

ARMD Transformative Aeronautics Concepts Program

CONVERGENT AERONAUTICS SOLUTIONS PROJECT

QTech

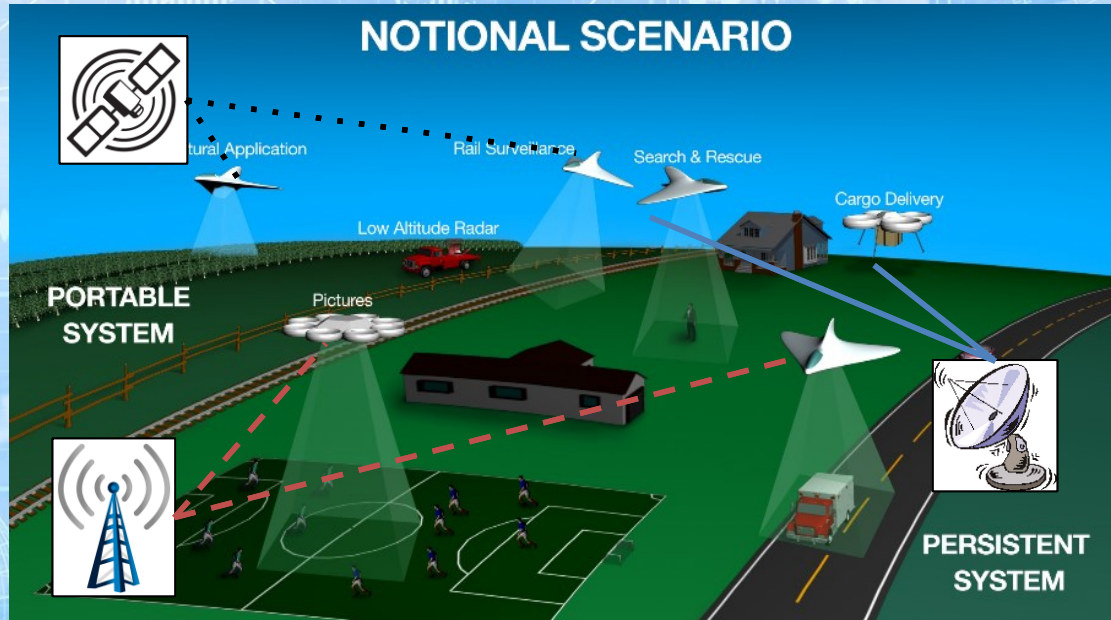
Eleanor Rieffel
ARC – Quantum Computing

Adam Wroblewski
GRC – Quantum Communications



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

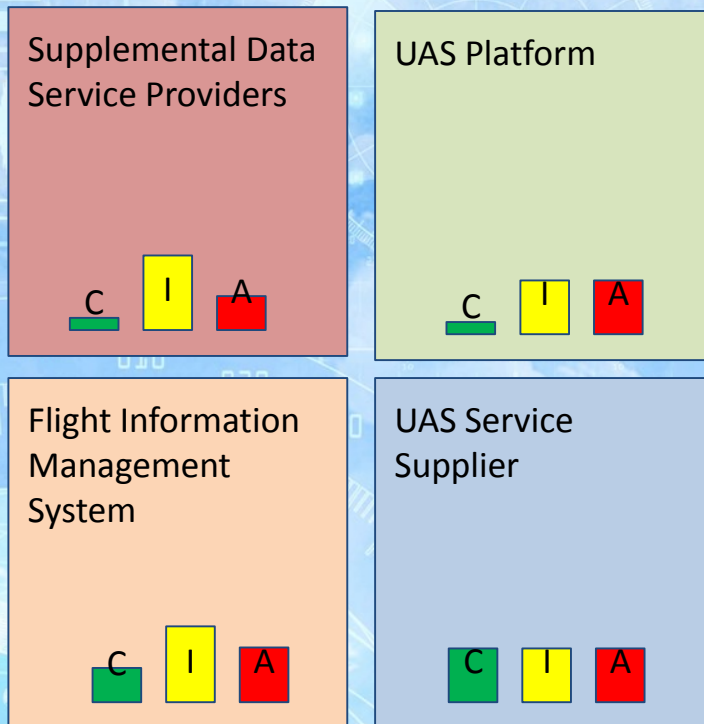
- Less of a concern

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

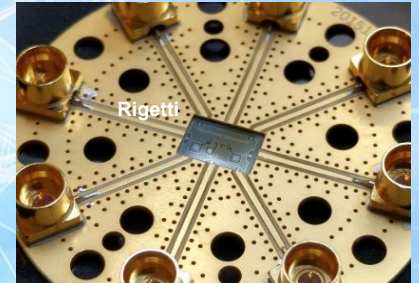
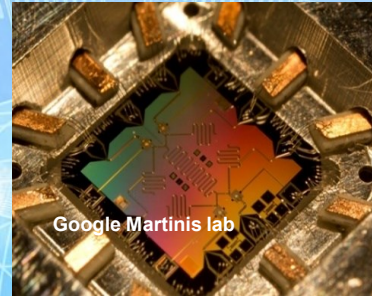
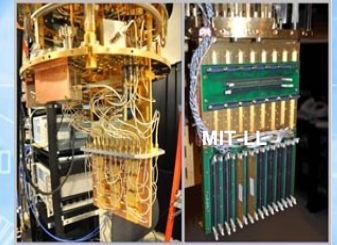
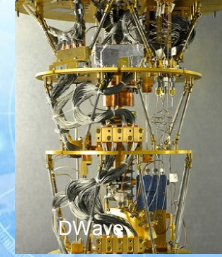


*From J. Rios (NASA ARC, Chief engineer for UTM):
Relative Importance of Confidentiality, Integrity,
and Availability for UTM*

Idea/Concept

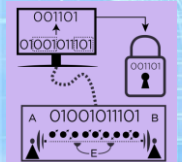
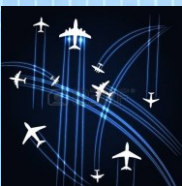
We propose a revolutionary approach to the 'Availability' challenge for UAS operations:

Harness the power of quantum computing and communication to address the cybersecurity challenge of availability



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

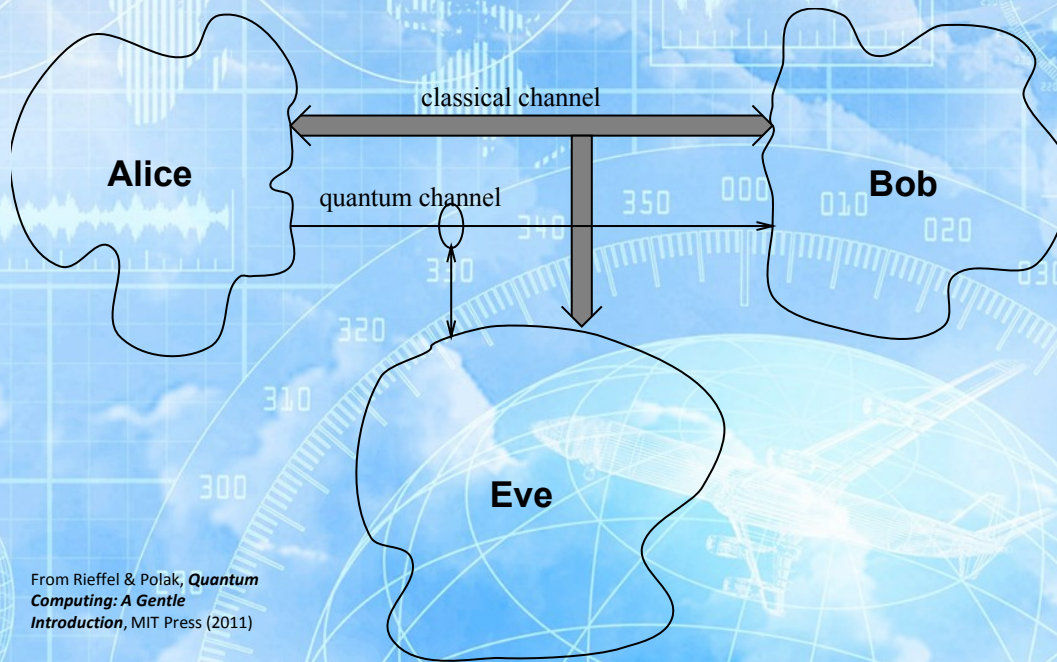
- What Shor's factoring algorithm can compute in days, would take a supercomputer longer than the age of the universe

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)



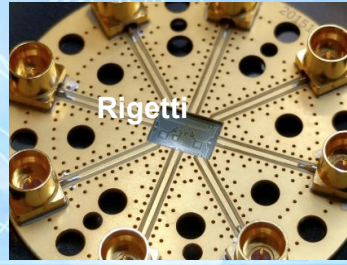
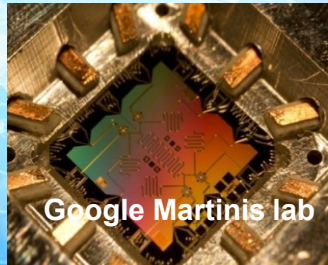
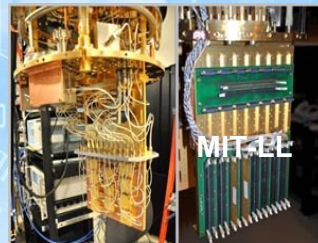
Two types of quantum computing devices

Quantum Annealers: *special-purpose* quantum optimization hardware



General-purpose gate-model quantum processors

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





HPC simulation of quantum circuits

Advanced the state-of-the-art

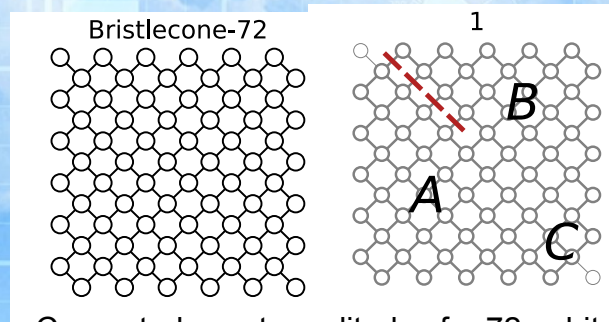
- can simulate **larger quantum circuits** than any previous approach
- **judicious use of cuts** within a tensor network
- **HPC memory tricks** and trade-offs
- can flexibly **incorporate fidelity** goal

Largest computation run on NASA HPC clusters

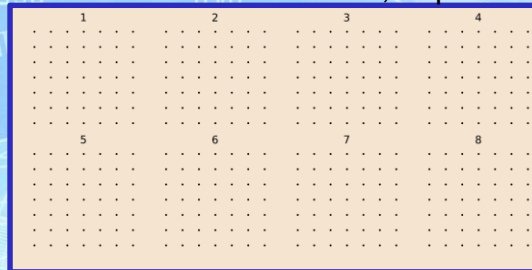
- 60-qubit subgraph, depth 1+32+1
- 116,611 processes on 13,059 nodes, peak of 20 PFLOPS, 64% of max
- across Pleiades, Electra, Hyperwall

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!

... but not useful quantum supremacy.

- Perform computations not possible on even the largest supercomputers

- Currently too small to be useful for solving practical problems

Unprecedented opportunity to explore and evaluate quantum algorithms empirically



Article Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Blaise Berr, John Booth, Joseph Bruch, Andrew Cleland, Daniel Collins, Brian Cooney, Brian Fowler, Matthew Fuhrer, Jesse Greco, Austin G. Green, Kristan Hamilton, Daniel Harlow, John Hartono, Alan Ho, Markus Hoffmann, Yun-Hong Hwang, Thomas Huang, Sergey V. Isakov, Evan Jeffrey, Dong Liang, Tommaso Albino, Michael J. Heuley, John J. Hofer, Joseph Johnson, Alexander Korbacz, Peter Kourtellis, David Landahl, Mike McEwen, Erik Lucero, Dongyuan Ma, Adam Megrant, Anand Melnick, Matthew McEwen, Andrew Megrant, Brian P. O'Neil, Daniel Orlovsky, Ryan O'Shea, Jeffrey P. O'Brien, Okechukwu Olayinka, Andrew P. O'Connell, Charles Quigg, Hsin-Yuan Ku, Scott J. Shott, Stephen Slichter, John Smolin, David S. Steiger, Brian T. H. Varcoe, Stephen V. Wehner, Michael C. Rubin, David Laro, Kiana S. M. Taniguchi, Vadim V. Shvachkin, Yuxuan Song, Matthew S. Swilling, Paul Vercouterre, Benjamin Vukobratovic, Thomas White, Zhen Yao, Peng Yin, Adam Zimmerman, Hartmut Neven and John M. Martinis*

The premier of quantum computers that can outperform classical computers in a task that is exponentially hard for a classical computer. A fundamental challenge in building a programmable processor capable of performing quantum algorithms is that the required range of operations is exponentially large. Here we report the use of a processor with programmable superconducting qubits¹ to create quantum circuits with a depth, corresponding to a computational complexity of O(2.8ⁿ), that is beyond the reach of any classical computer. Measurements from repeated experiments sample the resulting probability distribution, which we verify using statistical methods. Our 53-qubit processor takes about 200 seconds to sample one instance of a quantum circuit and the classical computer benchmark currently takes about 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy² for the specific computational task, heralding a new era of quantum computing.

Abstract The premier of quantum computers that can outperform classical computers in a task that is exponentially hard for a classical computer. A fundamental challenge in building a programmable processor capable of performing quantum algorithms is that the required range of operations is exponentially large. Here we report the use of a processor with programmable superconducting qubits¹ to create quantum circuits with a depth, corresponding to a computational complexity of O(2.8ⁿ), that is beyond the reach of any classical computer. Measurements from repeated experiments sample the resulting probability distribution, which we verify using statistical methods. Our 53-qubit processor takes about 200 seconds to sample one instance of a quantum circuit and the classical computer benchmark currently takes about 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy² for the specific computational task, heralding a new era of quantum computing.

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

Benjamin Villalonga^{1,2,3}, Dmitry Lyakh^{4,5}, Sergio Boixo^{4,5}, Hartmut Neven^{4,5}, Travis S. Humble^{4,5}, Rupak Biswas⁶, Eleanor G. Rieffel^{1,4}, Alan Ho⁶, and Salvatore Morandì^{1,7*}

¹Quantum Artificial Intelligence Lab (QAIL), NASA Ames Research Center, Moffett Field, CA 94035, USA
²USRA Research Institute for Advanced Computer Science (RIACS), 615 National, Mountain View, California 94043, USA
³Institute for Condensed Matter Theory and Department of Physics, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA
⁴Quantum Computing Institute, Oak Ridge National Laboratory, Oak Ridge, TN, USA
⁵Scientific Computing, Oak Ridge Leadership Computing, Oak Ridge National Laboratory, Oak Ridge, TN, USA
⁶Google Inc., Venice, CA 90291, USA
⁷Singer Cluettum Technologies Inc., 7701 Greenbelt Rd., Suite 400, Greenbelt, MD 20770

Abstract—Nobly Intermediate-Scale Qubits aim to perform computational tasks that are the most powerful classical computers, it is a major milestone. NISQ Supremacy requires comparison classical simulation. We report HPC sim quantum circuits (RQC), simulating an 281 Pflop/s (true single precision) on fastest supercomputer in the world. It a standard benchmark for NISQ using a tensor-network-based classical logic RQC, which are considered the leading Supremacy.

1. INTRODUCTION AND MOTIVATION
 As we approach the end of Moore's Law, the industry to develop alternative computational models. Examples of these models are quantum computing, quantum computers, namely they perform a universal set of discrete operations (P=NP) on a finite Quantum algorithm.

Joint work with Google establishing the quantum supremacy frontier

npi | Quantum Information www.nature.com/npiqi

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

Benjamin Villalonga^{1,2,3}, Sergio Boixo⁴, Bron Nepton⁵, Christopher Henzler⁶, Eleanor Rieffel⁷, Rupak Biswas⁸ and Salvatore Morandì^{9*}

Here we present qFlex, a flexible tensor network-based quantum circuit simulator. qFlex can compute both the exact amplitudes, essential for the verification of the quantum hardware, as well as low-fidelity amplitudes, to mimic sampling from Noisy Intermediate-Scale Quantum (NISQ) devices. In this work, we focus on random quantum circuits (RQC) in the range of sizes expected to also present benchmark NASA HPC peak of 20 performance over run or general app npi Quantum

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

Google, NASA, ORNL collaboration

Robust Communication Network Design

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

Cost function to minimize

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

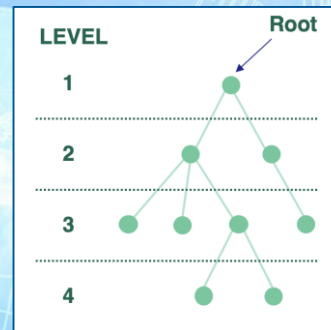
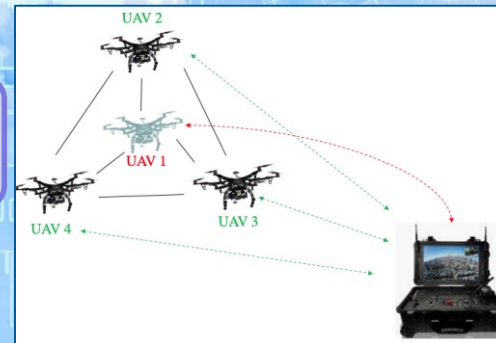
Constraints \longrightarrow Penalties

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

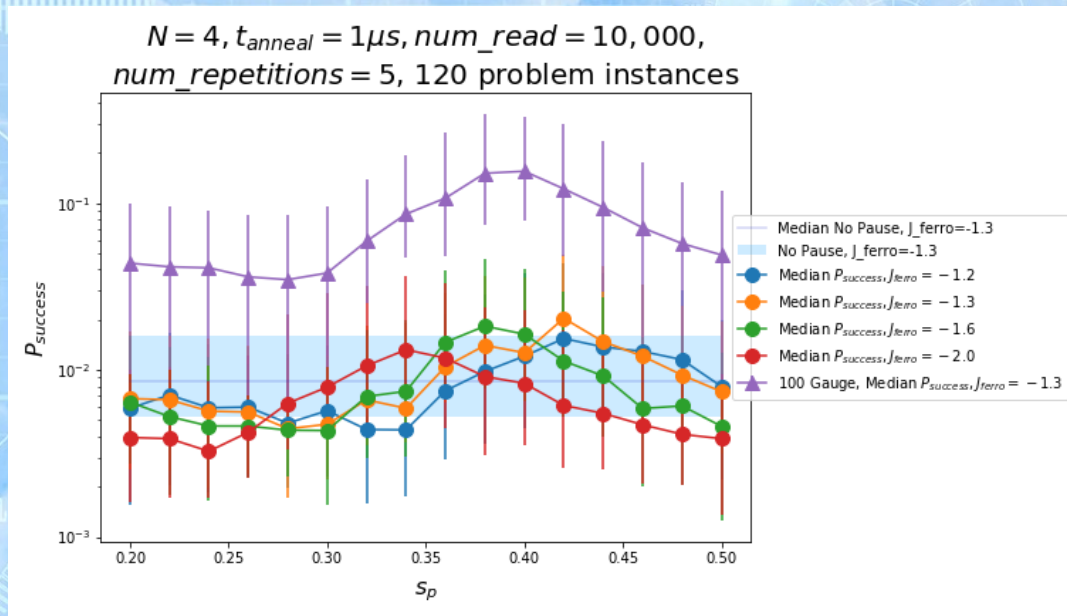
Over baseline quantum annealing runs

- > 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, Zihui Wang, Jeff Marshall, Stuart Hadfield, Eleanor G. Rieffel,



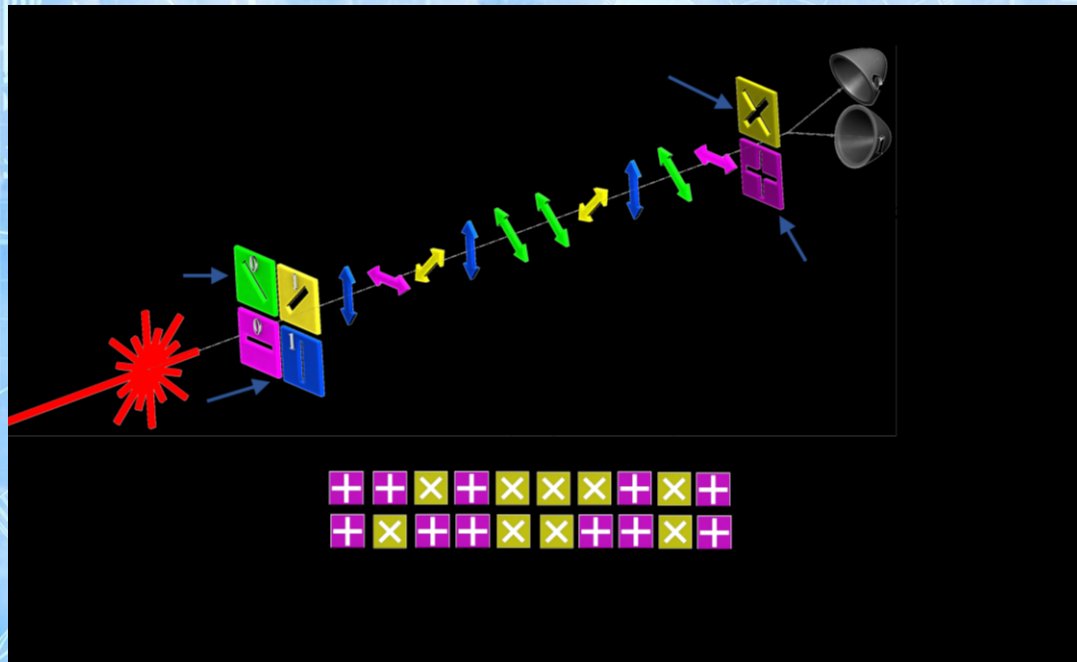
Requirements for Quantum Key Distribution (QKD)?

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

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

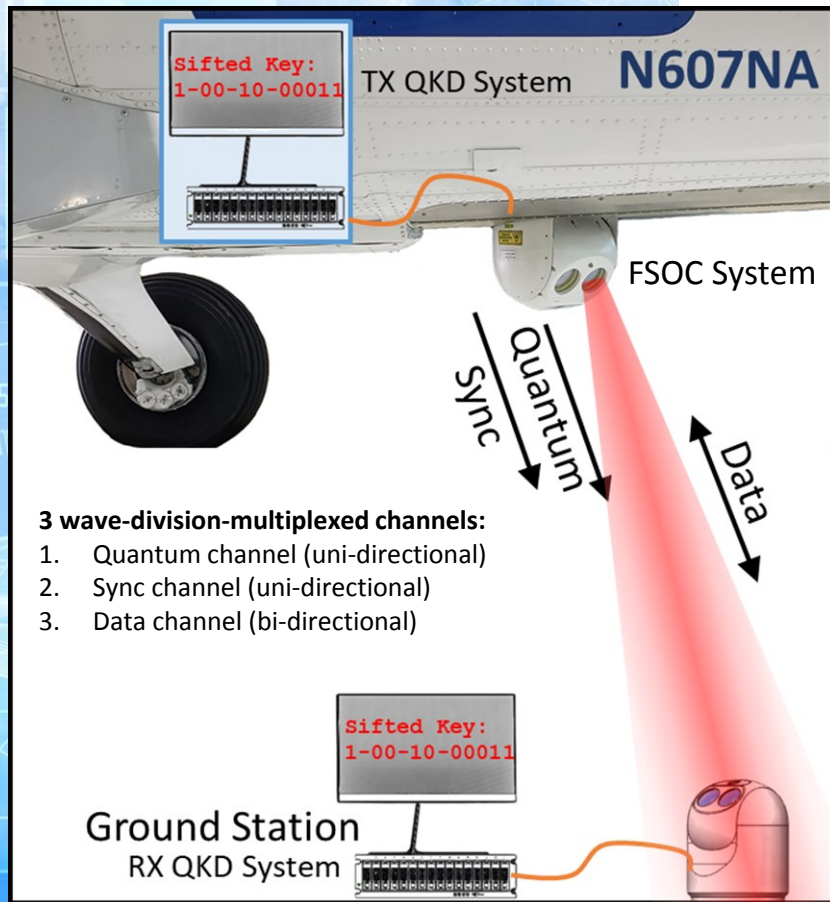


The QKD system is designed to be multiplexed within a classical free-space optical communication (FSOC) system, in order to achieve robust photon delivery and maintain data channel availability.

Key development paths are:

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

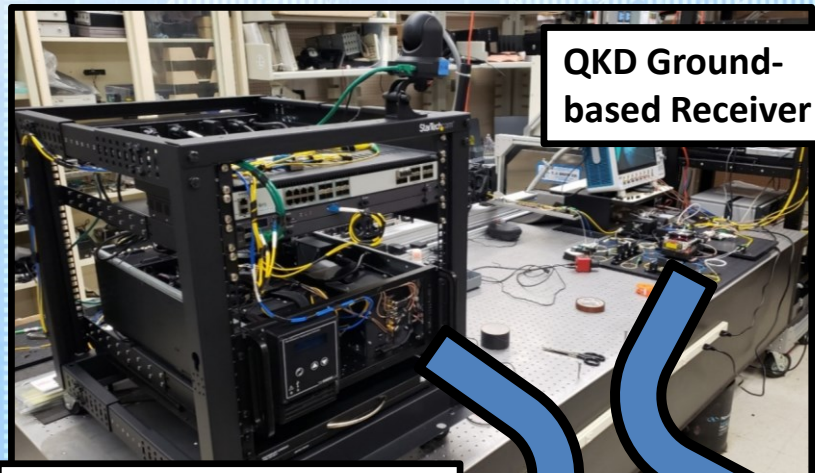
Thrust 2) FSOC: Continued development of FSOC terminals with robust pointing, acquisition, tracking (PAT) capability



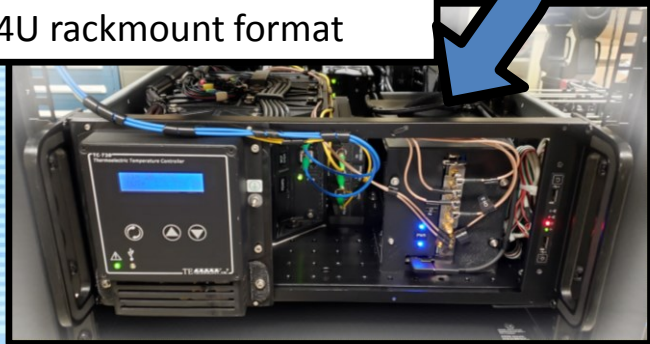
Thrust 1: QKD Prototype: Algorithm development in progress

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

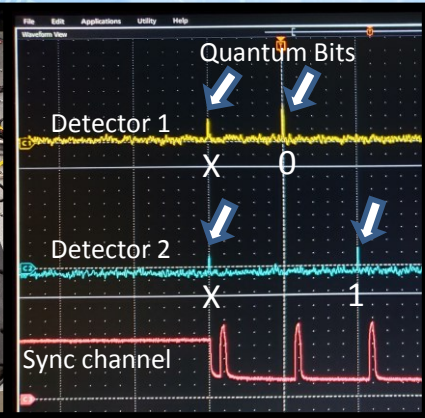
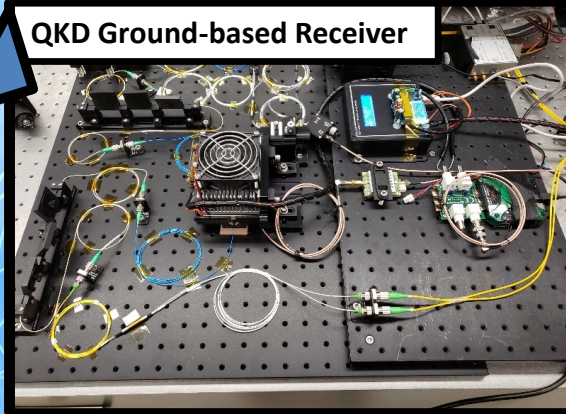
QKD Ground-based Receiver



QKD Mobile Transmitter
4U rackmount format

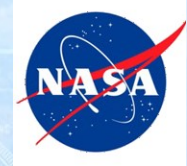


QKD Ground-based Receiver

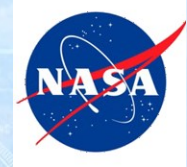




Thrust 2: QKD FSOC System, successful airborne FSOC test



- ✓ 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

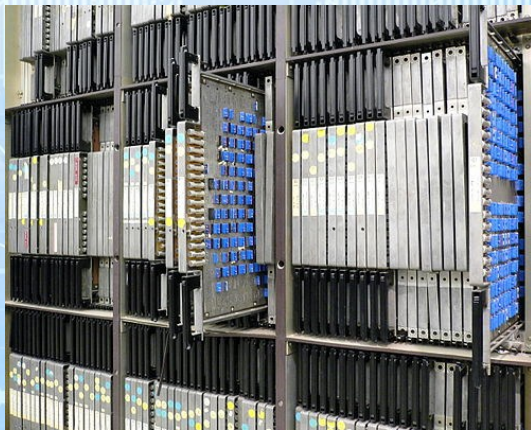


Assure the **availability** of the UAS Traffic Management (UTM) network against communication disruptions

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



Illiac IV - first massively parallel computer

- 64 64-bit FPUs and a single CPU
- 50 MFLOP peak, fastest computer at the time

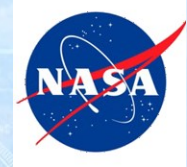
Finding good problems and algorithms was challenging

Questions at the time:

- How broad will the applications be of massively parallel computing?
- Will computers ever be able to compete with wind tunnels?



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



Thank you for your attention.

Many thanks to our team members.
And to CAS for funding our work.