Post-Quantum Cryptography for Space Communication

Securing Artemis Missions from Quantum Attacks

Dhanush Karthikeyan, Choi Tim Antony Yung, Shadrach W. Viste, Ruben Torres Romero
Faculty Advisor: Dr. Mohamed El-Hadedy Aly
Kepler-452b, California Polytechnic University - Pomona

Background

Certain commonly used conventional cryptography is proven to be vulnerable to attacks using a sufficiently powerful quantum computer. With its crucial importance in space exploration, the Artemis mission cannot fail, meaning it is necessary to ensure adversaries such as nation-state actors with sufficient resources cannot compromise the communications necessary to the mission's success.

Problem Statement

- A quantum resistant layer needs to be incorporated into space communications between field operations and mission control.
- Command and data transmission are vulnerable to the onset of quantum attacks and forgeries.

Objective

The project aims to incorporate Leighton-Micali Signature (LMS) stateful hash-based signature scheme to vulnerable data exchange channels. Scenarios can include data transmissions between mission control, satellite stations, and autonomous rovers. LMS signature, linked to the data and the sender, can be generated, sent over vulnerable channel, and verified by the receiver to prevent resend attacks and forgeries while avoid adding significant hindrance to the communication.

Engineering Design Process

Different versions of both the software and hardware were designed and improved. A set of requirements is referenced to design for and test against. Physical measurements and software debug information were obtained to aid improvements and optimizations. As a result, three major revisions of UGV were designed with various smaller changes made in between.

Fig 1. Iterations of Rover in Design Process

Prototype

To conduct this experiment, custom unmanned ground vehicles (UGV) were fabricated with scalability in mind. Every aspect of the UGV – mechanical assembly, hardware, and software – was informed with the potential to scale. Thus, we have modeled, fabricated, and deployed fully autonomous UGV's.

Fig 2. 3D Rendered Rover

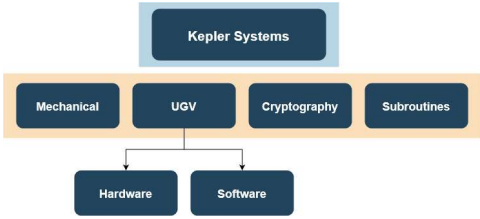
Fig 3. Fabricated and Rendered Rover

Innovations

The rover is fully modular and can be scaled for any mission. It is also fully responsive to the LMS cryptographic framework, with the ability to execute complex tasks with minimal overhead from LMS. Polymorphism is incorporated to ensure flexible accommodation to wide variety of data transmitted over the quantum secure channel.

Key Components of Design

The UGV is subdivided into the following the systems based on functionality. They are connected by their corresponding software or hardware interfaces.



Trade Table

Trade study was conducted on the core computing hardware:

Computing Hardware	Turing Pi	Pynq Z2	Raspberry Pi	ESP32
Parallel Computing	Yes	Yes	No	No
Hardware Acceleration	No	Yes	No	No
Real-time Applications	Low	High	Medium	High
Cost	High (+CM)	High	Medium	Low
Availability	Low (CM)	Medium	Medium	High

Benchmark Data

A benchmark of 100 communications involving signature generation and verification was performed on a commercially available low computational power Raspberry Pi 4B+ used as the core computation device of the system, the communication involving both signature generation, data and signature transmission over local network, and signature verification consume around 8.6361 seconds on average with a slight dependency on file size.

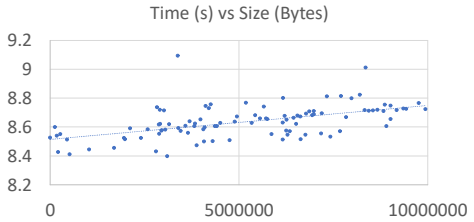


Fig 3. Illustration of Correlation of Information Size and Communication Time

Analysis

While the duration of the communication involving signature generation and verification is correlated to the size of the information, due to the context of the application, the commands will not likely be transferred in real time but in batches, the size of the information is unlikely to cause a significant increase of time and the delay caused by signing is trivial comparing to the transmission delay caused by the sheer distance the information need to travel. Therefore, it is considered that the signing and verification process is successfully executed without presenting a significant hinderance to the overall communications.