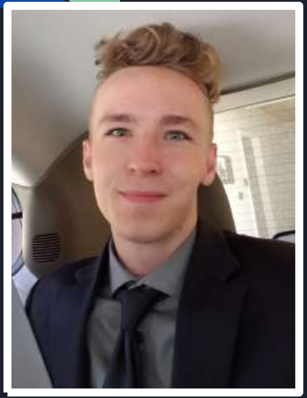
Post-Quantum Cryptography

for Modern Defense Security

Team Members



Erik Failing
Computer Science (Senior)
- Team Lead
- Cybersecurity SME
- Developer
- Researcher
- Interviewer

Cory Haralson
Computer Science (Senior)
- Quantum SME
- Writer
- Interviewer

Matthew Daigle
Computer Science & Mathematics (Senior)
- Researcher
- Interviewer
- Writer
- Algorithm Testing

Angela Allison
Computer Science (Senior)
- Literature Review
- Researcher
- Interviewer
- Writer

Sean Pagani
Computer Science (Senior)
- Literature Review
- Researcher
- Interviewer
- Benchmarks

Mentors and Affiliations

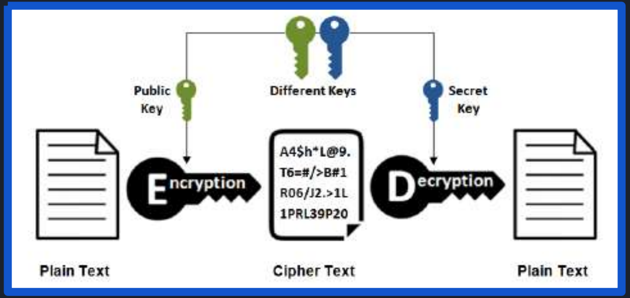
- [redacted] - Project Sponsor
- [redacted] - Professor

Quantum Computing

- Uses quantum mechanics to operate
  - Can be exponentially faster than classic computers
  - Use Qubits instead of bits
- Operation compared to classical computers
  - Classical computers use bits
  - Bits show information in 1’s and 0’s
    - 2 bit machine has 4 states
      - 00
      - 01
      - 10
      - 11
  - 2 qubit machine can be in all 4 states at once

Cryptography

- Cryptography is the practice of securing communications
  - It enables confidentiality, integrity, non-repudiation, and authentication
  - Ciphers are used to encrypt/decrypt messages
- Two Types:
  - Single/Symmetric key encryption
  - Public/Asymmetric key encryption (eg. RSA)
- Certain Asymmetric Cryptographic standards can broken by Quantum Computers
  - Can solve some hard problems exponentially faster than classical computers



The Need for Post Quantum Encryption

Post-Quantum Attacks are around 20 - 30 years away.

however...

Changes to standards take a long time.

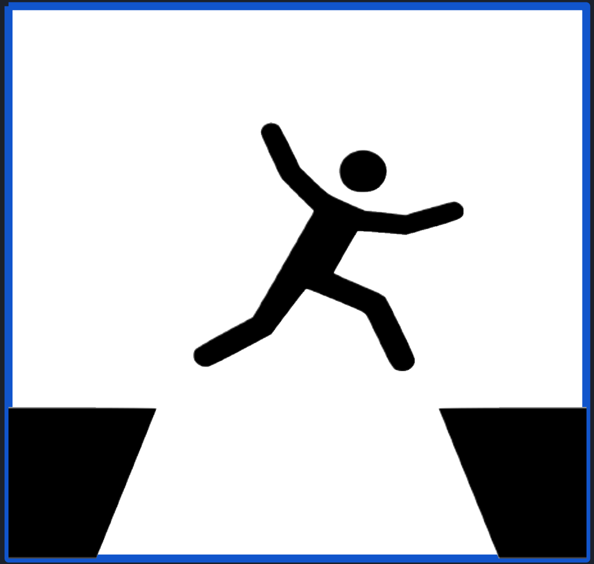
Attackers can start storing information now, for later.

Confidential Information has a long shelf life (20+ Years).

Our Challenge

Formal Problem Statement:

"Engineers within the Advanced Technology Program Executive Office require the ability to assess post-quantum cryptography algorithms in order to determine which could be employed to ensure data security for ballistic missile defense systems."



Original Hypotheses

- **Initial Thought:** A white paper analyzing quantum-safe encryption algorithms.
- Narrowing down algorithms to recommend the best Algorithm for Quantum Safe Encryption.
- Applicable to any organization with sensitive or classified information.

DEPLOYMENT

-A peer reviewed white paper analyzing promising PQC encryption algorithms.

BENEFICIARIES

- Cryptographers
- Cyber security analysts
- Network Specialists
- Cryptanalysts

MMC Version 1

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITIONS	BUY-IN & SUPPORT	BENEFICIARIES
[redacted] [redacted] [redacted]	-Research -Interview -Testing - Theoretical modeling in low performance and limited environments	**-Our analysis will provide increased understanding of PQC algorithms and enable the efficient hardening of systems against near future quantum computers**	[redacted]	- Cryptographers - Cyber security analysts - Network Specialists - Cryptanalysts
	KEY RESOURCES		**DEPLOYMENT**	
	-Access to cutting edge PQC encryption algorithms -A subject matter expert in quantum computing		-A peer reviewed white paper analyzing promising PQC encryption algorithms.	

MISSION BUDGET/COST	MISSION ACHIEVEMENT/IMPACT FACTORS
-Algorithms need to be able to run in low size, weight, power, and limited bandwidth environments (e.g., a raspberry pi with a 500 Mbps connection)	**-Succinct analysis of a multitude of PQC encryption algorithms** **-Identification of which promising PQC encryption algorithms should be used in a given environment (ex: low resource vs. high resource)**

Where did we start?

- We decided to do a white paper and followed through
  - We wanted to recommend the most secure algorithm
- Initial Idea: Layer two encryptions
  - Since NIST competition won't finish until 2023/2024
- Information gathering
  - What testing environments to use?
  - Who should we interview to learn more?
  - What resources are available to us?
  - How do we choose a "best" algorithm to recommend?
  - Is our initial idea on the right track?

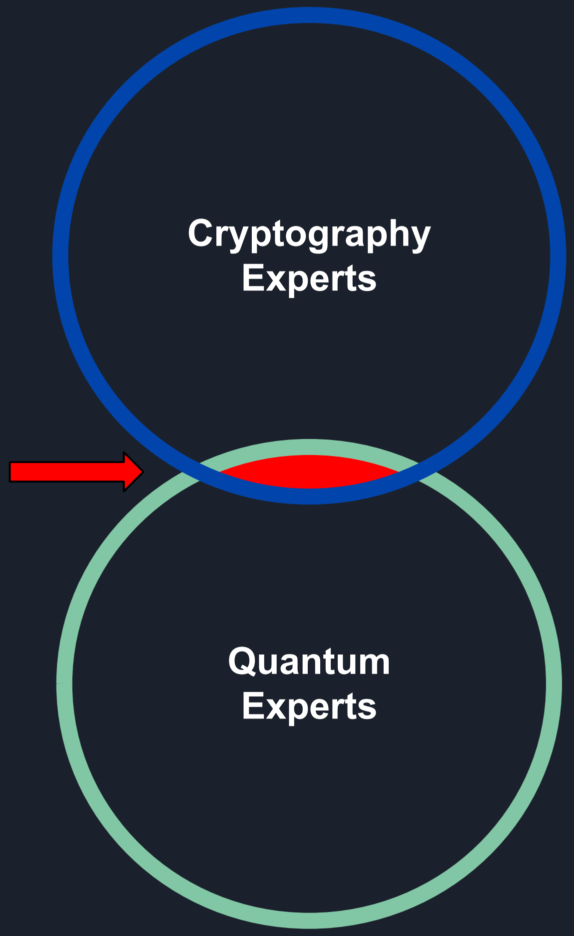
KEY ACTIVITIES

-Research
-Interview
-Testing
- Theoretical modeling in low performance and limited environments

The Interview Process

- 15 Interviews
  - 30 minutes to 3 hours in length
- Extended correspondence w/ an additional 8 experts over email
- Professionals in Cryptography and Quantum
  - Targeted people who knew both
  - Few are SMEs of both

Our need

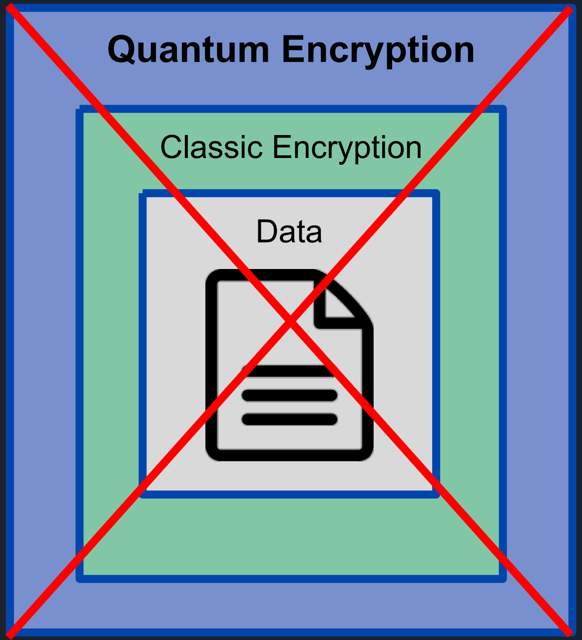


First Pivot: No Encryption Layering

Cryptography experts refuted layering two encryptions

- Waste of resources
- Opens more vulnerabilities; side channel attacks
- Poor time efficiency
- NIST standards are very reliable, why layer?

New Focus: Recommend a promising encryption algorithm for each of a variety of environments



Second Pivot: Re-Evaluate Success

Shifted Focus to:

- Raising awareness about the reality of quantum attacks
- Providing analysis of known Quantum Safe encryption algorithms
- Showing that the new quantum-safe algorithms could match up to our current standards

MISSION ACHIEVEMENT/IMPACT FACTORS

-Succinct analysis of a multitude of PQC encryption algorithms

-Identification of which promising PQC encryption algorithms should be used in a given environment (ex: low resource vs. high resource)

Before

MISSION ACHIEVEMENT/IMPACT FACTORS

- Reasonable timelining of quantum computing advancement
- Analysis of specific quantum-safe PKE algorithms based on operating environment conditions, established via theoretical analysis and concrete tests
- Provide awareness to the MDA about implementable quantum-safe solutions without the use of quantum computers

After

Third Pivot: Reducing Scope

Two Types

Key Generation & Key Establishment (17 Algorithms)

Digital Signatures (9 Algorithms)

Six Categories

One-Way McEliece (2)

Learning With Errors (7)

Quasi-Cyclic Parity Checking (2)

Lattices (2)

Syndrome Decoding (3)

Our 6 Choices

Classic McEliece

NewHope

BIKE

NTRU Prime

HQC

SIKE

Further Reduction

6 Choices → 3 Choices	
X Classic McEliece	Missing a header file which could not be sourced
✓ NewHope	
X BIKE	Used inline assembly, not compatible with ARM architecture
✓ NTRU Prime	
X HQC	AVX2 Instructions: cannot run on ARM processors
✓ SIKE	

MMC Version 10

KEY PARTNERS

- Strategic Alliances: [redacted]

- Co-opetition: [redacted]

- Joint-Ventures: [redacted]

- Suppliers: [redacted]

KEY ACTIVITIES

-Researching & Interviewing
-Testing PKE algorithms in various environments
- Analyzing PKE algorithms
- Time-lining quantum computing advancement
- Analyzing impact of a quantum attack on MDA's Secure Systems

KEY RESOURCES

-PKE C code implementations of Classic McEliece, NTRU Prime, SIKE, NewHope, BIKE & HQC
-Testing Environments: Raspberry Pi 3 (Cortex-A53 Processor), Cortex M4 on STM discovery board, Computer with Haswell Processor, FPGA, RTOS
- Interviews with Professionals in cryptography, quantum computing, and those in the MDA

VALUE PROPOSITIONS

- Provide increased understanding of quantum-safe PKE algorithms to allow the DoD to make a well-informed implementation decisions.

- Assist in deployment of quantum-safe PKE algorithms in appropriate environments to prevent performance impacts.

- Enable hardening of systems through quantum resistant algorithms to preserve classified information from quantum computing attacks.

BUY-IN & SUPPORT

- Wait for MDA to release a version of our paper suitable for the public before we post it anywhere.
- Post whitepaper to arxiv.org
- Present/Deliver paper to the MDA and the Advanced Technology Program Executive Office

DEPLOYMENT

-A white paper containing the following: Executive Summary, Introduction, Literature Review, Research Methodology, Findings, Analysis & Discussion, Recommendations and References

BENEFICIARIES

-Cyber Security Analysts
-Cryptanalysts
-Information Systems Security Managers
-Information Security Officers
-Security Architects
-Telemetry Engineers
- Crypto Researchers

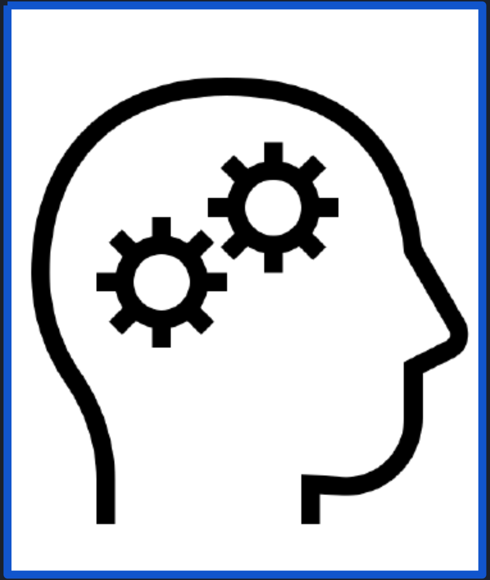
MISSION BUDGET/COST

- Algorithms need to be able to run in low size, weight, power, and limited bandwidth environments
- Raspberry Pi (3B+/4)
- Mission must be accomplished by April 30, 2020

MISSION ACHIEVEMENT/IMPACT FACTORS

- Reasonable timelining of quantum computing advancement
- Analysis of specific quantum-safe PKE algorithms based on operating environment conditions, established via theoretical analysis and concrete tests
- Provide awareness to the MDA about implementable quantum-safe solutions without the use of quantum computers

Lessons Learned



- Quantum computing is not a matter of IF but a matter of WHEN; we must be prepared for their potential
- Since attackers can save encrypted data, quantum-safe encryption is needed right now
- It's important to be aware of growing technologies even if they’re decades away

Our Next Steps

- Continue tests on the 23 other Round 2 NIST candidates
- Obtain and test on a larger variety of platforms
- Conduct further research into figuring out ways to improve the algorithms
- Continue meeting with professionals to gain a better understanding of the subject
- Continue expanding upon current white paper

Where the team is headed

Matthew Daigle - Graduating and continuing to a Master's in Computer Science. Willing to pursue this analysis further.

Erik Failing - Open to pursuing H4D project further - Cybersecurity Engineer - B.S CS late 2020 - A.S CISSP early 2021 - OSCP mid 2021 - M.S Cybersecurity 2023.

Cory Haralson - Posed to graduate with a Bachelors in Computer Science and start work. Will pursue more degrees in CS and Physics. Will not be continuing work on H4D.

Angela Allison - Graduating Senior with a B.S. in Computer Science and will be working as a Software Developer. Will not continue working on H4D project.

Sean Pagani- Senior Computer Science Student and will work in a related field. Will not continue working on H4D project.