U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Scalable Quantum Cybersecurity for Energy Storage Systems (SEQCESS) Oak Ridge National Laboratory

M. Alshowkan, D. Earl, P. Evans, W. Grice, B. Qi, M. Starke, B. Williams & N. A. Peters (Presenting)

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

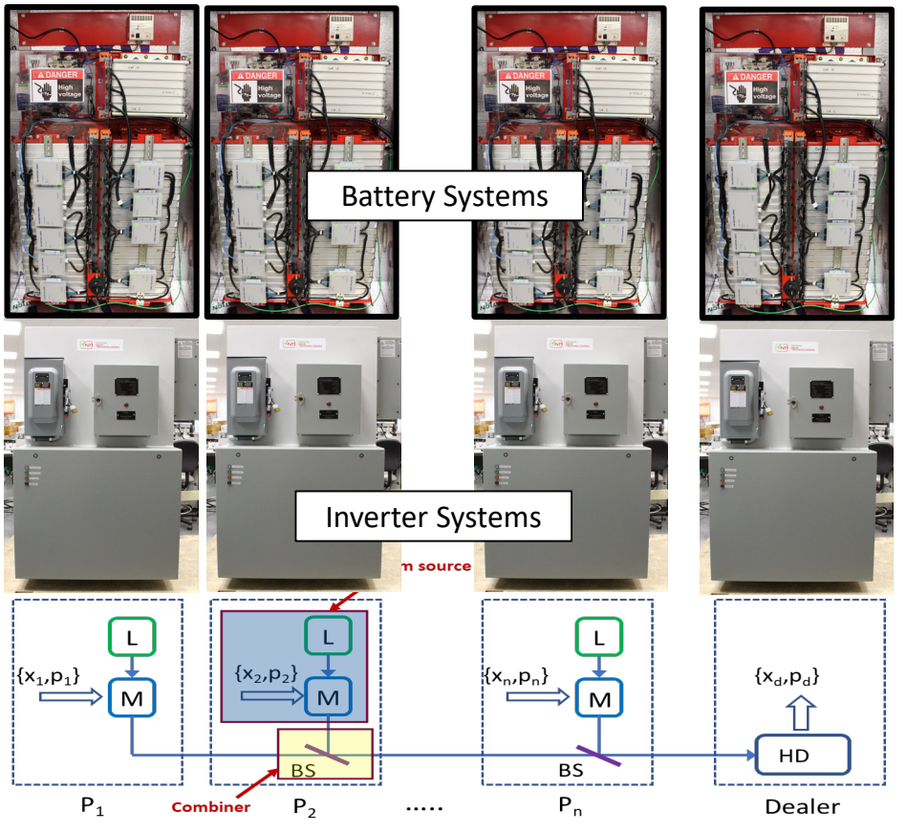
Scalable Quantum Cybersecurity for Energy Storage Systems (SEQCESS)

Objective

- Develop quantum communications interface to classical communications.
- Authenticate a single user to a single Distributed Energy Storage (DES) node.
- Enable single-to-many quantum secured communications to distributed DES nodes.

Schedule

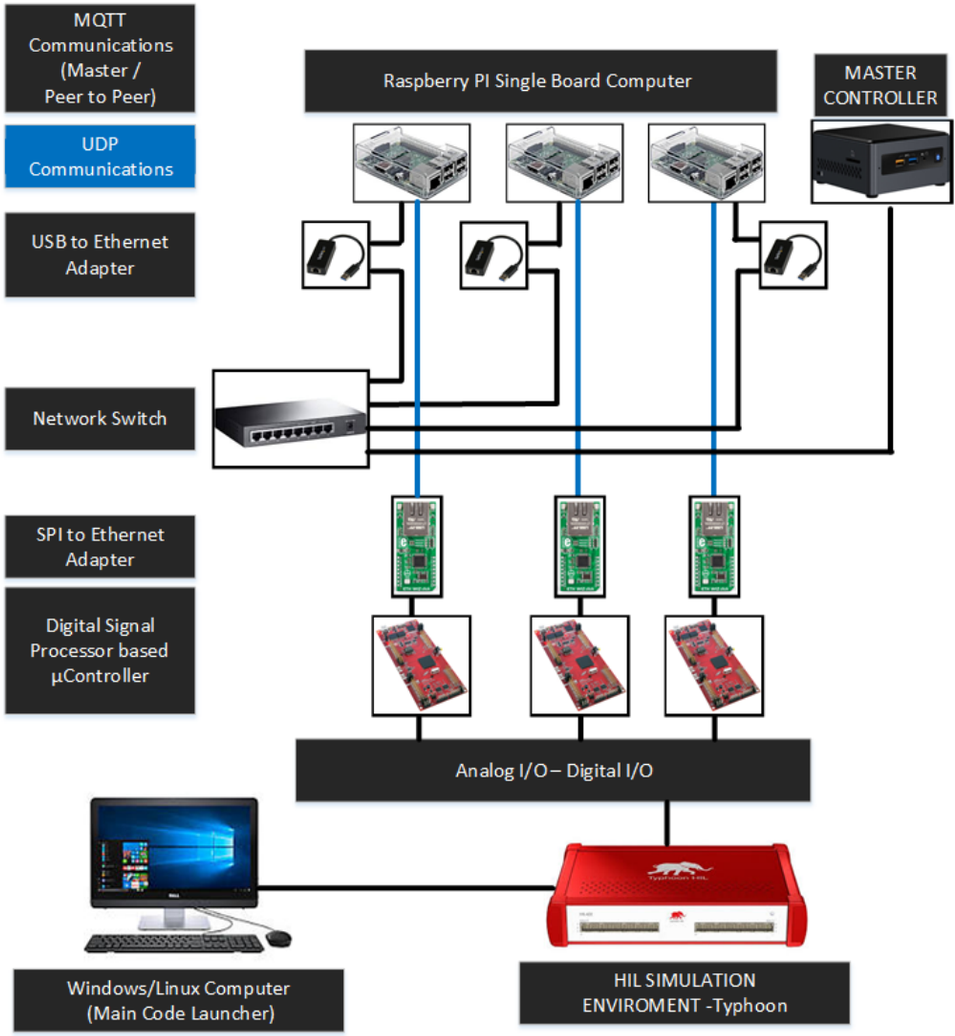
- 10/01/2019-09/30/2022
- Theme 1: Use commercial quantum key distribution for authentication (point to point).
- Theme 2: Develop new point-to-multi-point quantum protocols for authentication.
- Quantum-based long-lasting authentication will be interfaced to to the general energy SCADA communications.



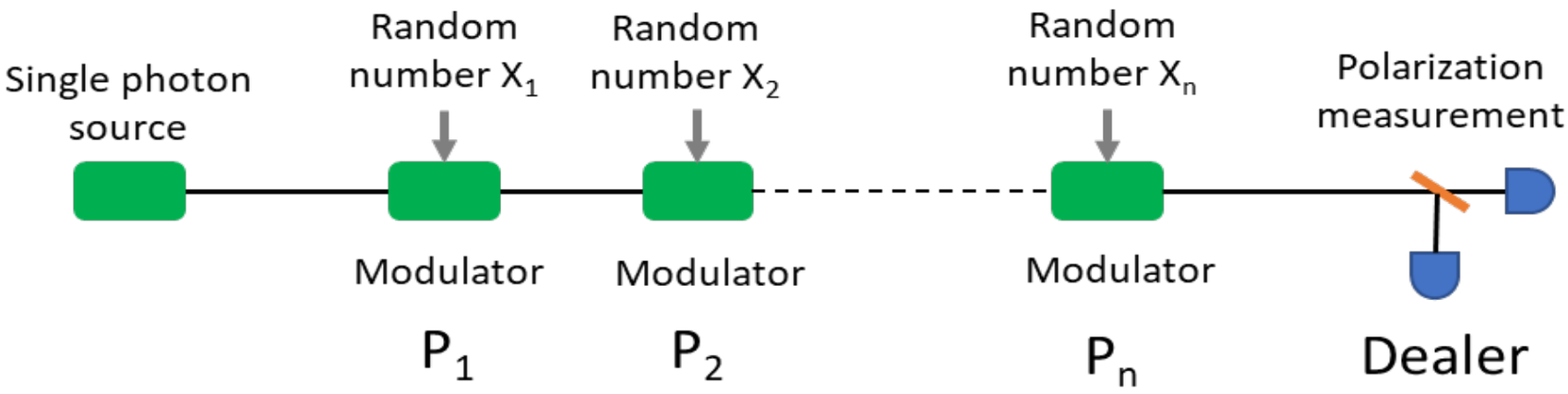
Total Value of Award:	**$3,194,000**
Funds Expended to Date:	**18 (38 committed)%**
Performer:	**ORNL**
Partners:	**EPB, Qubitekk, LANL**

Advancing the State of the Art (SOA)

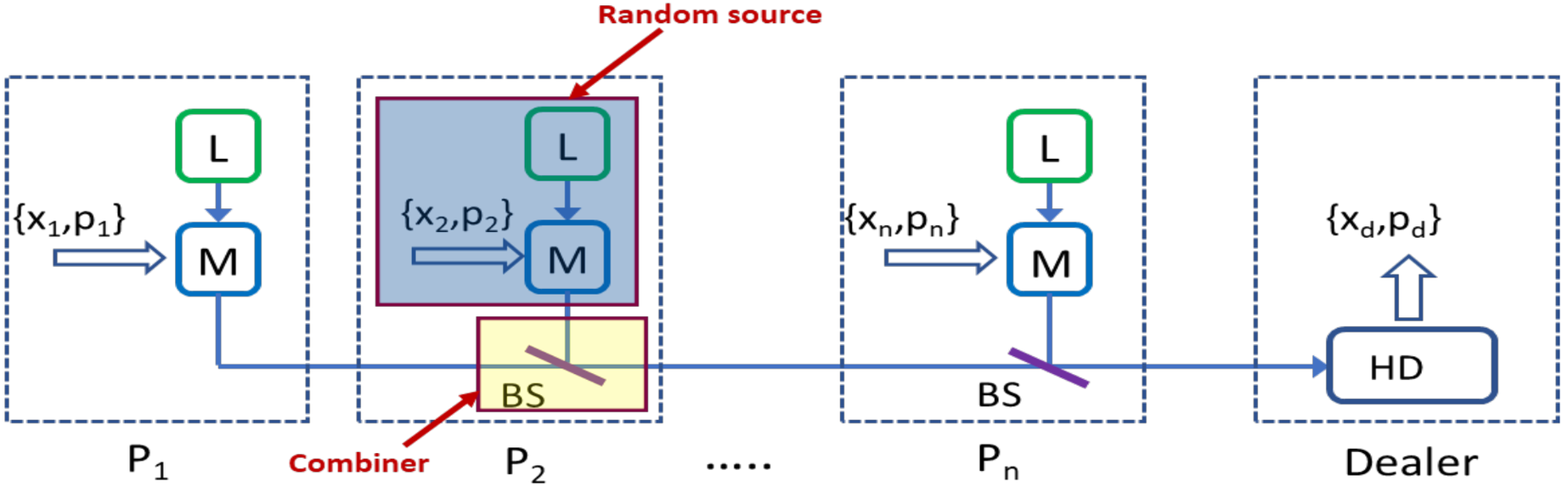
- "State of the art" ORNL Distributed Energy Storage (DES) communicates using Message Queuing Telemetry Transport (MQTT) publish/subscribe protocol.
- We are using quantum resources to build authentication into these communications.
- Authentication has "information theoretic" security – i.e., independent of computational sophistication assumptions, so it lasts lifetime of infrastructure.
- Messages remain in clear text so if anything breaks one can still see data.
- Strong authentication gives confidence data is genuine revealing adversarial manipulation.



Advancing the SOA: Secret Sharing



Problem: Trojan-horse attack—an adversary may send faked signals to the modulators and read out the encoded random number.



Solution: Remove modulator & inject quantum signal.

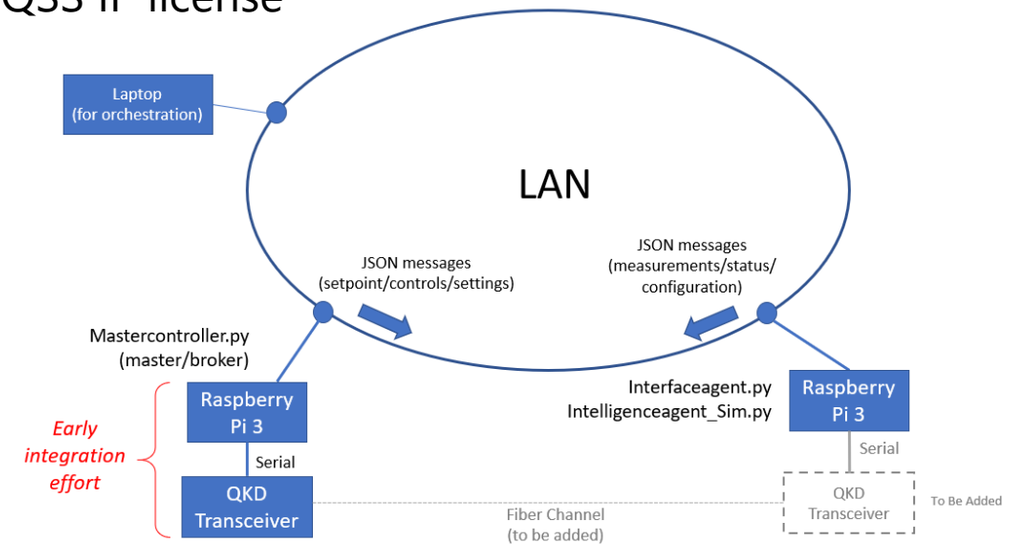
U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

W. P. Grice and B. Qi, "Quantum secret sharing using weak coherent states", Phys. Rev. A 100 022339 (2019).

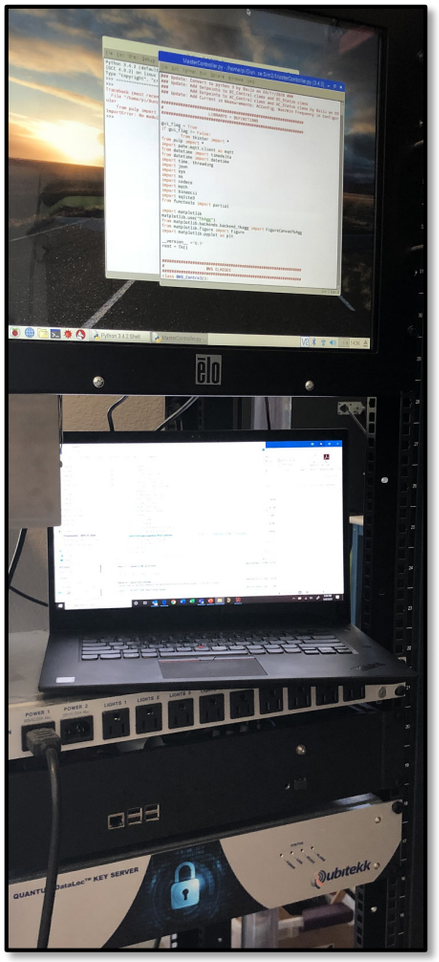
Progress to Date

Major Accomplishments

- Integration of ORNL emulators with physical QKD hardware (at Qubitekk).
- Integration of Qubitekk QKD emulators with ORNL hardware (at ORNL).
- Exploration of key transfer protocols and incorporation of keys into ORNL's lightweight authentication and encryption protocol.
- Construction of dedicated network for testing.
- Subcontracts in place September 2020.
- QSS IP license



Dedicated network at Qubitekk for integration testing.



Rackmount devices at Qubitekk for integration development

Challenges to Success

Challenge 1: COVID19 restrictions make it difficult to get into locations and slow collaboration

- Lab work moved to “shifts” to minimize people density.
- Focus on utility demo prep work so we are ready to go when a window of opportunity opens.
- Early focus on theory which could be done from home.
- Maximized remote work, both from home offices but also, by sharing resources between CA and TN.

Challenge 2: Subcontracting delays/personnel changes

- Started subcontracting process (SOW development) as soon as we learned of funding.
- Ordered required materials early.

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

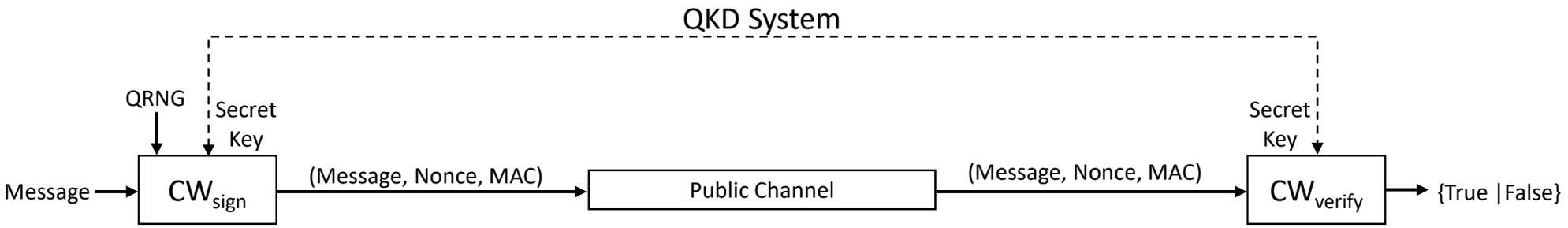
- Work with partners to directly transfer results.
- Quantum Tech Transition Website: https://quantumsciencetechnology.ornl.gov/technologies-available-for-licensing/
- Plans to gain industry acceptance: Yearly tests planned at EPB in Chattanooga & Red team review by LANL.
- Sector adoption can take place along with QKD system use.

Next Steps for this Project

Approach for the next year or to the end of project

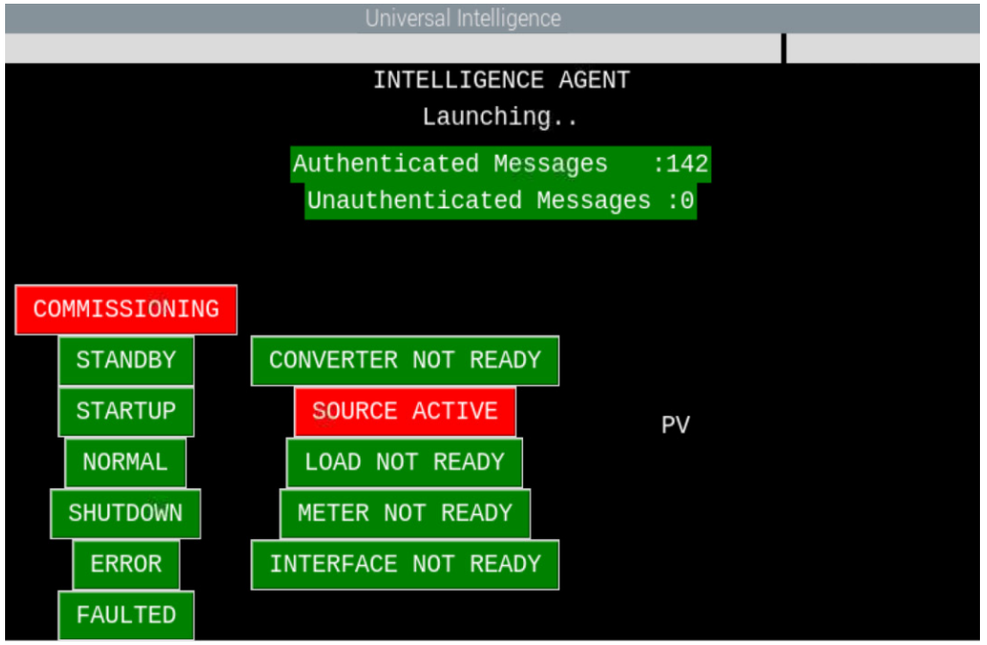
- Demo of Qubitekk keyed authentication of MQTT DES communications at EPB at the end of October.
- Develop Quantum Secret Sharing hardware with continuous variable encodings – good for networks with classical traffic.
- Develop Quantum Digital Signature System with Qubitekk Polarization Entanglement Hardware.

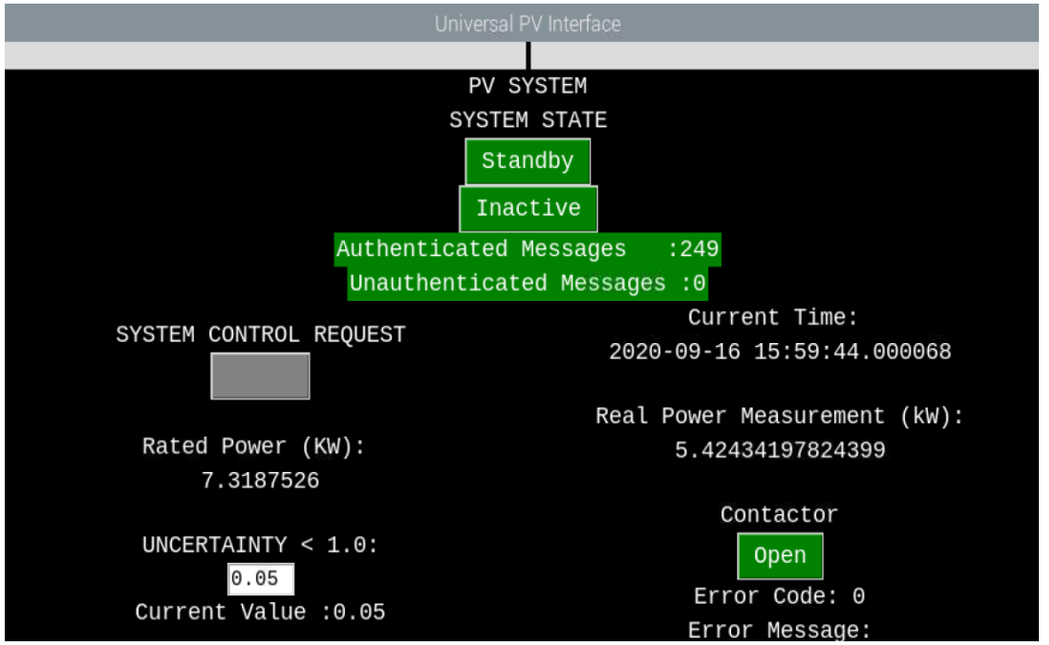
Signing and Verification



- **Key Management**
  - Retrieve key material as a string of bits.
  - Verify the key length is 256-bit.
  - Associate each key with an arbitrary identifier.
  - Create a key table with Boolean status flag.
- **Random numbers Management**
  - Retrieve random number from QRNG as binary file.
  - Process the large binary file to 128-bit chunks.
  - Associate each number with an arbitrary identifier.

Successful authentication of published messages





Match

```
Standby--PV/State--1600288314--7380
Key:    56031090556694191636151677483690230086325472504571419961418682364552695386879
Nonce:  de5ce87aa0a1a1fa6ece2769b8e79933
MAC:    4ce0281a85daea4d2a0d9f620c5711a9
```

Publisher

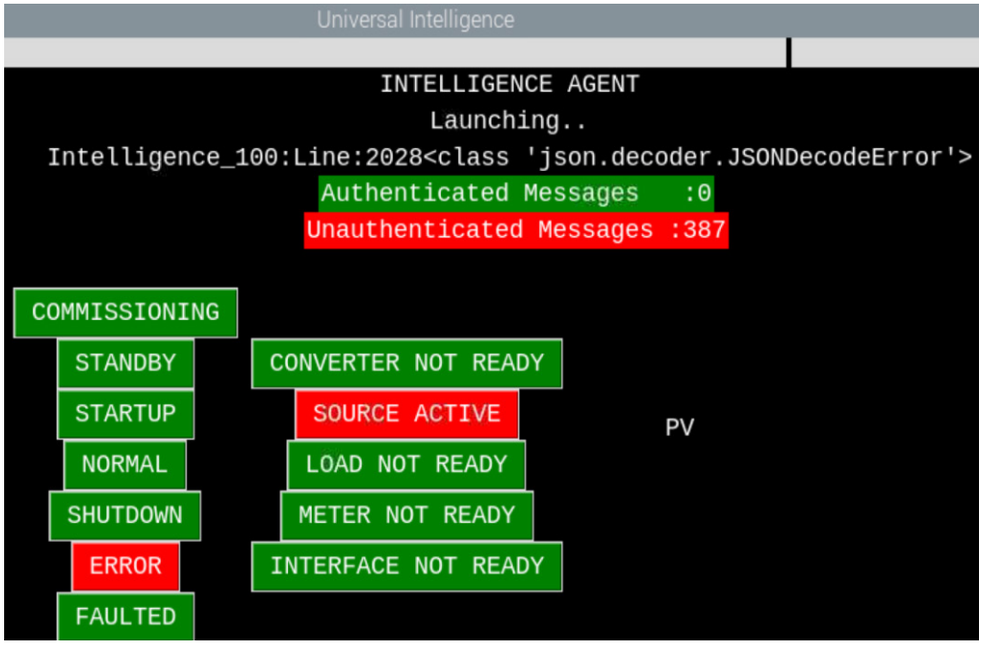
```
Standby--PV/State--1600288314--7380--de5ce87aa0a1a1fa6ece2769b8e79933--4ce0281a85daea4d2a0d9f620c5711a9
Key:    56031090556694191636151677483690230086325472504571419961418682364552695386879
Nonce:  de5ce87aa0a1a1fa6ece2769b8e79933
MAC:    4ce0281a85daea4d2a0d9f620c5711a9
The message is authentic
```

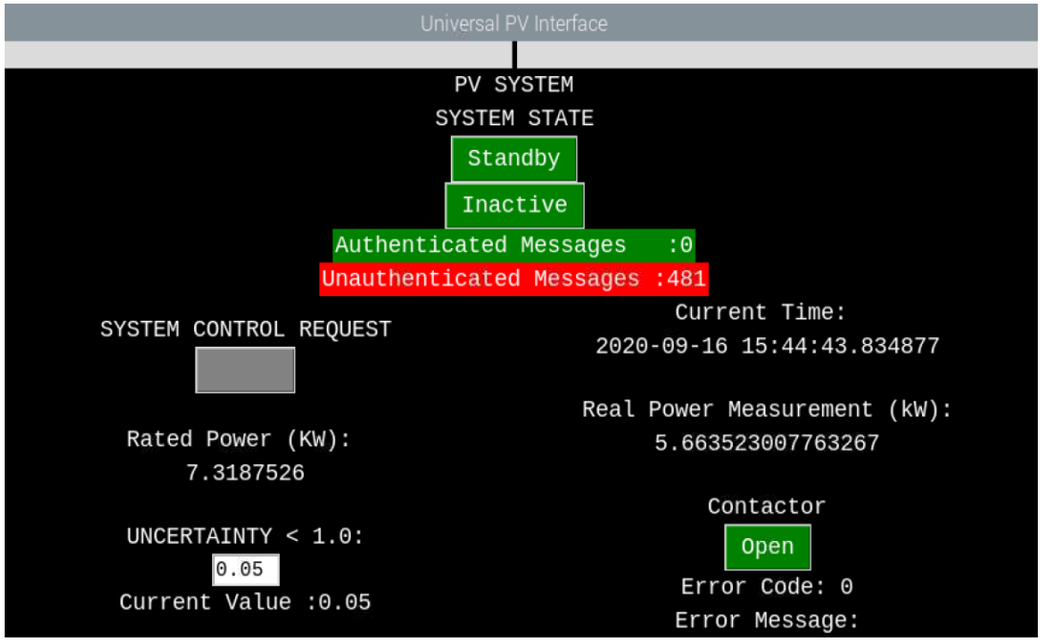
Subscriber

Authenticated

Publisher and subscriber share **valid** secret keys

Unsuccessful authentication of published messages





Invalid

```
Standby--PV/State--1600284321--170
Key:    377697945612338772585243686256097708172547655914783199952842424936382255209 40
Nonce:  55aebd3aa526b0bc9fb2ab832893063c
MAC:    adf924105fd72baab413e04efb1eabe5
```

Publisher

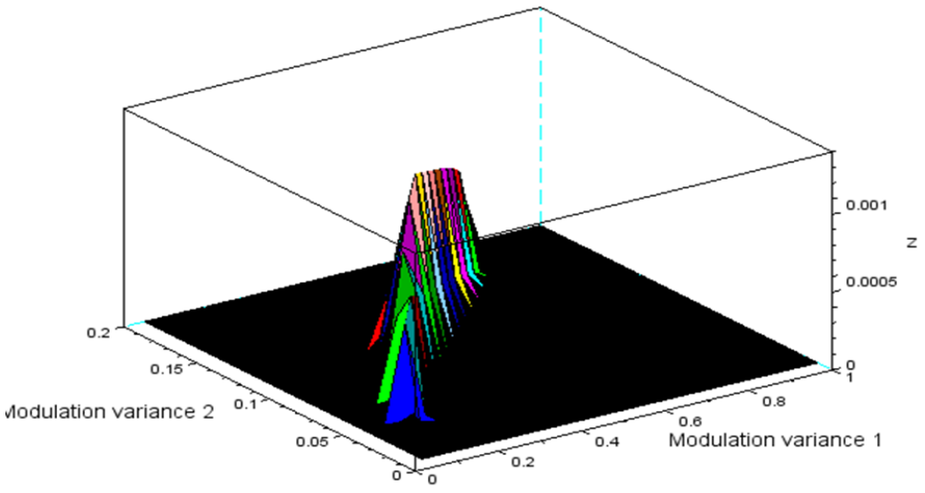
```
Standby--PV/State--1600284321--170--55aebd3aa526b0bc9fb2ab832893063c--adf924105fd72baab413e04efb1eabe5
Key:    165753795101510001037640841543139715020911952655967189114173746786460345980 33
Nonce:  55aebd3aa526b0bc9fb2ab832893063c
MAC:    adf924105fd72baab413e04efb1eabe5
Error: cannot authenticate the message!
```

Subscriber

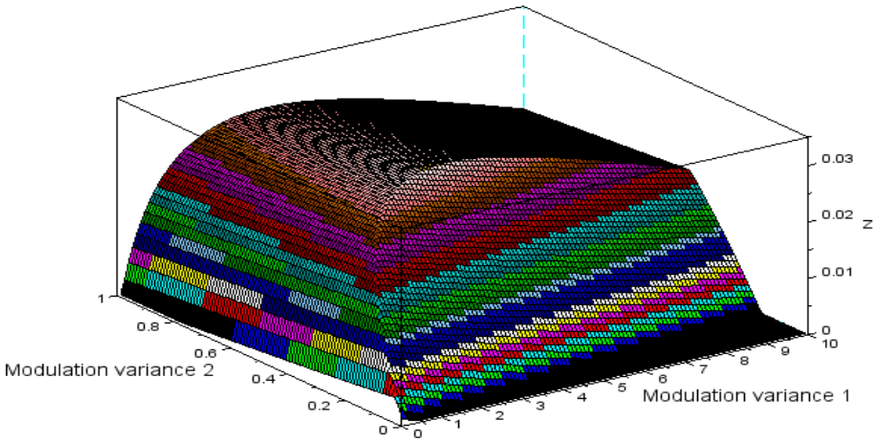
Unauthenticated

Publisher and subscriber share **invalid** secret keys

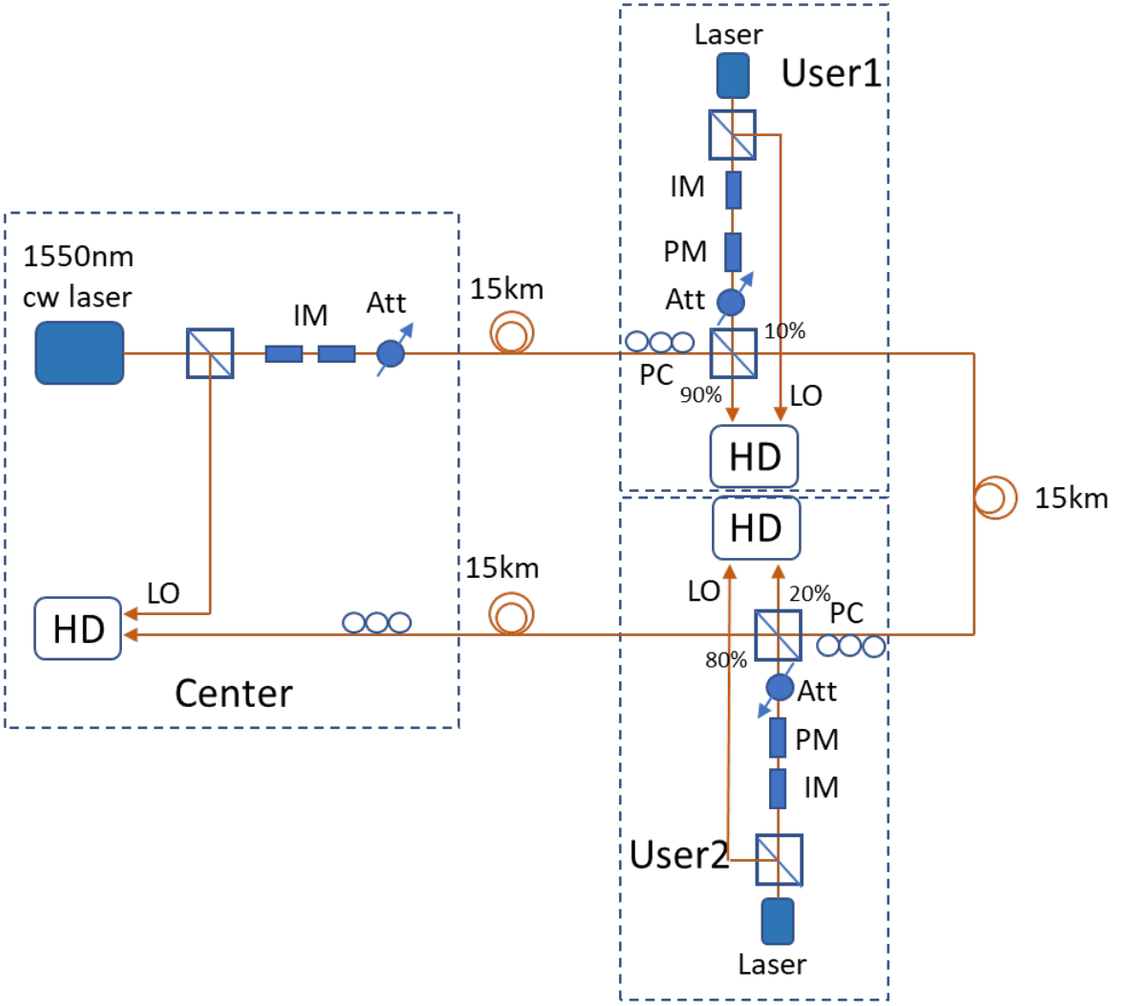
Three-party CV QSS design and simulation



Simulation results with 150KHz laser



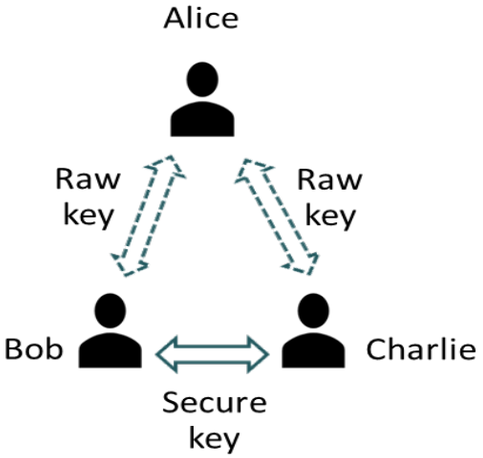
Simulation results with 10KHz laser



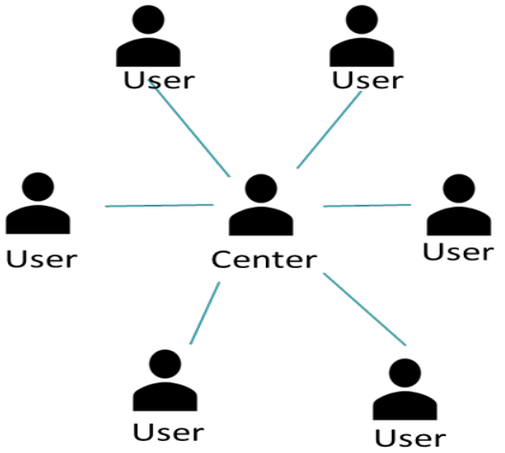
Proposed setup

Quantum digital signature

- Digital signatures can offer authenticity and integrity, non-repudiation, and transferability;
- Classical digital signatures are based on public key crypto, such as RSA, so cannot provide information-theoretic security (ITS);
- Quantum digital signature (QDS) can have proven security and can be implemented using QKD infrastructure;
- Existing QDS protocols lack the feature of universal verifiability and cannot completely replace digital signatures based on PKI.



Prior Art



Proposed scheme using EPR source