ARMD Transformative Aeronautics Concepts Program

CONVERGENT AERONAUTICS SOLUTIONS PROJECT

QTech

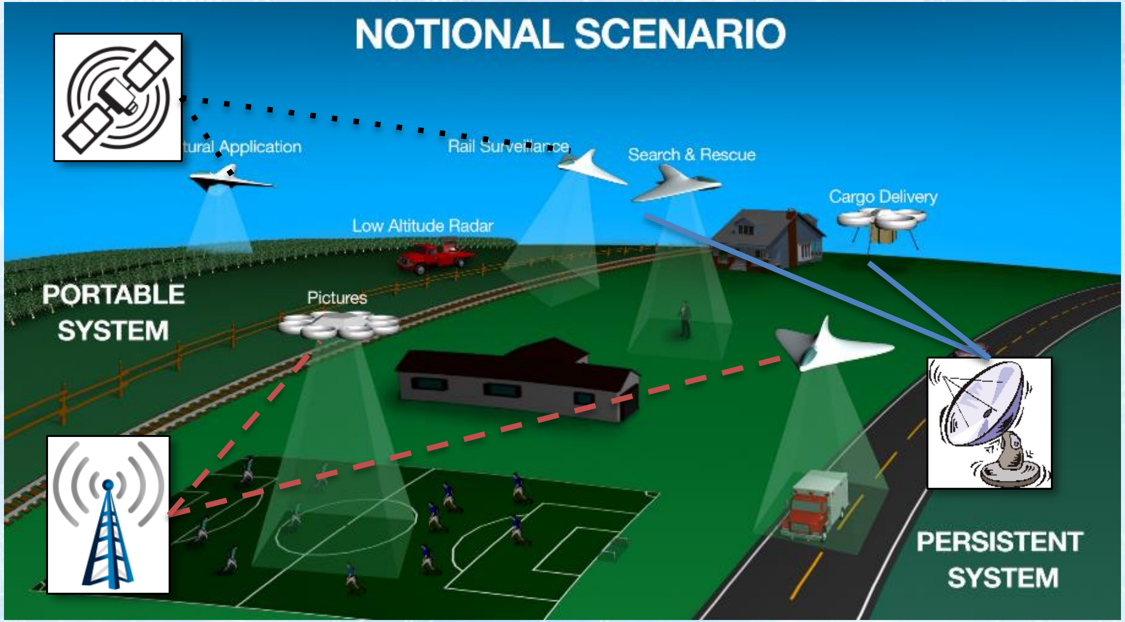
Eleanor Rieffel
ARC – Quantum Computing

Adam Wroblewski
GRC – Quantum Communications

13 November 2019

Challenge

Assure the **availability** of the UAS Traffic Management (UTM) network against communication disruptions



Kopardekar, P., Rios, J., et. al., *Unmanned Aircraft System Traffic Management (UTM) Concept of Operations, DASC 2016*

Background: Components of UAS cybersecurity

Secure communications requires:

Confidentiality (C) concerns keeping communicated data private

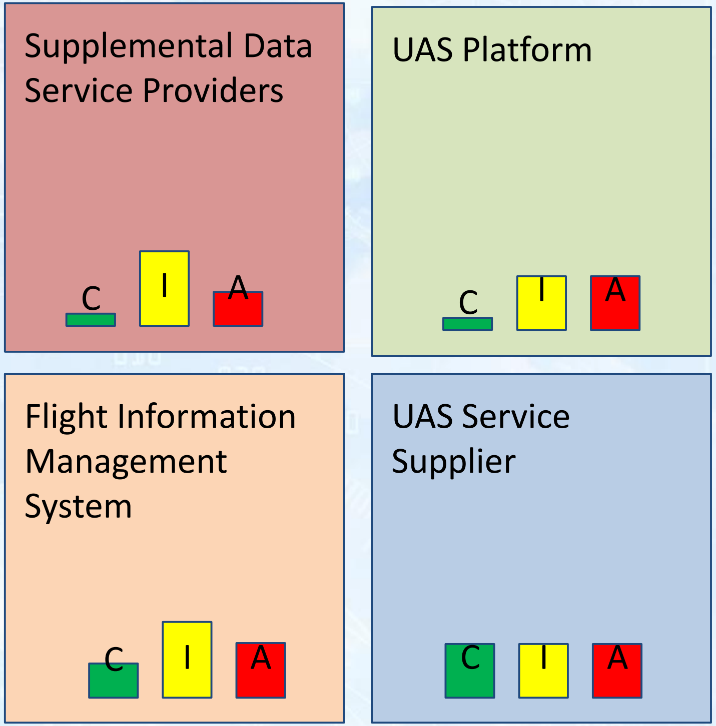
– Less of a concern

Integrity (I) concerns ensuring that messages received come from the expected sender and have not been tampered with

– Good classical solutions exist

Availability (A) concerns ensuring messages get there in the first place

– Biggest challenge

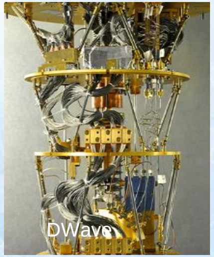


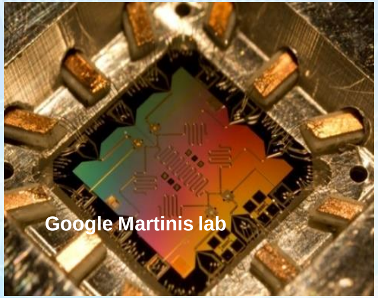
From J. Rios (NASA ARC, Chief engineer for UTM): Relative Importance of Confidentiality, Integrity, and Availability for UTM

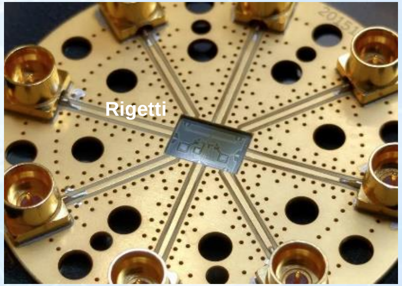
Idea/Concept

We propose a revolutionary approach to the 'Availability' challenge for UAS operations:

Harness the power of quantum computing and communication to address the cybersecurity challenge of <u>availability</u>





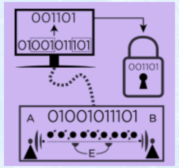


Proposed solution/approach

Quantum computing algorithms and **quantum communication** protocols to address challenges in **Availability**

– Quantum optimization algorithms to design **robust networks**

– Utilize quantum optimization algorithms **resource allocation**



– Utilize quantum key distribution (QKD) to execute secure **key sharing** in anti-jamming protocols for RF communication

What is quantum computing?

Quantum effects

quantum interference

quantum tunneling

quantum entanglement

quantum measurement

quantum many-body delocalization

quantum sampling

etc.

Encoding information in a non-classical, quantum way

Take advantage of uniquely quantum effects

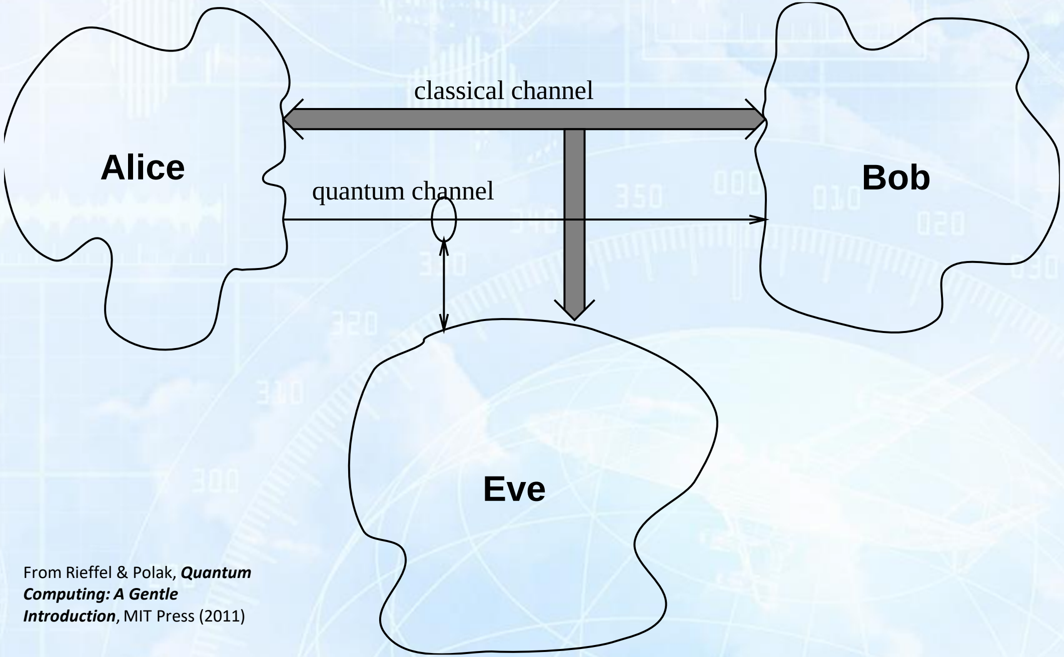
Quantum effects can provide more efficient computation and higher levels of security

- What Shor's factoring algorithm can compute in days, would take a supercomputer longer than the age of the universe

Emerging quantum hardware enables empirical investigation of quantum optimization for myriad applications

What is quantum key distribution (QKD)?

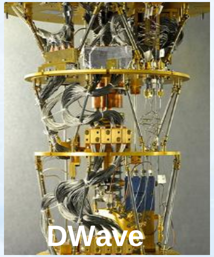
QKD provides means to **securely exchange encryption keys**, to use for subsequent data encryption/decryption



From Rieffel & Polak, ***Quantum Computing: A Gentle Introduction***, MIT Press (2011)

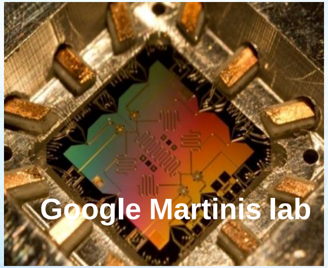
Two types of quantum computing devices

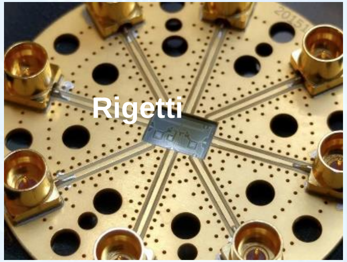
Quantum Annealers: *special-purpose* quantum optimization hardware



All devices are small:
must devise representative problem classes of small problems to evaluate feasibility

General-purpose **gate-model quantum processors**





HPC simulation of quantum circuits

Advanced the state-of-the-art

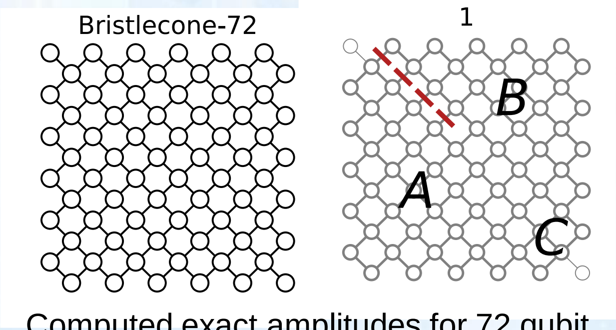
- **can simulate larger quantum circuits than any previous approach**
- **judicious use of cuts within a tensor network**
- **HPC memory tricks and trade-offs**
- **can flexibly incorporate fidelity goal**

Largest computation run on NASA HPC clusters

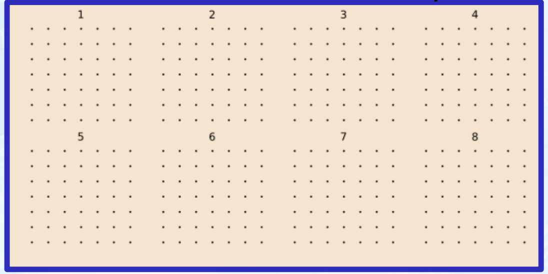
- **60-qubit subgraph, depth 1+32+1**
- **116,611 processes on 13,059 nodes, peak of 20 PFLOPS, 64% of max**
- **across Pleiades, Electra, Hyperwall**

Applications

- **benchmark emerging quantum hardware**
- **quantum supremacy experiments**
- **empirically explore quantum algorithms**



Computed exact amplitudes for 72 qubit Bristlecone random circuit, depth 1+32+1



Villalonga et al., ***A flexible high-performance simulator for the verification and benchmarking of quantum circuits implemented on real hardware***. arXiv:1811.09599

Villalonga et al., ***Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation***, arXiv:1905.00444

New era for quantum computing

Quantum supremacy has been achieved!

- Perform computations not possible on even the largest supercomputers

… but not <u>useful</u> quantum supremacy.

- Currently too small to be useful for solving practical problems

Article

Quantum supremacy using a programmable superconducting processor

Cover article, Nature, 24 Oct 2019

Google, NASA, ORNL collaboration

Unprecedented opportunity to explore and evaluate quantum algorithms empirically

Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation

Benjamin Villalonga, Dmitry Lyakh, Sergio Boixo, Hartmut Neven, Travis S. Humble, Rupak Biswas, Eleanor G. Rieffel, Alan Ho, and Salvatore Mandrà

Joint work with Google establishing the quantum supremacy frontier

npj | Quantum Information

ARTICLE OPEN

A flexible high-performance simulator for verifying and benchmarking quantum circuits implemented on real hardware

Benjamin Villalonga, Sergio Boixo, Bron Nelson, Christopher Henze, Eleanor Rieffel, Rupak Biswas and Salvatore Mandrà

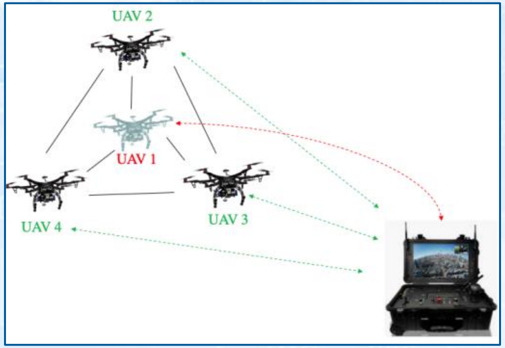
qFlex, HPC quantum circuit simulator open sourced Oct 2019
https://github.com/ngnrsaa/qflex

Robust Communication Network Design

Problem class: *Minimum Weighted Spanning Tree with degree constraints*

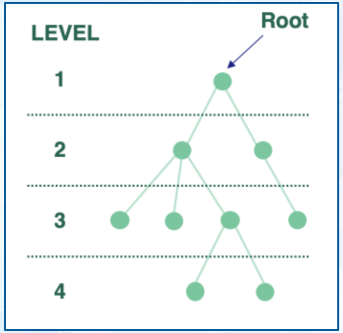
Cost function to minimize

$$C_{obj} = \sum_{p,v} w_{p,v} x_{p,v} \quad where \quad x_{p,v} = 1 \quad if\ p\ parent\ of\ v$$



Constraints ⟹ **Penalties**

- Every non-root node has one parent
- Every node exists at one level
- If p parent of v, p's level is one less than v's
- Maximum degree is Δ

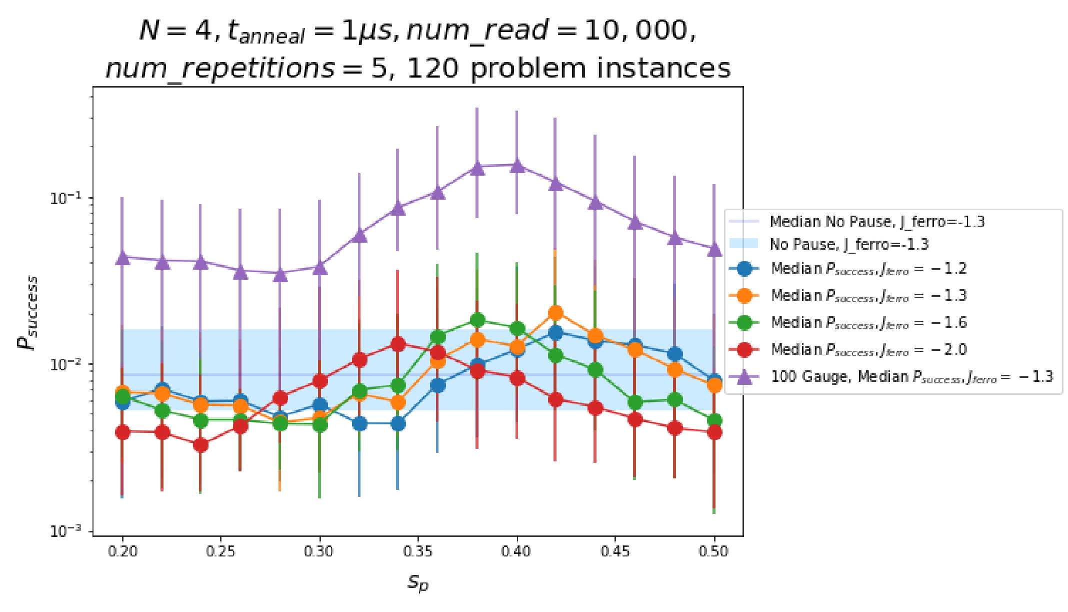


Preliminary results on effectiveness of pause on embedded problems

Successful solution of bounded degree spanning tree problems

Over baseline quantum annealing runs
- > 5x with well-chosen pause location
- Consistent pause location across instances
- ~10x improvement with partial gauges

Similar results for N=5 problems



Recent results of
Zoe Gonzalez, Shon Grabbe, Zhihui Wang, Jeff Marshall, Stuart Hadfield, Eleanor G. Rieffel,

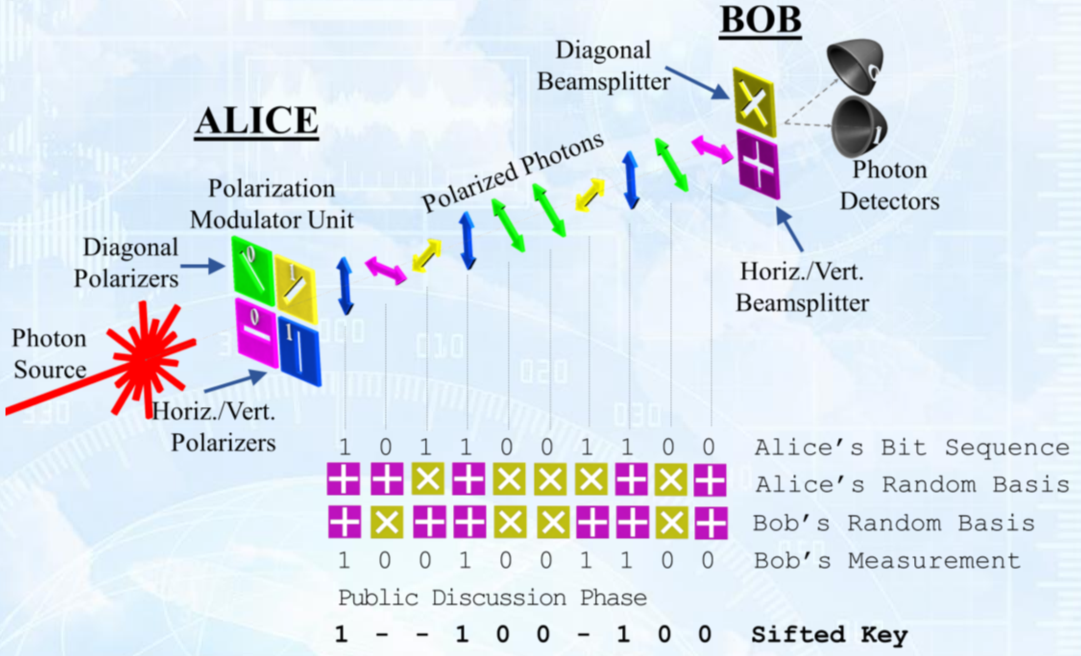
Requirements for Quantum Key Distribution (QKD)?

Why? QKD is used for <u>secure exchange of encryption keys,</u> for applications in <u>symmetric cryptography</u>

What? QKD is based on the transfer of polarization-modulated photons

We need:

- Quantum transmission
- Timing & Synchronization
- Bi-Dir Data Exchange



Bits are encoded with photon polarization states and are referred to as quantum bits

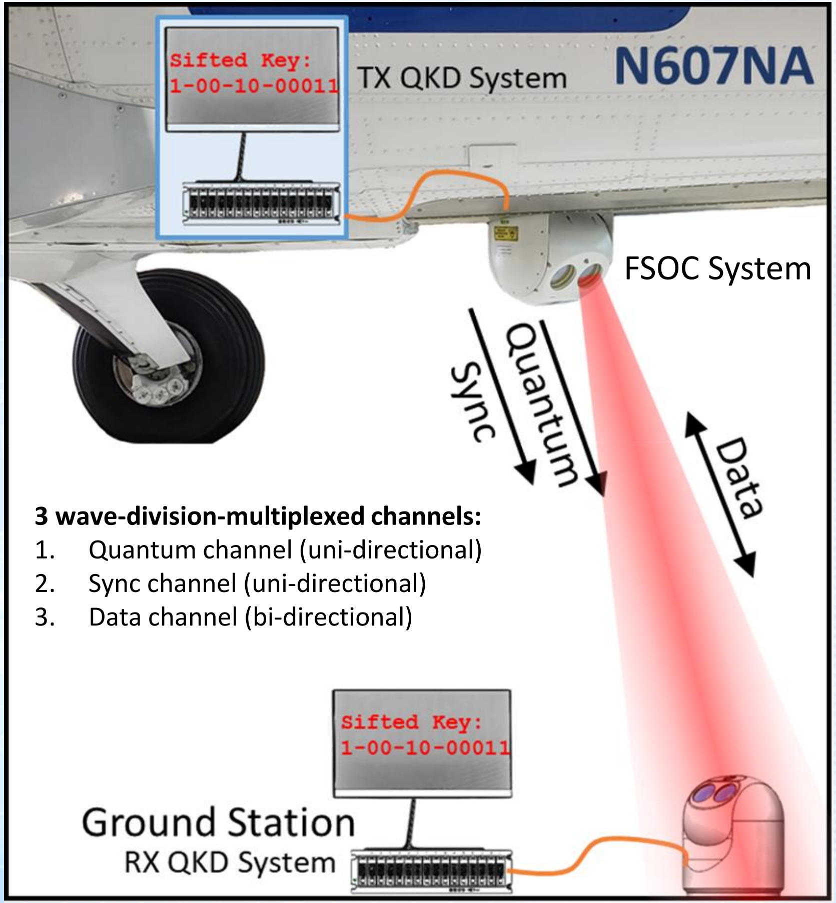
Quantum Key Distribution (QKD) effort

The QKD system is designed to be multiplexed within a classical free-space optical communication (FSOC) system, in order to achieve robust photon delivery and maintain data channel availability.

Key development paths are:

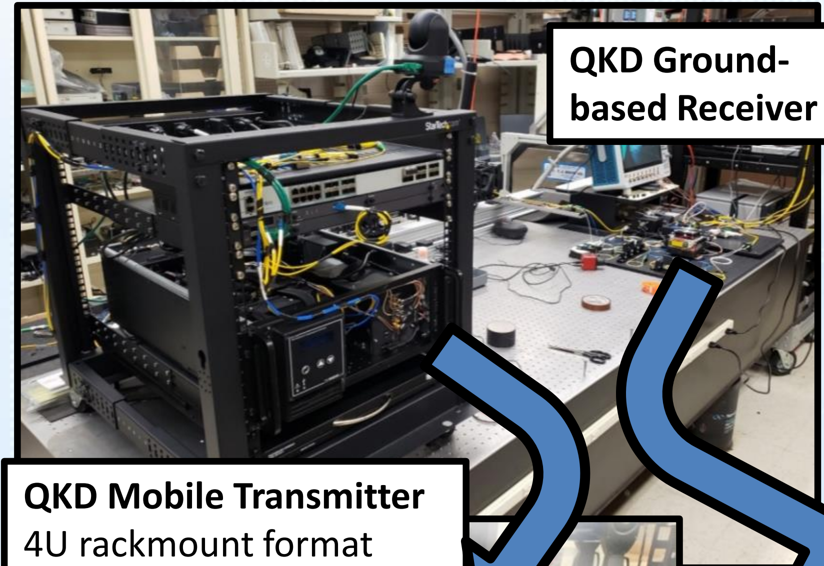
Thrust 1) **QKD:** Development of a practical and deployable QKD system, capable of FSOC system integration.

Thrust 2) **FSOC:** Continued development of FSOC terminals with robust pointing, acquisition, tracking (PAT) capability



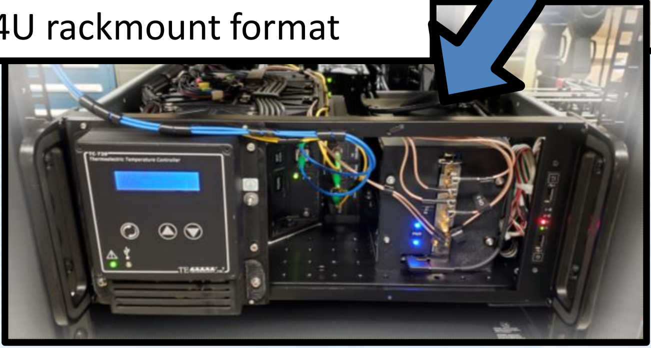
Thrust 1: QKD Prototype: Algorithm development in progress

- ✓ Fiber-optic-based QKD system **successfully transmits quantum bits at rates >100MHz**
- ✓ **Miniaturized, capable of independent operation**, free from lab equipment
- ✓ Designed to be **integrate-able within aero-style FSOC gimbals**

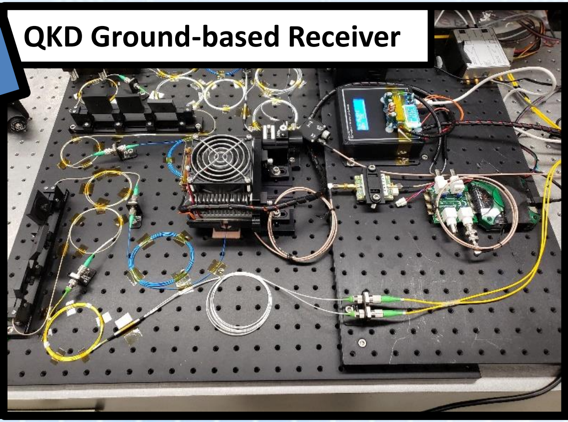


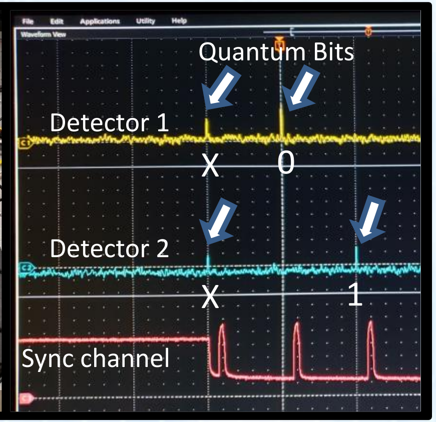
QKD Ground-based Receiver

QKD Mobile Transmitter
4U rackmount format

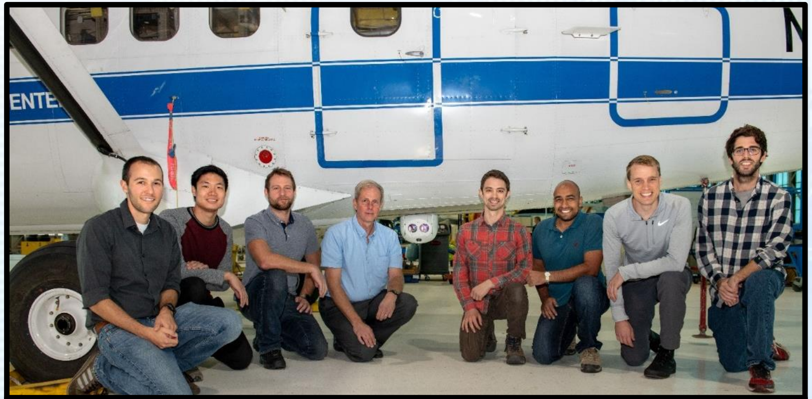


QKD Ground-based Receiver





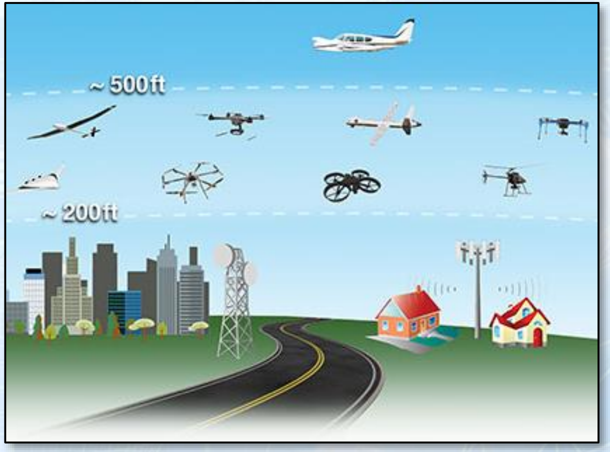
Thrust 2: QKD FSOC System, successful airborne FSOC test



- ✓ Evaluated pointing, acquisition, and tracking (PAT) capability **in real airborne conditions**, for use in QKD applications.
- ✓ The PAT performance showed that this tracking hardware/strategy is a **strong candidate for QKD photon transfer**
- ✓ ***Bonus:*** Maintained optical links at slant path ranges **2x greater than expected!**
- ✓ ***Bonus:*** Optical modems were operated at **maximum data rates** for distances **1.6x greater than expected**

Summary and Impact

Feasibility of a revolutionary approach to the 'Availability' challenge for UAS operations:
Harnessing the power of quantum computing and communication to address the cybersecurity challenge of availability



Assure the **availability** of the UAS Traffic Management (UTM) network against communication disruptions

Enable a safe and secure future for emerging operations, flexible services, and new users and missions

Ensure a scalable solution for securing networks in high density, heterogeneous air traffic management operations

A Historical Perspective

NASA Ames director Hans Mark brought Illiac IV to NASA Ames in 1972

Illiac IV - first massively parallel computer

- 64 64-bit FPUs and a single CPU

- 50 MFLOP peak, fastest computer at the time

Finding good problems and algorithms was challenging

Questions at the time:

- How broad will the applications be of massively parallel computing?

- Will computers ever be able to compete with wind tunnels?

Thank you for your attention.

Many thanks to our team members.

And to CAS for funding our work.