Warren Grice

Oak Ridge National Lab

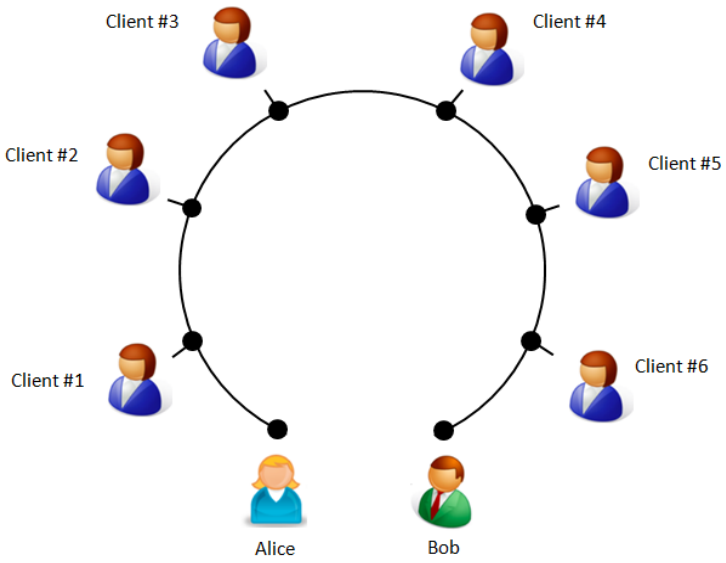
Practical Quantum Security for Grid Automation

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary: Practical Quantum Security for Grid Automation

- **Objective**
  - Develop and demonstrate a novel quantum encryption technology that improves the versatility and accessibility of QKD.
  - Incorporate that technology into commercial grid instrumentation.
- **Schedule**
  - Start Dec. 2012; End Oct. 2015
  - Key deliverables:
    - ✓ 08/23/2013: AQCESS technology demonstrated
    - ✓ 11/15/2013: Prototype design complete
    - 09/19/2014: Prototype testing complete
    - 09/02/2015: Field tests complete
  - New capability: Cost-effective and accessible quantum security for the grid



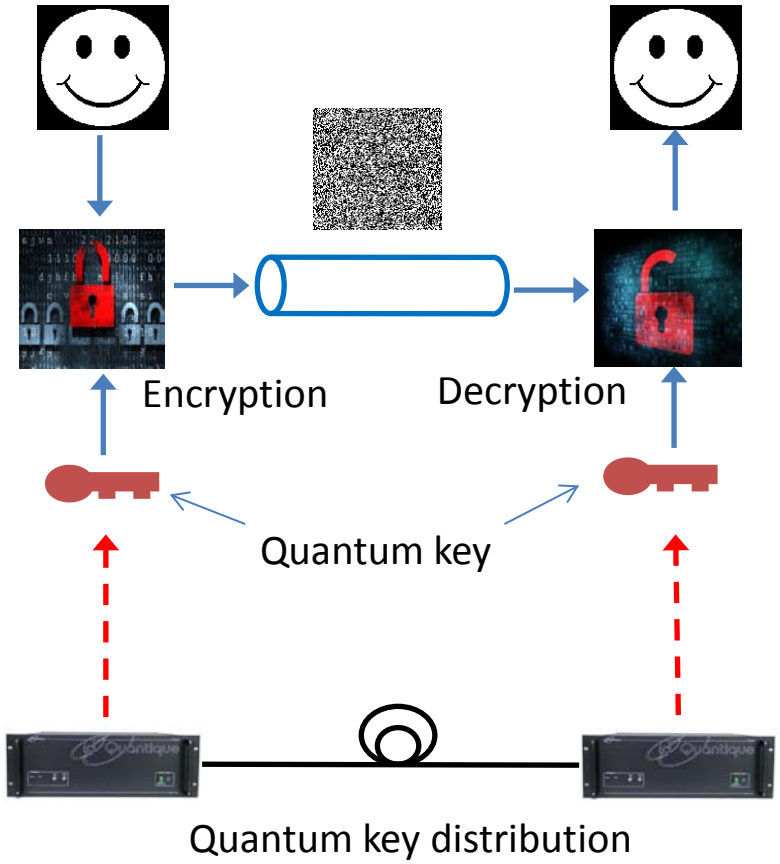
- **Total Value of Award:** $ 2.9M
- **% Funds expended to date:** 57%
- **Performer:** Oak Ridge National Lab
- **Partners:** GE, ID Quantique

Security of cryptographic system is largely dependent on secrecy of encryption key

- **Symmetric ciphers, such as Advanced Encryption Standard (AES), are commonly employed in modern cryptographic systems**
  - Pre-shared encryption keys are required
  - NSA recommends AES with 256-bit keys for TOP SECRET information
- **Asymmetric ciphers, such as RSA and Elliptic Curve Cryptography (ECC), can be employed to distributed encryption key**
  - Security of asymmetric ciphers are based on unproven mathematical assumptions (**insecure** once a quantum computer is available)
  - Computationally intense (NIST key management guidelines suggest AES with a 256-bit key requires a 512-bit ECC key size or a 15,360-bit RSA key size)

Enhance modern cryptographic systems with quantum keys

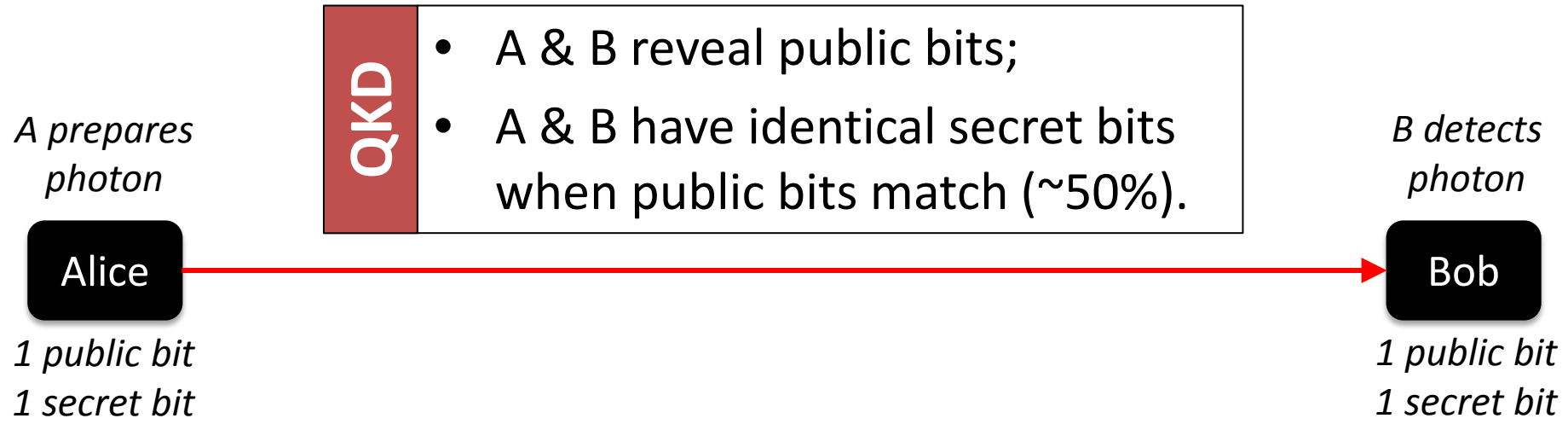
- **Quantum key distribution (QKD) is the only existing key distribution protocol with proven security**
  - The security of QKD is based on fundamental laws in physics
  - Simple key generation algorithm
  - Speed of state of the art QKD system is above 1Mbits/second, much faster than the speed of asymmetric ciphers
- **Quantum keys can be applied in any cryptographic protocols where a key is required!**



Advancing the State of the Art (SOA)

- **Classical Encryption**
  - Key security is critical
- **QKD is a proven technology, but has not been applied to grid security (unique needs; unique opportunities)**
- **QKD traditionally is limited to two parties**
- **This project**
  - Makes QKD cost-effective and accessible to multiple parties
  - Integrates QKD into commercial grid instrumentation

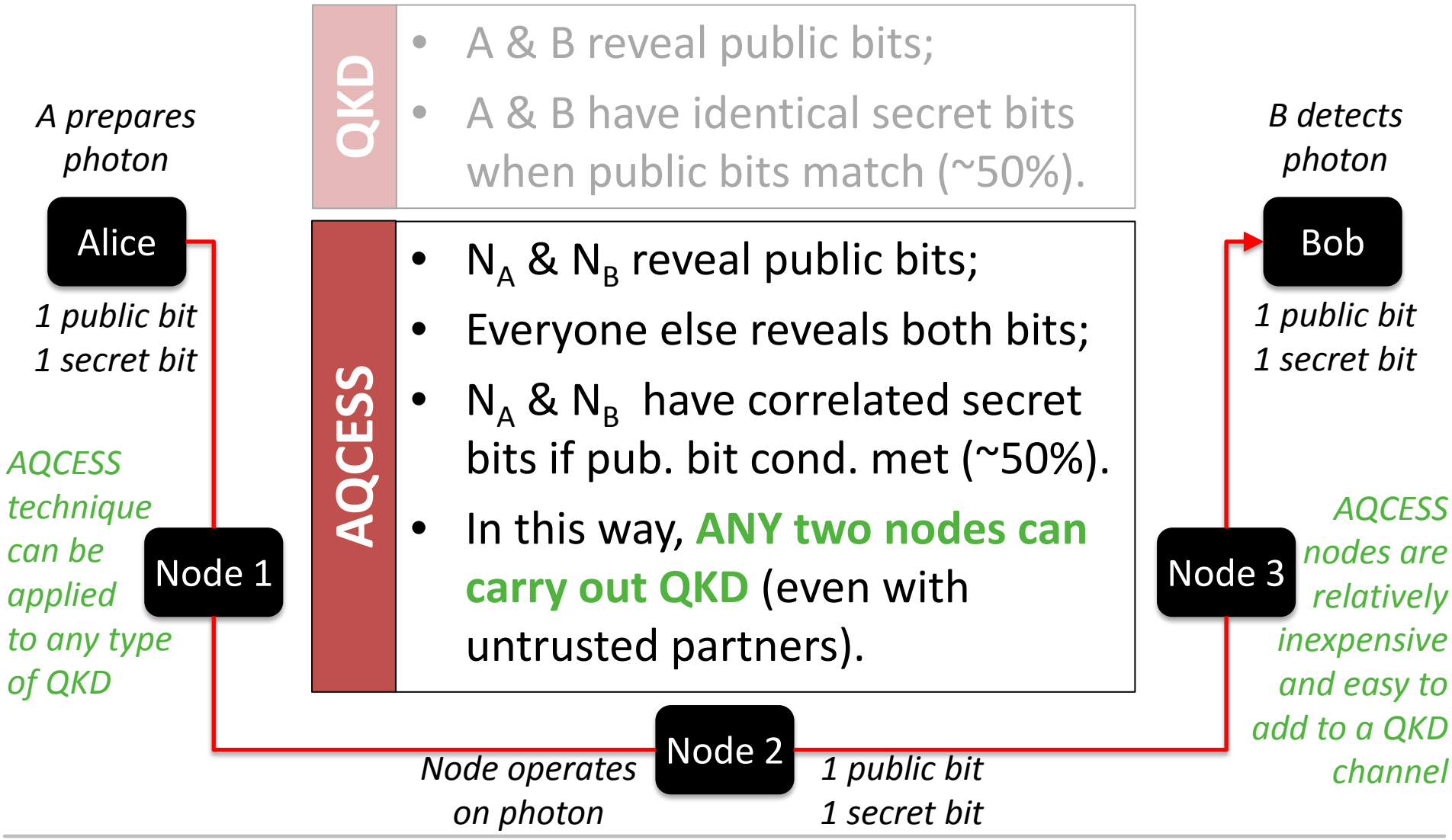
Accessible QKD for Cost-Effective Secret Sharing (AQCESS)



Problem: QKD only supports two parties

- A separate QKD link is required for every pair of clients who need to share a key!

Accessible QKD for Cost-Effective Secret Sharing (AQCESS)



Project Team

Oak Ridge National Laboratory

- *AQCESS technology*
- *System integration*

GE Global Research

- *Power Systems instrumentation*

ID Quantique

- *QKD systems and technology*

Challenges to Success

- **Challenge 1: Export control restrictions**
  - Patience…
  - Re-distribution of responsibilities
- **Challenge 2: Proof-of-Concept demonstration required some "un-engineering"**
  - Lots of help from ID Quantique
- **Challenge 3: Grid community ≠ QKD community**
  - Emphasis on building a system that can be used with existing grid instrumentation
  - Ongoing dialog

Progress to Date

- **Major Accomplishments**
  - Modulation of QKD signal demonstrated 06/21/2013
  - QKD with AQCESS node demonstrated 09/13/2013
  - GE device (JungleMUX) selected for prototype integration 09/27/2013
  - Prototype design complete 11/15/2013
  - Hardware modifications for AQCESS module complete 04/18/2014
  - JungleMUX authentication key uploaded via FTP connection 04/18/2014

Device Selection: JungleMUX

- **Selection Criteria**
  - Power impacted; Information impacted; Service area
- **Selection Method**
  - 400+ GE products evaluated; top candidates reviewed by project team
- **Selection: JungleMUX SONET Multiplexer**
  - Handles large data volume with large power impact
  - QKD key will be used for access control

Collaboration/Technology Transfer

- **Technical paper soon; two conference presentations**
- **Participation on IEC TC 57 WG 15 (SFB)**
  - TC 57 is responsible for development of standards for information exchange for power systems and other related systems including Energy Management Systems, SCADA, distribution automation & teleprotection
  - WG 15 is focused upon Data & Communication Security (IEC 62351)
- **Disseminating the Results to Users: JungleMUX Users Conference**
- **Other (contact W. Grice)**

Next Steps for this Project

- **FY14**
  - Complete prototype testing
- **FY15**
  - Build additional prototype modules
  - Devise field test plan and carry out field tests
  - Disseminate results