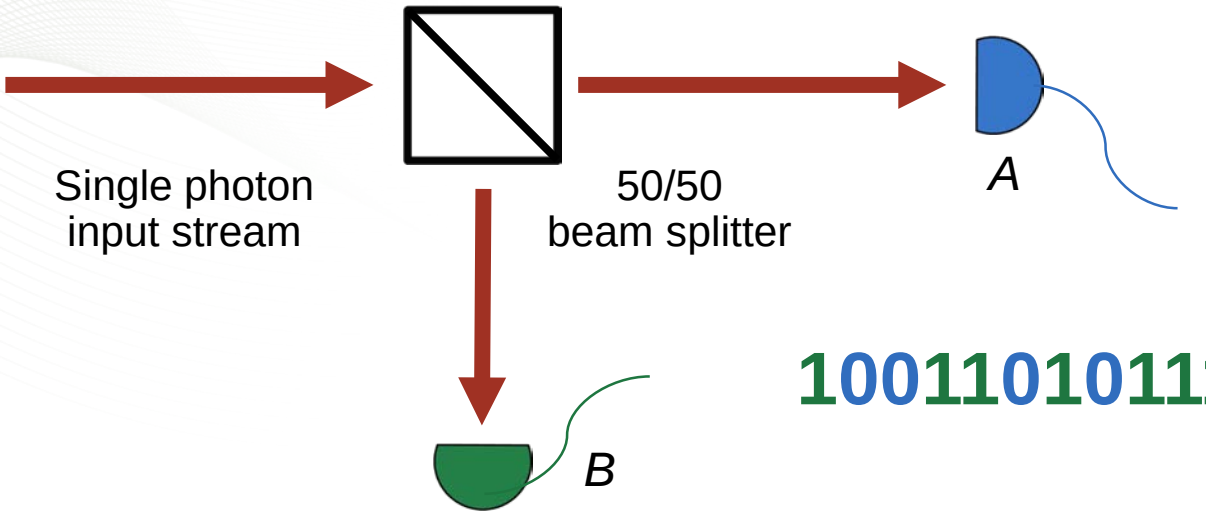
Quantum objects exist in a superposition of **ALL** allowed states….
… until a measurement is made



Entanglement

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

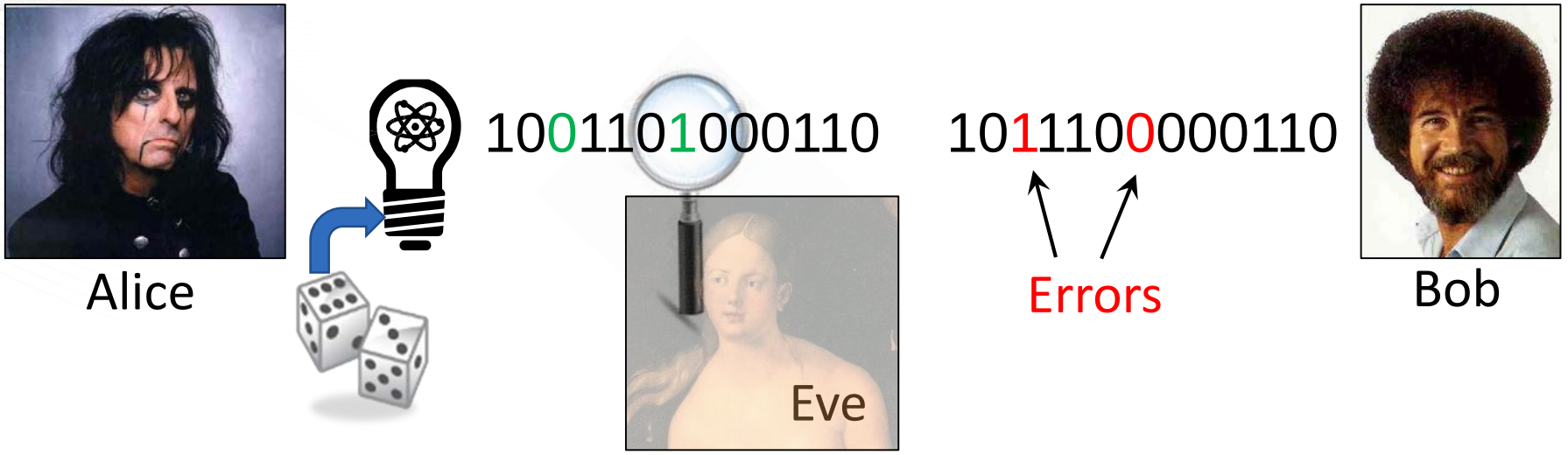
Truly Random Numbers



10011010111010100011011

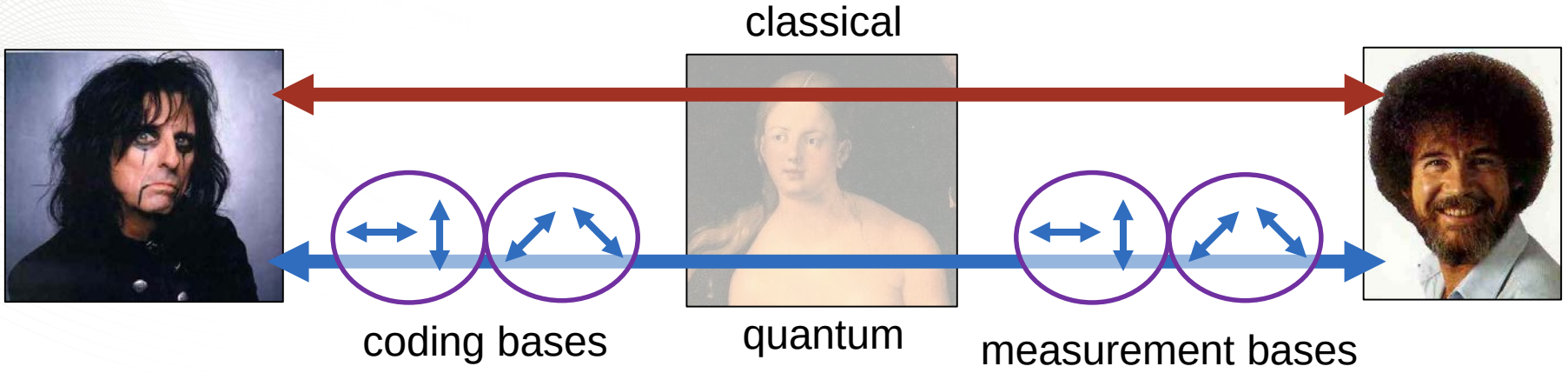
- Single photon source
  - Emission time of photons is **random**
- Reflection **OR** transmission at the beam splitter
- Detectors register single photon events
- Output is truly random bit stream
  - … except for biases

Secure Communications



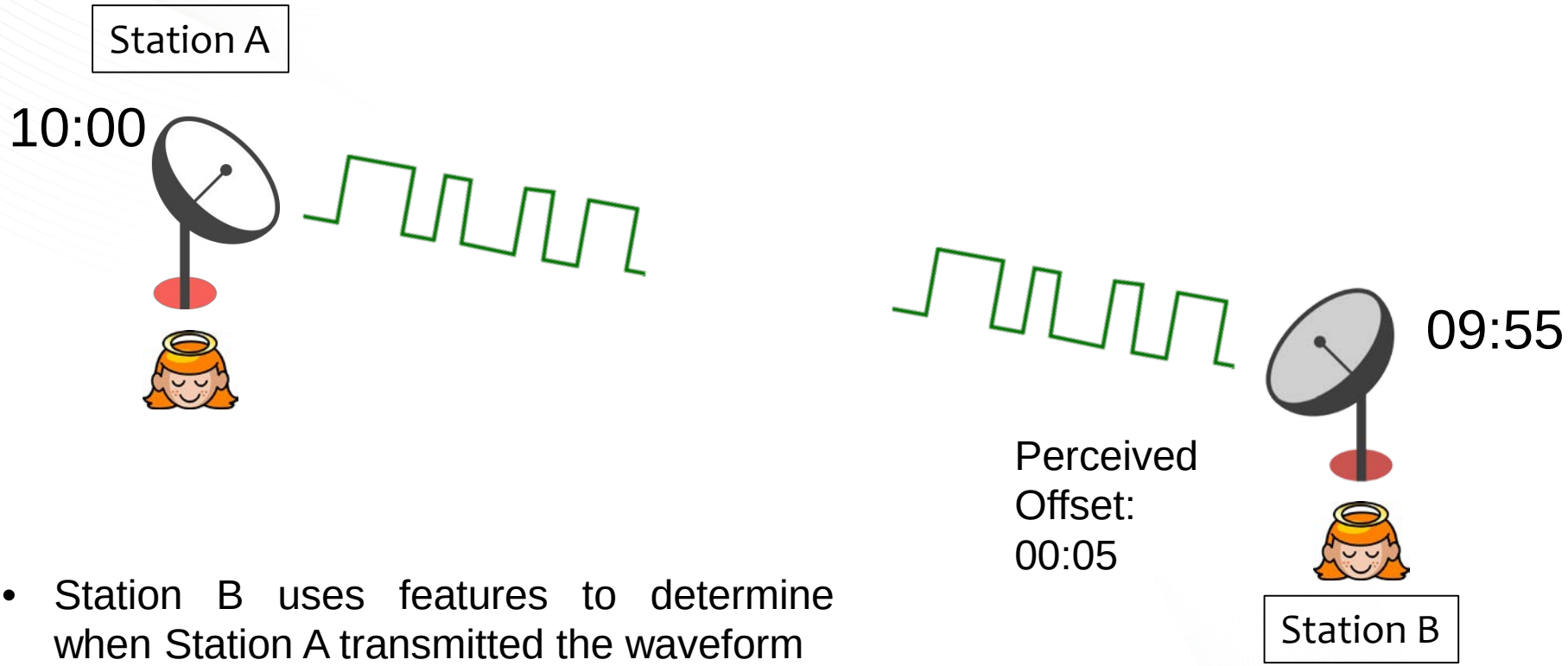
- *Alice* prepares single photon states (using a QRNG!)
- *Bob* detects single photons
- *Eve* **cannot** measure and prepare Alice's state
  - No cloning allowed – the **uncertainty principle** in action
  - Introduces **errors** with her measurements

Secure Communications



- 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

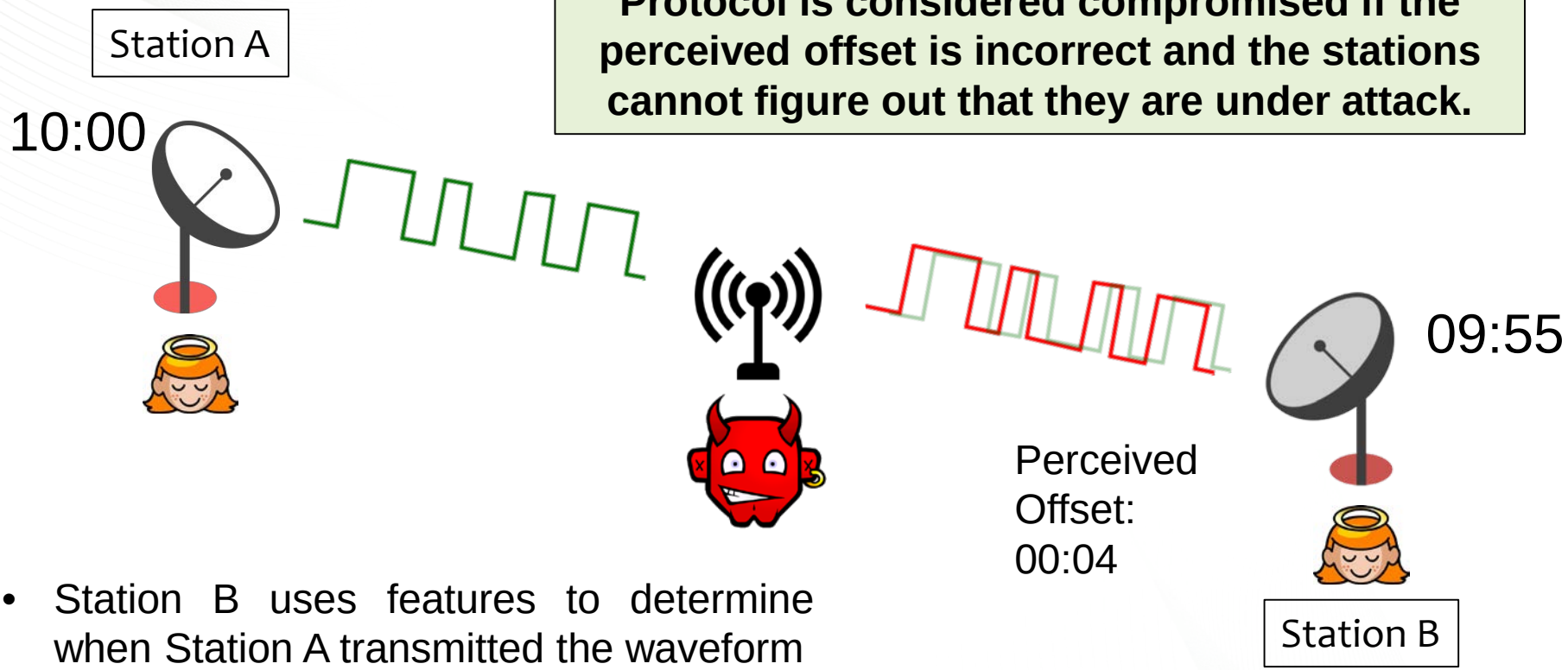
One-Way Time Distribution is Insecure



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

One-Way Time Distribution is Insecure

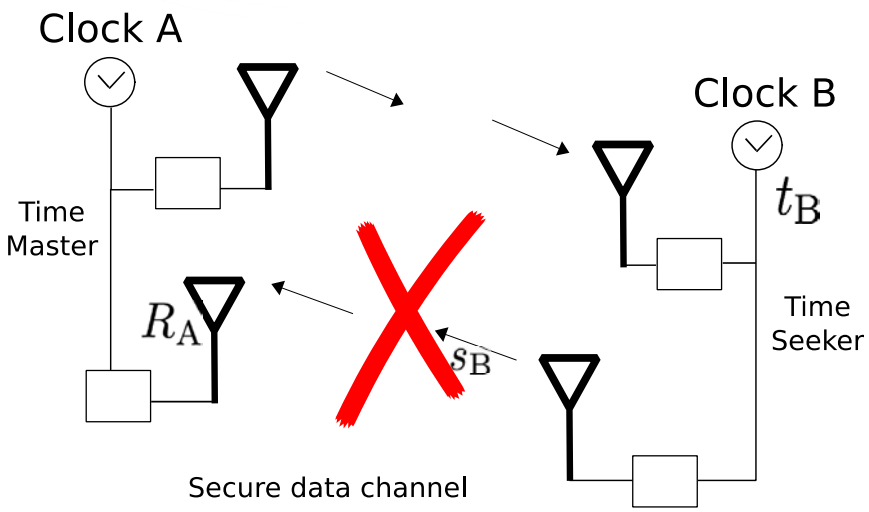
Protocol is considered compromised if the perceived offset is incorrect and the stations cannot figure out that they are under attack.



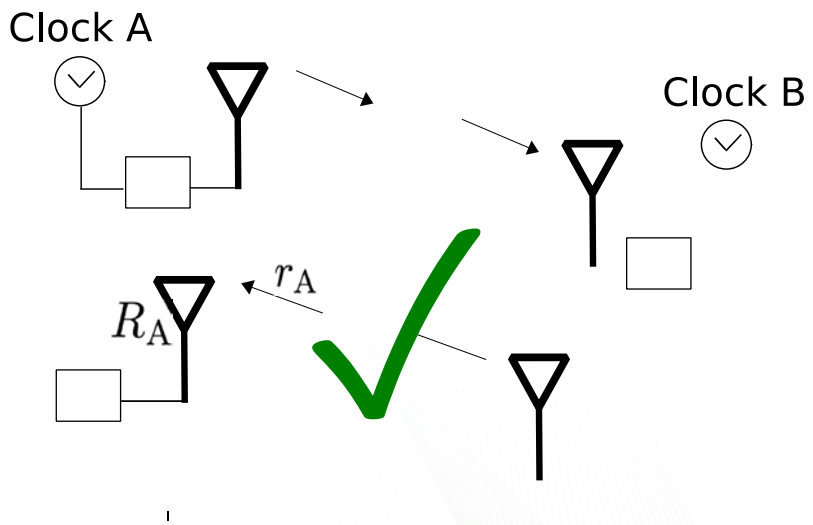
- Station B uses features to determine when Station A transmitted the waveform
- Station B takes the propagation delay into account

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.



One-way



Two-way

L. Narula & T. Humphreys, DOI: [10.1109/PLANS.2016.7479783](https://doi.org/10.1109/PLANS.2016.7479783)

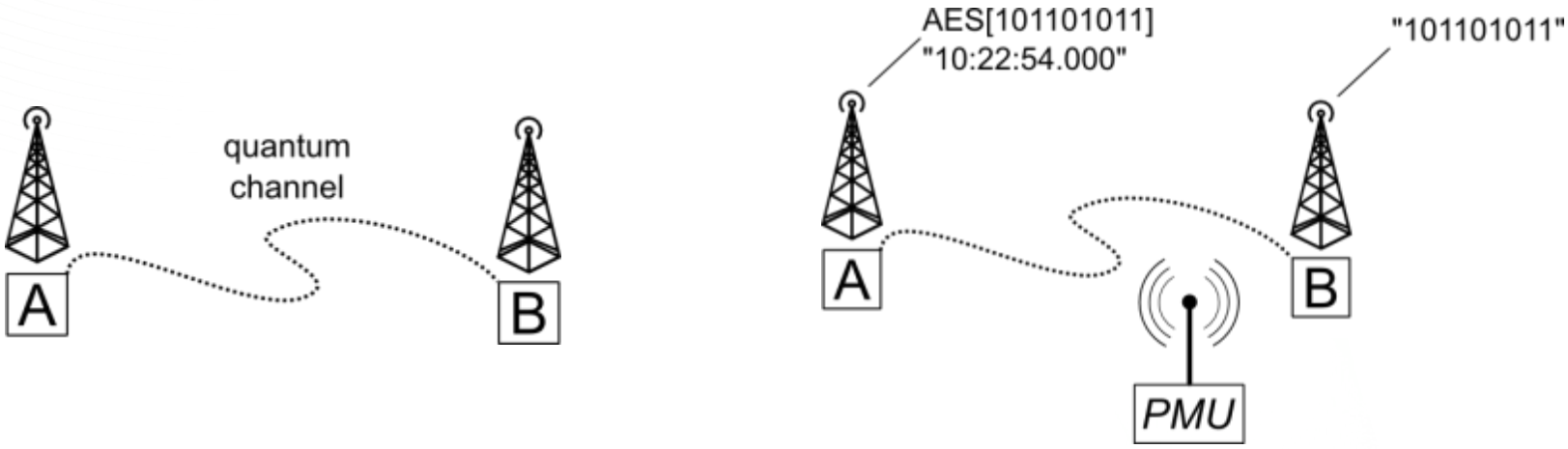
How Quantum Technologies Can Help

We can use quantum-generated and distributed keys as a system resource

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

Secure Time over the Air

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

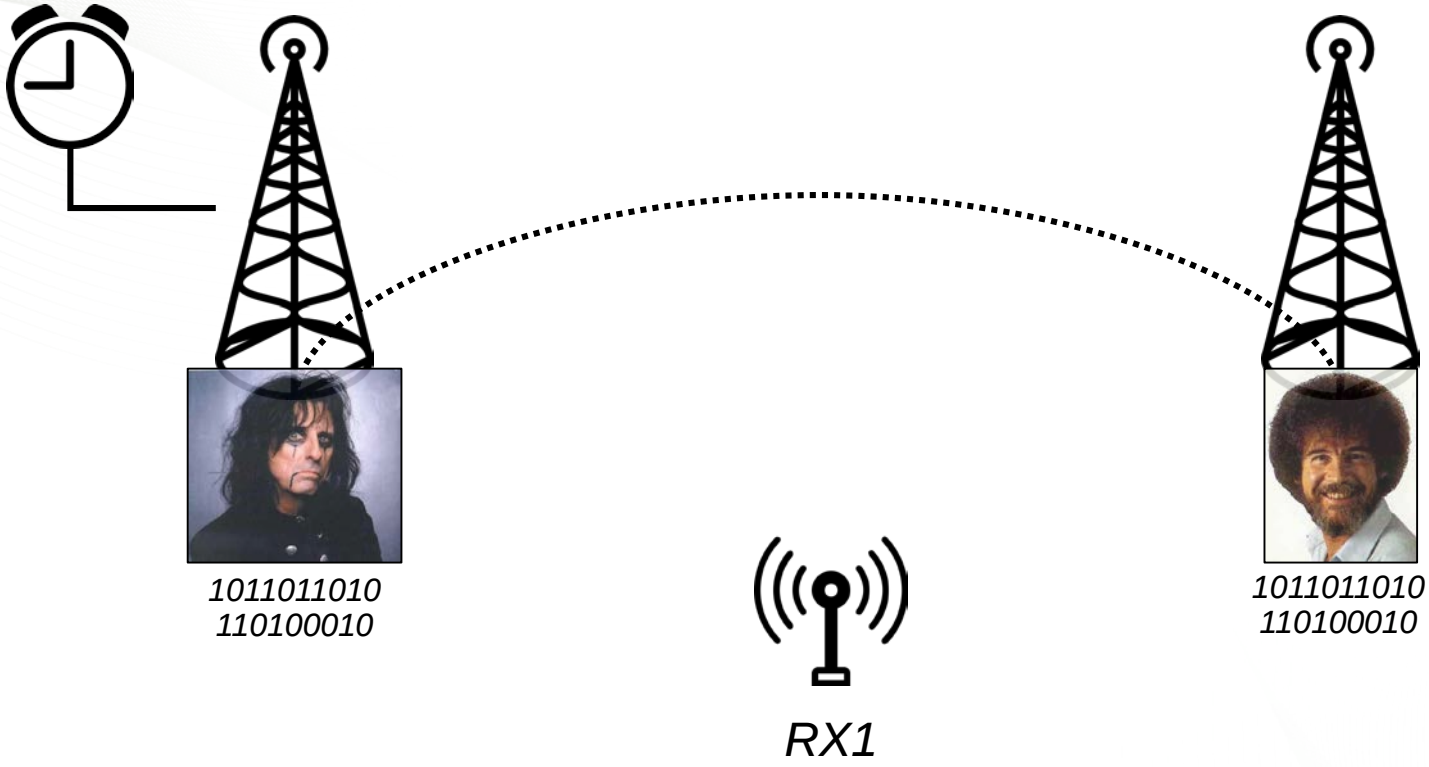


- Timing Authentication Secured by Quantum Correlations (**TASQC**)
  - Currently funded by DOE CEDS
  - Proof of principle demo at PNNL Cyber-RF test bed
  - SDG&E demo coming Summer 2017

TASQC

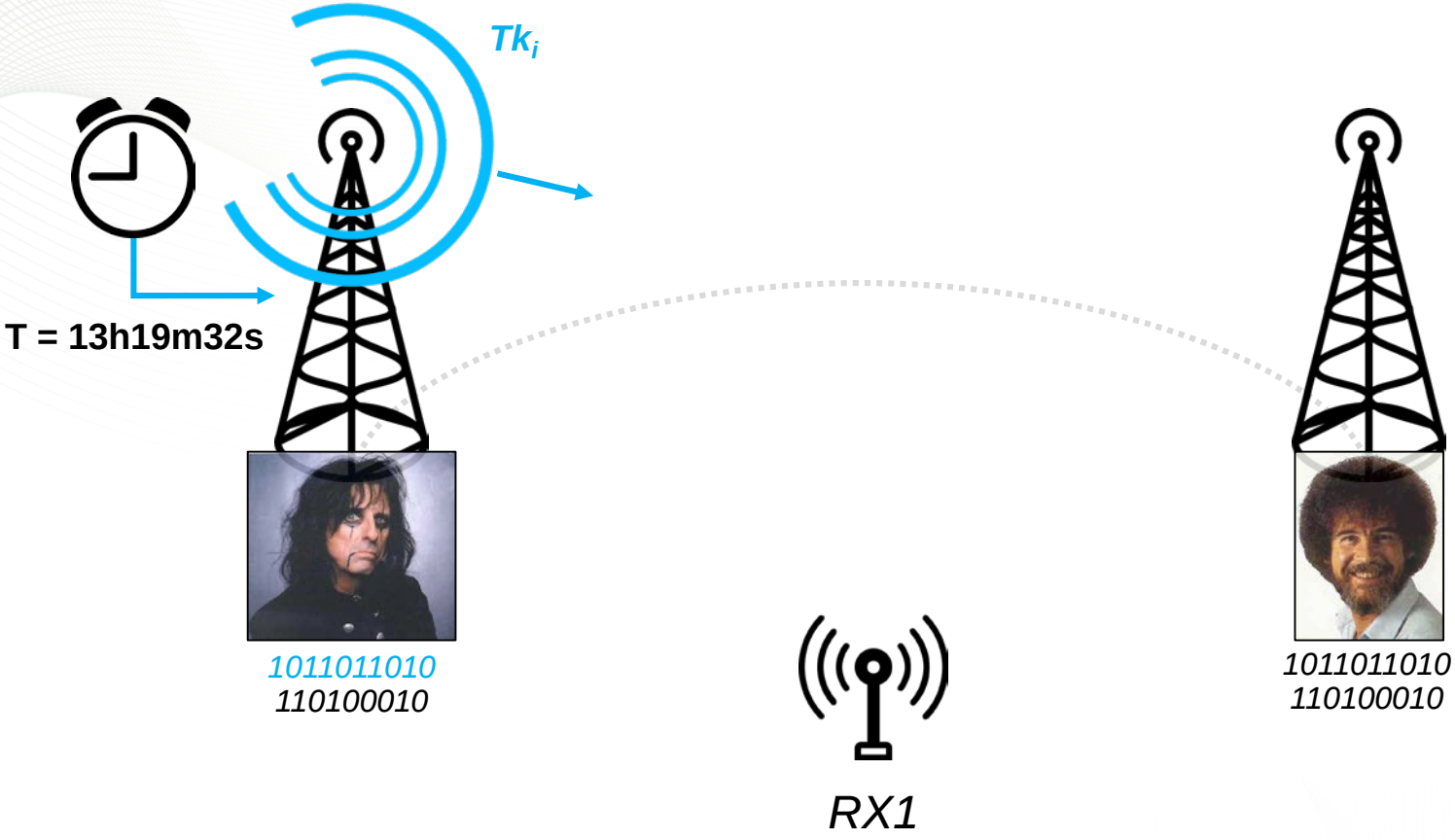
- Full 2-way secure time distribution
- Quantum technologies utilized as a resource
- Scalable approach for multiple beacons, multiple receivers
- TASQC base system is flexible
  - Inherently compatible with many QKD schemes
  - Can utilize & piggyback on any existing RF infrastructure
  - Other protocols can be developed and deployed
    - e.g., secure message passing – notification of outages or leap events
- Utility / operator owns the system

TASQC 2-Way Secure Time Protocol



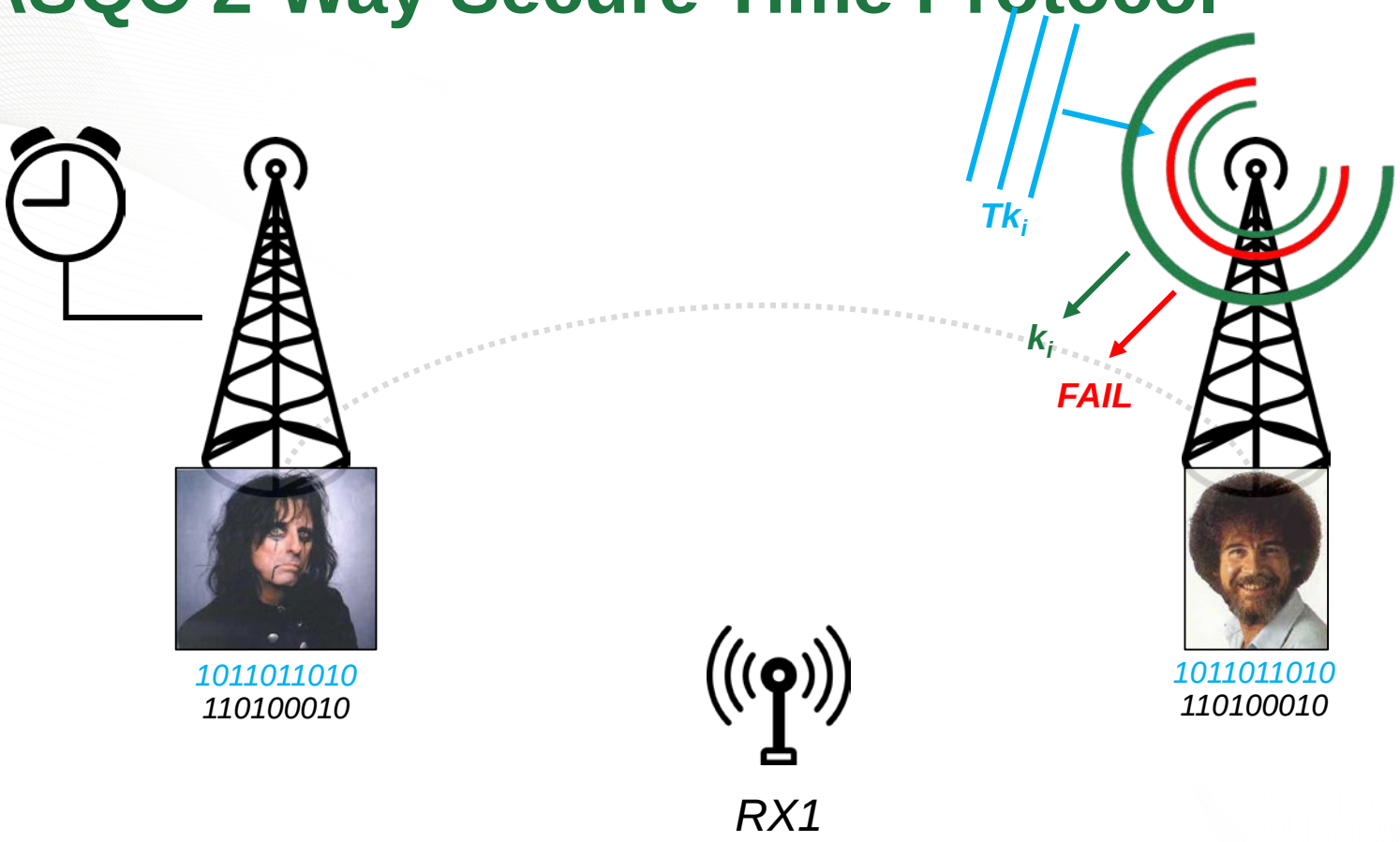
(0) *Alice* and *Bob* establish and share secret keys – using QKD – over an optical fiber link. This occurs in the background.

TASQC 2-Way Secure Time Protocol



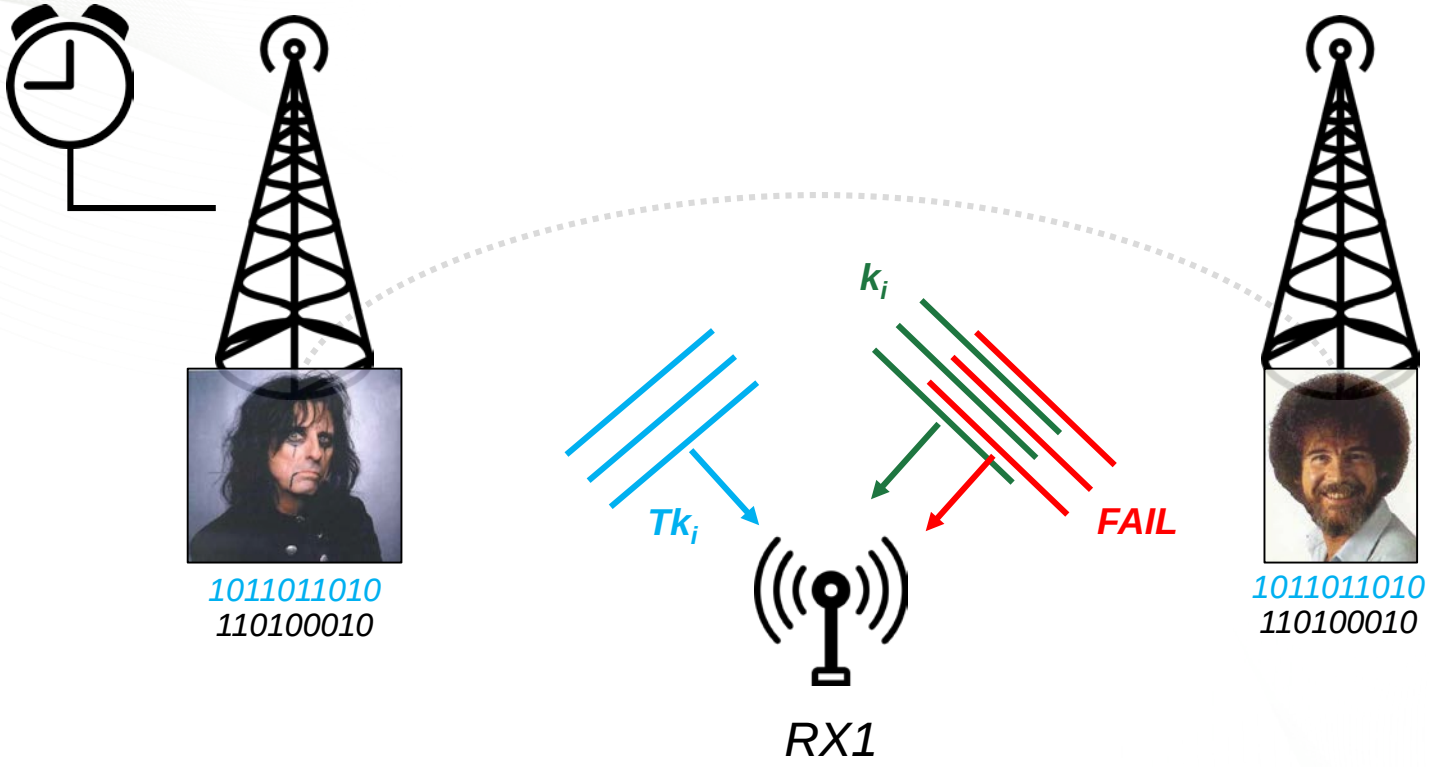
(1) *Alice* requests current time *T* from the Master Clock, encrypts with key *i*, broadcasts this as message Tk_i.

TASQC 2-Way Secure Time Protocol



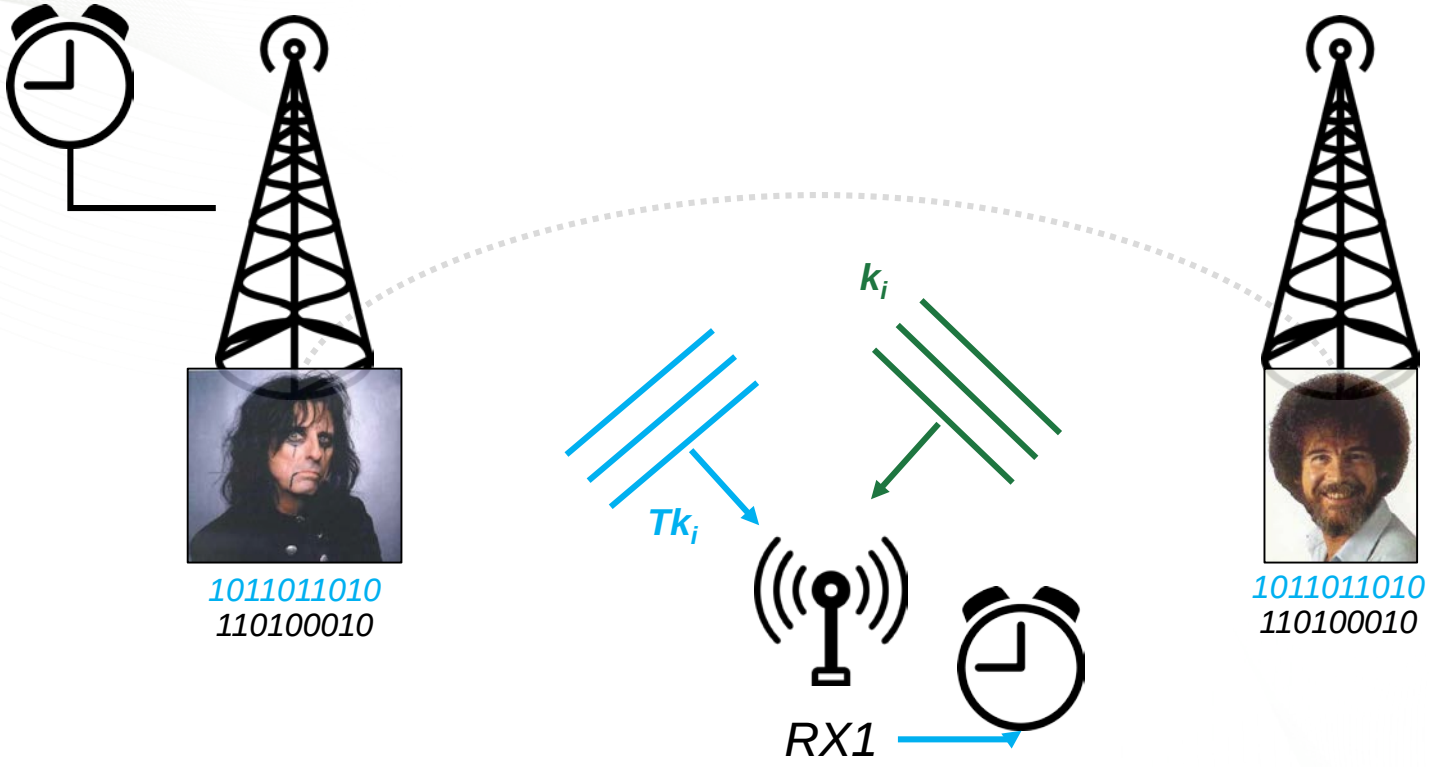
(2) *Bob* receives Tk_i and checks for authenticity by using his key *i* to decrypt. If successful, *Bob* transmits k_i in the clear. If not, *Bob* transmits FAIL

TASQC 2-Way Secure Time Protocol



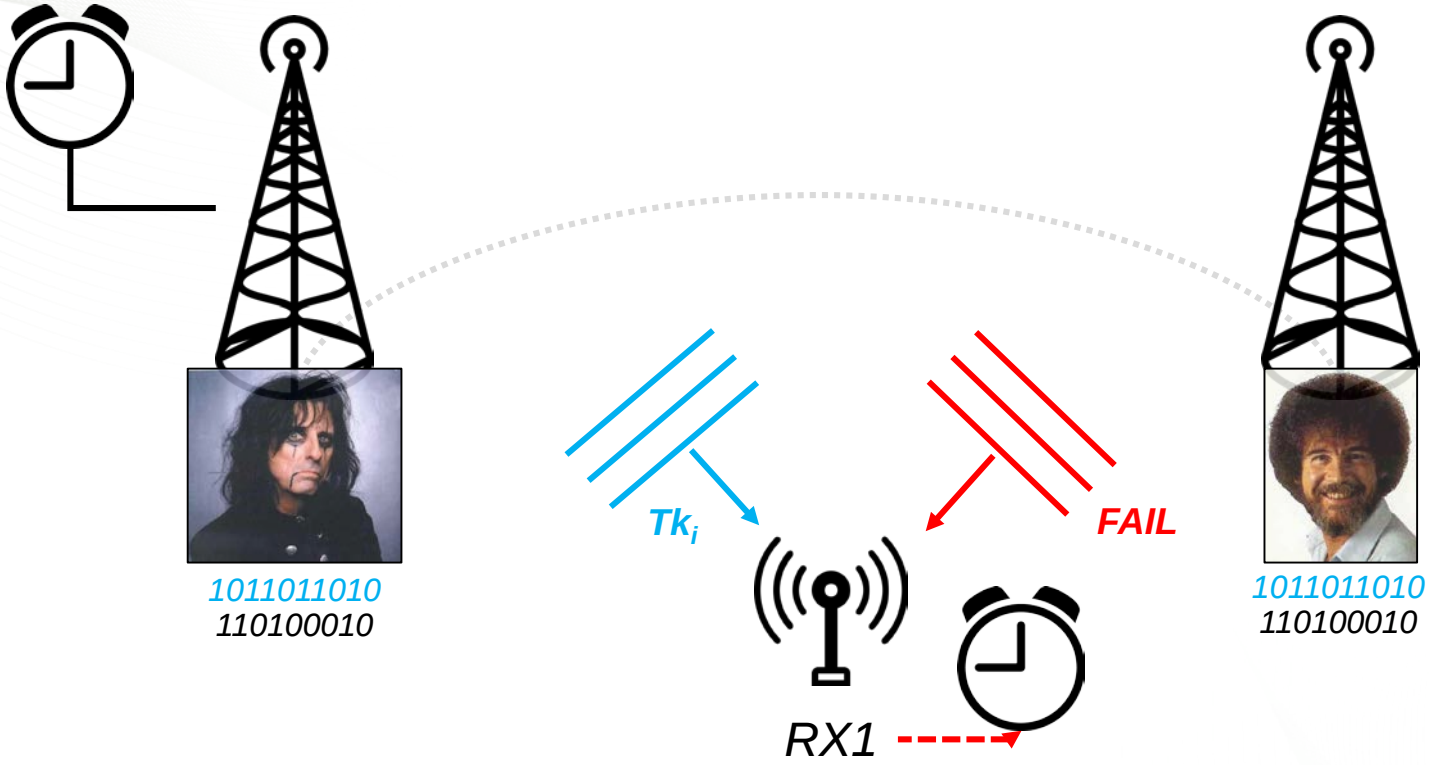
(3) *RX1* receives two messages - Tk_i from *Alice*, k_i or FAIL from *Bob* - and time tags their arrival with its local clock

TASQC 2-Way Secure Time Protocol



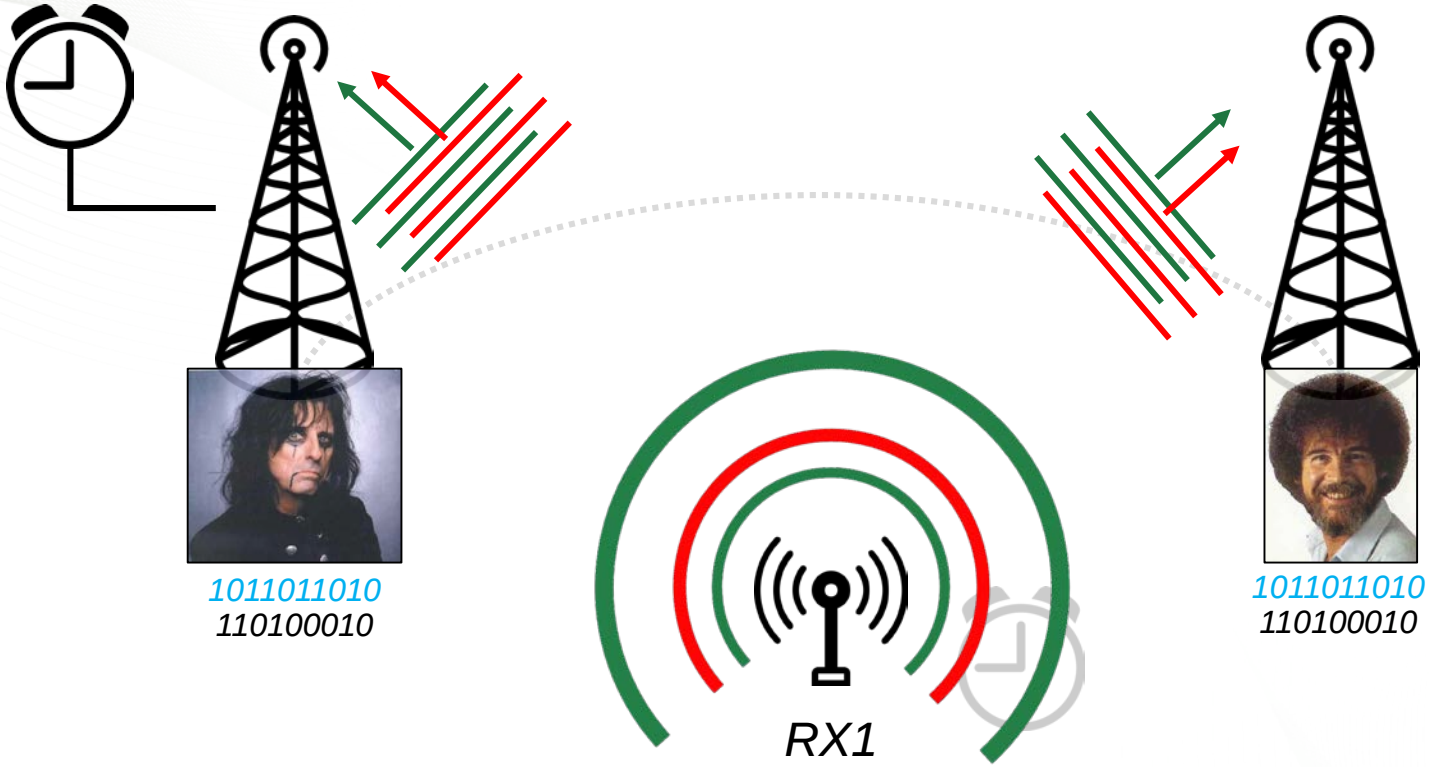
(4a) If k_i, Tk_i is decrypted, the Master Clock time recovered. ToF corrections are applied and *RX1*'s local clock is updated.

TASQC 2-Way Secure Time Protocol



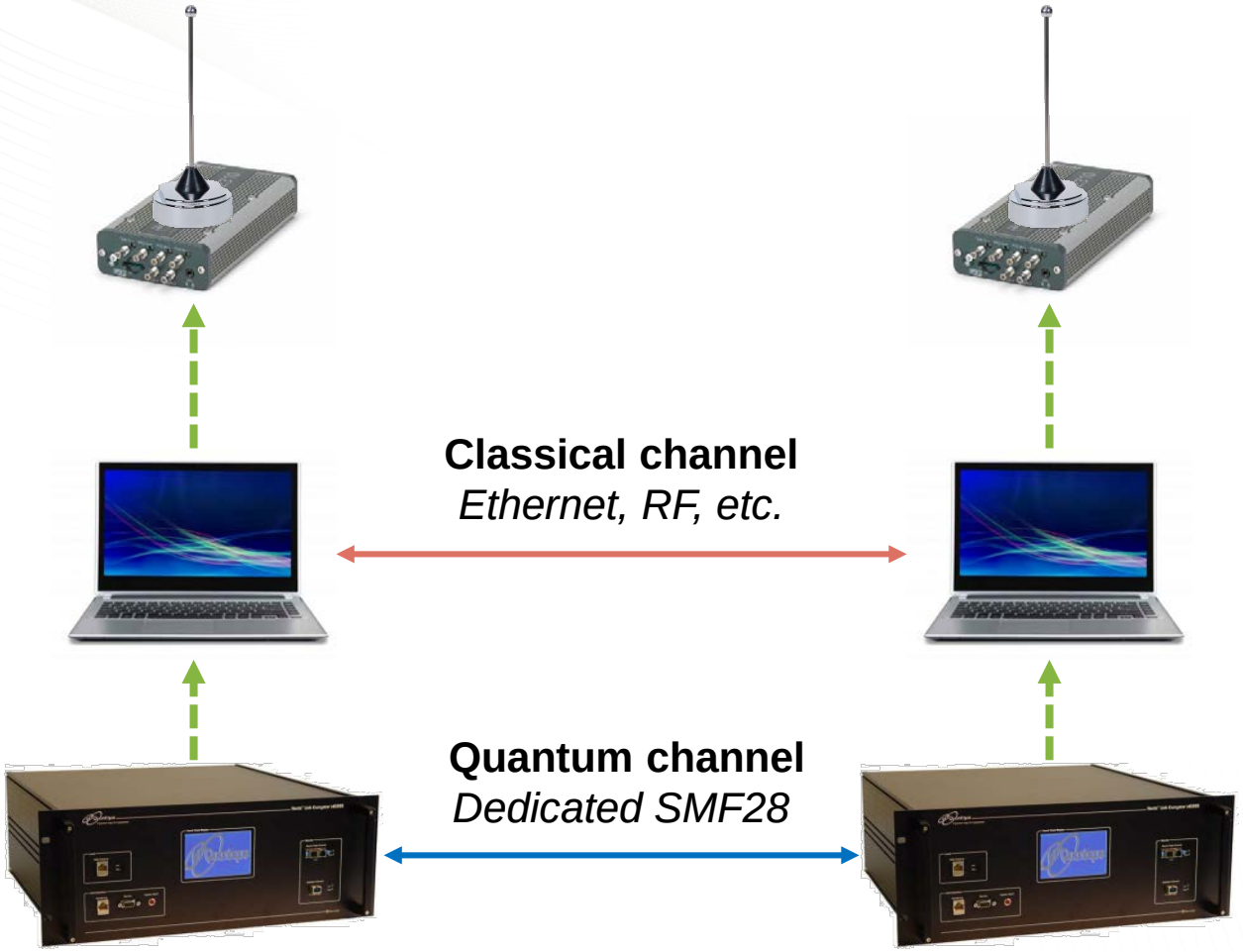
(4b) If FAIL, messages are discarded. *RX1* continues to flywheel.

TASQC 2-Way Secure Time Protocol



(5) *RX1* generates SUCCESS or FAIL messages and broadcasts. These are received by both *Alice* and *Bob*.

TASQC Implementation - TX



RF Hardware
Ettus SDRs
902-928 MHz ISM

QKD Controllers
Ubuntu Linux machines

QKD Hardware
e.g., IDQ Clavis2

TASQC Implementation - RX

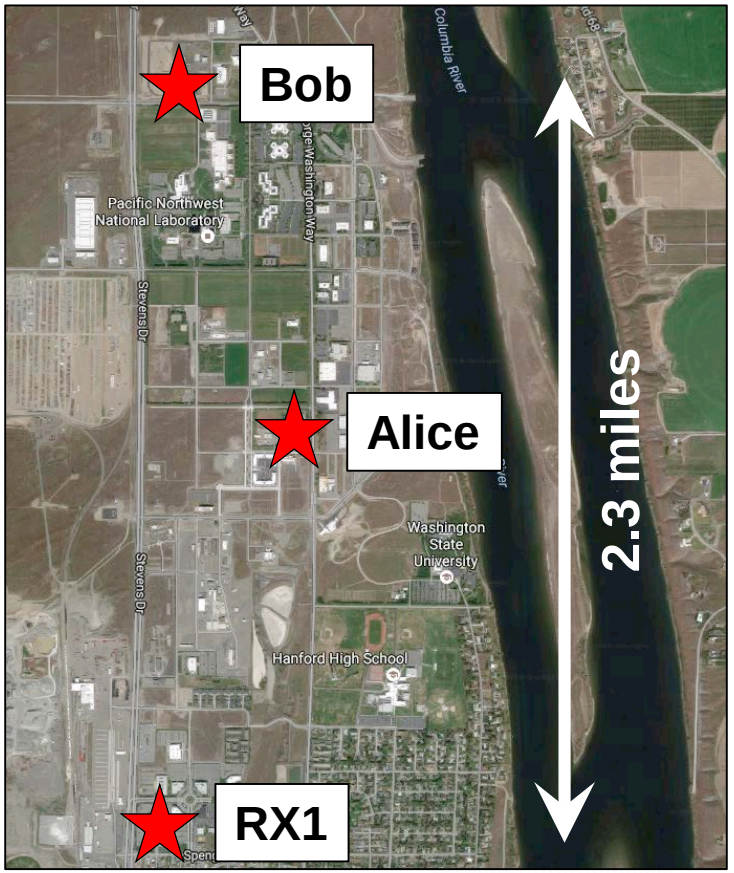
RF Hardware
Ettus SDRs
902-928 MHz ISM

Time Correction & Signal Generation
ToF calculations; generation of IRIG-B, IEEE-1588 (PTP) signals

Power systems device
e.g., PMU

Field Tests @ PNNL

- QKD running in background on PNNL fiber network
  - Sustained ~2.5 kbps @ < 1% QBER
  - A, B receive QKD keys via *keyTrans*
- 1-way time transfer ✓
- 2-way time transfer ✓
- Secure message passing ✓
- Remote test bed setup ✓



TASQC system functionality demonstrated

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 crypto
  - Leveraging provably secure communications
- **Demonstrated use cases**
- **Increased quantum adoption in cyber systems**
  - critical infrastructure to follow!


Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965


Sandia
National
Laboratories


THE UNIVERSITY OF
TEXAS
AT AUSTIN


Qubitekk

Questions?