Anametric QPUF USSF TACFI program summary

Today, orbital platforms communications are under ever-increasing assault by both Nation State Adversaries as well as by criminal cyber attackers. This increasing level of attack is motivated by the swelling numbers of LEO platforms; originally intended for commercial purposes, but used more and more in areas of international conflict. Due to the opportunity for profit, the number of attackers are growing at a faster rate than the platforms themselves. At the same time, the attackers are rapidly gaining in sophistication, with advanced Machine-Learning based cyberattacks proliferating. The security of inter-satellite and ground-to-orbit communications are of paramount importance to the success of remote platforms such as satellites. Further, the ability of USSF operations to continue to operate successfully in such a contested environment is highly dependent on maintaining secure communications over long-term missions.

In order for these satellite-based platforms to communicate securely, a reliable means to confirm each system's identity is needed. Structures called Physical Unclonable Functions (PUFs) are used to form the root-of-trust of these secure IDs as well as to enable secure onboard storage of encryption keys and other security-related data. PUFs are unique; even two chips from the same wafer will have different PUF values. However, many PUFs are beginning to be threatened by advanced machine learning (ML) attacks. While these ML-based attacks have been known for over a decade, they are gaining in sophistication, due to recent advances in ML technology.

In the recently-completed Phase 2 effort, Anametric developed an alternative quantum photonic-based PUF –a "QPUF". The Anametric QPUF technology is not subject to electromagnetic interference. Anametric has built and tested two generations of QPUF chips and have demonstrated that the fabricated chips based on this patent-pending technology exhibit both a theoretical as well as a measurable advantage over current products to ML-based attacks. A second advantage of the patent-pending Anametric QPUF design is a unique feature that will allow them to be remotely "re- configured", effectively preventing the secured system from being affected by replay attacks.

The Anametric QPUF is very small, low-cost, lightweight, mechanically robust and very low power, making it ideal for use in the Pentagon's new Replicator initiative as well as for deployment in Satellite-based applications. In addition to the minimal CSWaP aspect, the Photonic IC fabrication technology used is inherently robust against Ionizing Radiation damage, making the QPUF highly suitable for high-altitude and in-orbit deployment. The mission impact of this project can be widespread. Anametric's goal is to provide a new strategic capability to enhance the security of our National Defense systems against both current and future threats, addressing a critical mission need.