Cryptographic Security for Satellite Rendezvous and Proximity Operations

Caroline M. Fedele, Christopher D. Petersen, and Kevin R. B. Butler
University of Florida, Gainesville, FL

Tyler M. Lovelly
Air Force Research Laboratory, Albuquerque, NM

Satellites in space are increasingly functioning and operating at close range to each other, making controlling them from the ground difficult or infeasible. Rendezvous and proximity operations (RPO) enable satellites to autonomously operate at close distances and perform processes such as docking, on-orbit servicing, refueling, and formation flying. Certain data must be shared in every RPO process to protect the physical integrity of all satellites involved. However, a security risk arising with RPO is satellite characterization, the ability for satellite stakeholders to make inferences of other satellites' capabilities based on shared data. We propose secure multi-party computation (SMC) as a means of preserving satellite privacy during RPO. Applied to several satellite-specific algorithms, we determined what minimum privatization is needed to both protect sensitive inputs and maintain efficiency. We test several common RPO algorithms on autonomous system hardware, both unsecured and secured with SMC, and benchmark the performance overhead, determining what input values should remain private and examining how SMC effects efficiency in RPO operations. We find that privacy-preserving operations move computation time from the order of microseconds to milliseconds but complete in significantly less than 1 second, well within the operational time constraints for RPO. We thus motivate integrating cybersecurity into space dynamics development and directly on board spacecraft. We also demonstrate SMC as a viable solution for securing autonomous operations for satellites and other resource-constrained systems.

I. Introduction

Satellites are necessary for many services we enjoy today, such as GPS, space-based internet, and global communications. They are a necessary component of civil, commercial, and national security, widely used in operations such as meteorology, Earth observance, surveillance, signal intelligence, and orbital traffic monitoring. With a significant rise in satellite development, particularly from the commercial sector, security will become an increasingly needed priority. Cybersecurity needs to be a top goal while space development is in its relatively early stages, and this needs to be addressed proactively. Waiting until a breach has occurred or vulnerabilities have been detected is a risky approach to take with computer systems in general, especially in the highly-contested space environment where mistakes are costly. Accurately anticipating security threats and predicting adversarial models are essential to ensuring the success of future development in space.

There are four main segments of space security technology: ground, link, user, and space. A comparison of the current state of these segments is depicted in Figure 1. Historically, space security approaches have mainly focused on the ground and link segments, with some efforts on the user segment [1]. The space segment has been largely assumed secure due to the inaccessibility of the spacecraft itself once launched. As the number of operators and stakeholders of space assets rises dramatically, the assumption that satellites in orbit are inaccessible can no longer hold and security measures directly on board space assets must be addressed [1]. Our research approaches security directly in the space segment as well as the user segment, where communication occurs directly between actors in space.

This research is particularly relevant as there is a growing need for operations where multiple satellites are in close range to each other [2]. **Rendezvous and proximity operations (RPO)** are what dictate tasks such as on-orbit servicing, refueling, inspection, docking, formation flying, and debris removal. Autonomous RPO is a growing area of interest, as it is becoming essential for the complexity and requirements of RPO that make ground control difficult or infeasible, motivating the need for strong in-space security. This also reduces the risk of human error. As RPO is critical in assuring physical safety in a variety of satellite operations, it is an area of growing necessity in the space research

Ground	Link
Strong security Well-understood threat model Easier to manage/update systems	Strong security Well-understood threat model Established comms security practice
User	**Space**
Strong ground security Weak space security Human control/interaction Need in-space cooperation	Weak security Outdated components and assumptions Growing number of actors/agencies Need security in autonomy

Fig. 1 Chart of four segments of space technology. The space segment has weak security protocols and outdated assumptions.

community. However, there are challenges in maintaining data security and privacy during RPO. There is also a lack of widely accepted standards for responsible performance of RPO, especially between satellites of different agencies, companies, or countries [3]. RPO maneuvers require that detailed information about a satellite's attitude, position, and trajectory be shared with others nearby, as well as the error margins on all of those values. As satellites are very expensive and difficult to launch into space, physical safety is a top concern. However, RPO maneuvers, which require location and trajectory data to be shared with other satellites, can expose potentially sensitive data. A privacy issue that arises with RPO is satellite characterization. When satellites are operating at close quarters, satellite stakeholders can make inferences about the capabilities or purposes of other satellites based on the shared data they receive. This is particularly concerning with defense satellites or mutually distrustful parties.

Satellite designers and operators must know the measure of trust they place in their sensors to make decisions based on their quantified accuracy, often determined by covariance matrices. Sharing accurate measurements, though, can allow other satellite stakeholders to infer their capabilities, purposes, or intents, such as what types of sensors are on board. This problem is known as **satellite characterization**, a privacy issue that has existed with satellites for decades but increased with RPO. Potentially sensitive values that satellites need to share in RPO include position, time to collision, sensor noise and accuracy, power and heat use, fuel levels, and other factors, which when shared can create a security risk for stakeholders and compromise proprietary satellite design. Figure 2 demonstrates a visual chart of this characterization process. One satellite operator can take observables from the hardware of another satellite or shared data in RPO, use filters to infer the properties of the system based on that data, and then use learning to infer the application, purpose, or owner of another vehicle. This is a particularly concerning capability for defense satellites or where mutually distrustful parties are involved. We propose a novel solution to protecting private data values in RPO calculations using **privacy-preserving computation**.

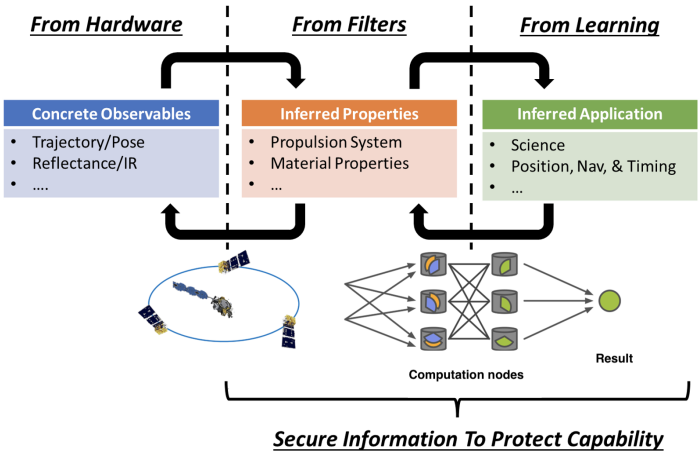


Fig. 2 Characterization Problem Flow

While there are several methods of implementing privacy-preserving computation (e.g., partially and fully homomorphic encryption), secure multi-party computation (SMC) is one of the most well-researched and application-

ready approaches according to existing literature [4]. We implement this in two different satellite algorithms to benchmark the overhead that SMC adds to the computations and ascertain the functionality of this approach for securing autonomous operations on satellites and other resource-constrained systems. The algorithms include a collision avoidance algorithm and a measurement optimization algorithm. Our goal with these algorithms is to demonstrate the application of SMC in relevant RPO scenarios and show the protection of satellite characteristics with privatized sensor error margins. This research provides the following contributions to the space security community:

- A domain-informed understanding of the intersection of security and space dynamics, specifically introducing RPO and associated security concerns.
- An implementation and evaluation of privacy-preserving computation in an RPO environment.

We bring the growing area of RPO into the scope of space security research and demonstrate the application of secure multi-party computation in a relevant RPO scenario.

II. Background

Space is a complicated environment to operate in due to the expensive and logistical difficulty of launching satellites into orbit. Hardware requirements pose a unique challenge since the components running on a satellite must have baseline operating abilities in a harsh, high-radiation environment. They typically undergo significant vibration and thermal testing and are a niche manufacturing market [5]. Most commercial electronic products cannot survive this environment, with the exception of a few products that have undergone extensive testing [6]. Historically, most radiation-hardened products designed for space are not state-of-the-art products with high computing performance. This trade-off is an increasingly relevant topic of research in the space computing community. Space is also challenging to operate in because the number of satellites in orbit has steadily increased in the past few decades. By 2030, the number could be over 30,000, according to some estimates [7]. This substantially increases the risk of satellite operation and makes positional awareness in space a vital capability [8]. With an increasing number of satellites in space, physical safety is a great concern for satellite operators and stakeholders. Private companies also have a vested interest in securing their on-orbit assets to maintain a competitive advantage and governments see this orbital data as a national security concern [9]. Operations where sensitive data must be shared to ensure satellites' physical safety, such as positional information in collision avoidance calculations, thus become a distinct challenge.

A. Rendezvous and Proximity Operations (RPO)

RPO has been a concept and practice since early space development, but it has only recently exploded as a research area with the rise in commercial satellite development and growing usefulness for on-orbit servicing and maneuvers. It is an expansive and growing area of work that encompasses other space-related specialties including sensors, orbital dynamics, contact and hardware docking, and data processing and sharing techniques [3]. In general, RPO refers to activities where satellites are in the same orbit and approach each other at close distances. These activities include on-orbit servicing and repairs, docking, refueling, formation flying, and debris removal. Many missions currently make use of these capabilities including broadcast satellites, reconnaissance satellites, and large constellations. There are two types of RPO that most of these maneuvers fall under. *Cooperative RPO* occurs when information transfer (e.g. position, trajectory, health status) is multi-way over crosslinks or via ground station, such as a docking procedure with the International Space Station (ISS) or a multi-point inspection of a downed satellite. *Non-cooperative RPO* refers to activities where the information transfer is one way, such as active debris removal or inspection of a downed satellite. As space is a costly and harsh environment to deploy technology in, services that can improve or extend the lifetime of satellites are of great interest to stakeholders.

RPO maneuvers require that detailed information about a satellite's attitude, trajectory, and state-of-health information be shared with others nearby. The error margins on all of those values also must be shared to properly assess the risks of certain maneuvers and confidence in the calculated distances or other measurements. This is often vital to maintain physical safety and the need for accuracy increases as satellites operate closer and closer to one another. In many calculations, this is determined using covariance matrices. Uncertainty is part of all stochastic systems since values such as position are probabilistic in space, not deterministic, meaning there is some element of randomness that must be accounted for and quantified. Covariance matrices define an ellipsoid around a satellite that describes the uncertainty about a measured value, such as a satellite's location in space. As shown in Figure 3, this typically about $10 - 15$ km at the widest point. The $1/3\sigma$ accuracy is conventional for guaranteeing high accuracy for measurements in empirical systems, and is therefore the standard for space measurements.

A large motivating factor in RPO development is autonomy. Increasingly, satellites are operating in such close

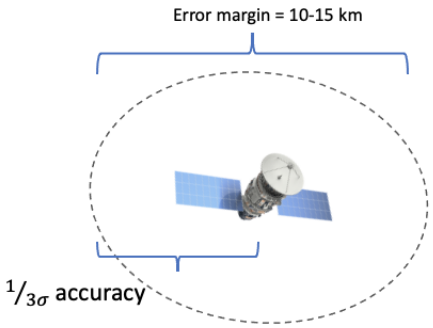


Fig. 3 Satellite ellipsoid of error margins

Table 1 Values of distances, time, and speeds for determining when satellite control can be done from the ground station and when autonomous RPO becomes necessary.

	Ground Station	On-board
Example	Conjunction Analysis	RPO
Satellite Distances	$1 - 10$ Mm	< 500 km
Time Needed	days - weeks	< 1 day
Speed	km/sec	m/sec

ranges that controlling them from the ground is difficult or infeasible. Instead, they need capabilities to run autonomous, on-board operations to make adjustments in real-time. Table 1 lists some of the contributing factors to differentiate when operations need to be done autonomously and on-board or when control can be left with the ground station. Conjunction analysis is one example of an activity between two or more satellites that can be done through communication via ground stations. This is because the satellite distances are on the order of megameters so operators typically have days or weeks to coordinate trajectories. Autonomous capability becomes necessary once the distance between satellites drops to about 500 kilometers. At these ranges, the satellites have anywhere from a day to just a couple of minutes to coordinate their trajectory.

B. Privacy Preserving Space Computing

Privacy-preserving computation is a set of cryptographic protocols that allow for mutually distrusting parties to jointly compute some function without revealing information about their inputs. Currently, strong cryptographic measures exist in standardized practice for data 'in transit' or 'at rest' but there is not yet an accepted standard for data 'during computation'. Data typically has to be decrypted in order for operations to be carried out [10]. This is where privacy-preserving computation shows great promise for data security in a variety of fields [11, 12]. Secure multi-party computation (SMC) in particular is a well-researched and promising method of privacy-preserving computation. The field of secure computation was initiated by Yao's work in the 1980s on the millionaire's problem and secure function evaluation [13, 14]. Many general-purpose compilers have since been developed to securely compute arbitrary functions, make SMC a more accessible approach for developers, and enable more widespread use of this as a privacy solution. [15].

There are two main approaches to SMC: garbled circuits and secret sharing. The garbled circuit approach is based on Boolean circuits and is used when only two parties are involved. The other mathematical approach is secret sharing, which provides information-theoretic security guarantees and allows for secure computation with an arbitrary number of parties. This method relies on strong multiplication rather than public-key primitives and uses zero-knowledge proofs to ensure that users and computing parties are following the protocol [16]. Secret sharing schemes divide the secret from "donors," parties providing the input, into shares distributed randomly among N computing parties or "miners", as shown in Figure 6a. Authorized subsets of N perform the computation and then return the output to the donors. This method guarantees that no useful information can be gained about the secret until a sufficient number of the miners, k out of N, are compromised and combine their respective shares. In other words, there is no loss of

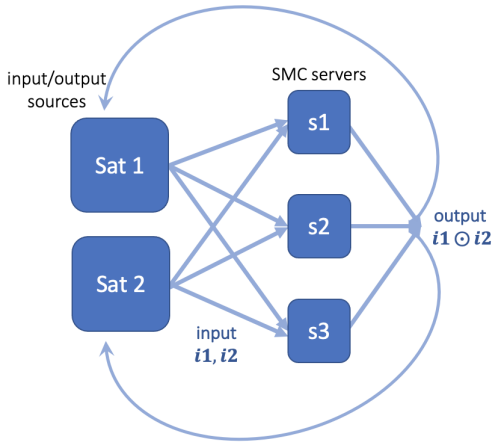


Fig. 4 Linear Secret Sharing SMC Setup

security through the compromise of $k - 1$ shares. This is an important consideration in the space environment (or any other harsh environment), as some of the miners could be compromised by an adversary or by a radiation event or other natural catastrophe that occurs in space. Our research uses this secret sharing approach for SMC where a minimum of 3 satellites are needed for SMC computation: 2 or more donors submitting shares of information and 3 miner satellites, which can also function as donors. We implement this using the Sharemind software platform, a secret sharing-based collection of dedicated servers and libraries for C++ applications [17].

C. Previous Efforts with SMC in Space

Privacy is difficult to implement on-orbit given the constraints of the limited technology that survives in space and the limited processing power available on board. Studies have been done specifically with the goal of addressing conjunction analysis with SMC, including a detailed report by the RAND corporation [18], a hybrid SMC approach developed by Hemenway et. al [19], and a secret sharing approach developed by Sharemind researchers in partnership with DARPA [20]. Determining the feasibility of using modern cryptography methods to secure SSA data is a problem of growing interest and is being explored by numerous government organizations and many private companies [21].

The works by Hemenway et al. and Kamm [19, 20], each explain a numerical collision probability method to calculate conjunction analysis where the privatized input is composed of four parts: position vectors, velocity vectors, covariance matrices, and radii. Both papers demonstrate that SMC operates very well and with high precision, even in highly complicated mathematics such as these numerical probability calculations. The problem is that position and velocity values do not need to be kept secret at these distances, as public databases exist with detailed trajectory information that is more than accurate enough to prevent collisions at these vast distances [**?**]. In the calculations detailed in these papers, the only values that may be beneficial to keep private are the covariance matrices, which could lead to inferences about the sensors and satellite design. Our research is in a different vein of satellite security since conjunction analyses occur at ground stations and do not need on-board capabilities at these large distances. As shown in Table 1, it is not until satellites drop to distances of kilometers apart from each other that RPO and autonomous capabilities become relevant. The focus of our paper is on RPO security and addressing additional challenges associated with on-board and autonomous processing.

D. RPO Regulation and Security Efforts

There is a glaring absence of security and privacy being addressed in RPO development. Efforts are being made to increase regulatory framework and policy standards, including the Consortium for Execution of Rendezvous and Servicing Operations (CONFERS) established by DARPA, which seeks to enhance operational safety and mission success in RPO [22]. Additionally, NASA and other ISS partner agencies have ongoing efforts in place to establish international space operations standards, including a section on rendezvous system interoperability standards [23]. This details different phases of RPO extensively and is part of the larger goal of multiple international space agencies to

create compatibility between spacecraft regardless of the spacecraft developer via internationally accepted designs and standards. Efforts are also being made to ensure physical safety through widely recognized standards controlling RPO and increased information sharing, but these neglect to account for data security and privacy [24].

III. Design and Implementation

A. Security Model and Threat Assumptions

The attack surface in space is becoming exponentially larger as space becomes more accessible and the numbers of both space- and ground-based assets rise. The vulnerabilities present in space are not only problematic for space-based assets but also pose great risks to ground-based systems. In past decades, cyber attacks in space were not a great concern for several reasons, mainly a closed supply chain for critical infrastructure, unique space-specific hardware and software, communications systems that were air-gapped from the commercial internet and inherently more secure, and nearly impossible physical access once the spacecraft was launched [1]. According to Global Counterspace Capabilities, the trend toward increased commercial space systems opens up great potential for innovation on earth but also creates greater levels of unsecured congestion and competition in space [25].

One issue that we address in this research is a rising problem with increased satellite usage and growing commercial development in space: satellite characterization. Certain questions, such as what space assets are in orbit, who they belong to, what their purpose is, and what is their operational status, can all be answered through the characterization process [26]. Traditionally, satellites are characterized from the ground through optical data, such as brightness or reflectance, that determines satellites' size, orientation, and material properties [27]. These correlations between spacecraft states and associated properties are captured with a certain level of accuracy in characterization, and covariance matrices are determined based on the built-in uncertainty in the optical sensors to determine confidence in the characterization results. While optical characterization is well-established and often necessary to maintain safe operations in space, RPO introduces a new level of characterization possibilities that may be unfavorable to private companies seeking to maintain innovative properties or privacy of sensitive data. Values such as proprietary design or novel sensor development may be determined from shared information about sensors. This is due to the need to share detailed information about satellite hardware, state-of-health telemetry (such as power and heat use), and associated covariance matrices to protect spacecraft operations at close distances. Certain observables can be examined from the ground and optical equipment, but others can only be obtained from being in close proximity to other spacecraft and especially from shared information from other vehicles. As Figure 2 illustrates, concrete observables of other satellites, such as the orientation or trajectory, can be filtered to lead to inferred properties, such as what kind of propulsion system is being used, which can then lead to inferred applications, such as the satellite's origin or application, determined by learning algorithms and data analyses. Our threat assumptions therefore include satellite stakeholders or operators that would seek to use characterization for negative purposes, including gaining knowledge of proprietary designs or compromising the privacy of sensitive data.

B. Software Design

For this paper, we perform tests of two example RPO algorithms where we privatize certain data inputs and measure the overhead that SMC adds to the secured algorithm. This is to demonstrate the usefulness and feasibility of SMC in real-world RPO scenarios. The values we determined remain private are domain-specific and will vary based on the objectives of the satellite owner. While this research demonstrates very specific examples, the broader applications are numerous and can be extended to any other data type that the satellite operators deem to be sensitive. First, we tested *matrix multiplication* to gain an understanding of how SMC scales for a computation that scales exponentially with matrix size. Then we tested two sample RPO algorithms directly to gain insight into how SMC would impact their efficiency in space. The second algorithm in our testing process is an attitude optimization algorithm, used in most RPO maneuvers to guide the vehicles into the same orbit, where both the fuel and the ending state are the parameters being optimized. The third algorithm is the quadratic program, a sensor fusion algorithm to optimize the information gathered by multiple vehicles' sensors and return the optimized data to each vehicle. Each of these algorithms is instrumental in many RPO maneuvers and therefore important in the testing and benchmarking process. The third algorithm is the only one we test, however, to address the RPO characterization problem, demonstrating the privatization of the satellites' sensor covariance matrices. Figure 5 gives a visual of how SMC works in an autonomous RPO algorithm, housed in the guidance navigation and control (GNC) unit of a satellite, which allows for on-board trajectory modification and

path-updating capabilities.

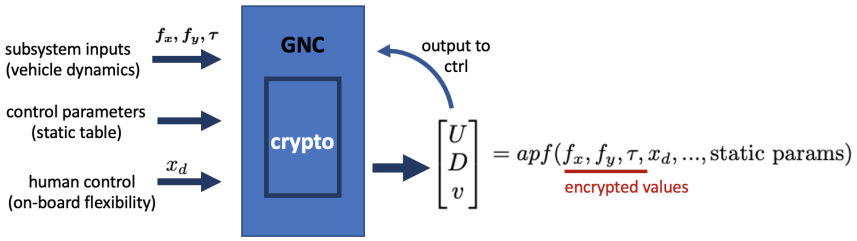


Fig. 5 Example Computation with Cryptography in the GNC Unit of a Satellite

The software is built using the Sharemind SMC framework. We chose this platform as it has been used in a wide variety of applications, including space scenarios and algorithms [20]. According to the evaluation of existing SMC compilers done by Hastings et al., Sharemind demonstrated a high level of functionality and support for many different data and operation types [15]. These algorithms are written in SecreC, Sharemind's C-like language that allows for protection domains, which define different SMC schemes, to be declared. For this research, we use the *shared3p* protection domain, as we are testing the case of three computation nodes. SecreC allows for detailed instructions to be given to the computation servers regarding which input parameters must remain secure [28]. We benchmark the overhead in each algorithm by comparing the time needed to perform the operations under different constraints. The benchmarking metrics are detailed further in Section V. For this research, we use primitive data types, Boolean and unsigned integer values (specifically *uint64*) in the operations to understand the impact of SMC in the algorithms' efficiency. Sharemind also supports operations for more complex data types including floating point numbers. Security in Sharemind applications is dependent on the assumption that the three satellites do not collude. We tested a preliminary matrix multiplication program to gain an idea of the feasibility of this SMC approach with a computationally expensive program. This was determined to be very reasonable so we moved on to testing RPO algorithms.

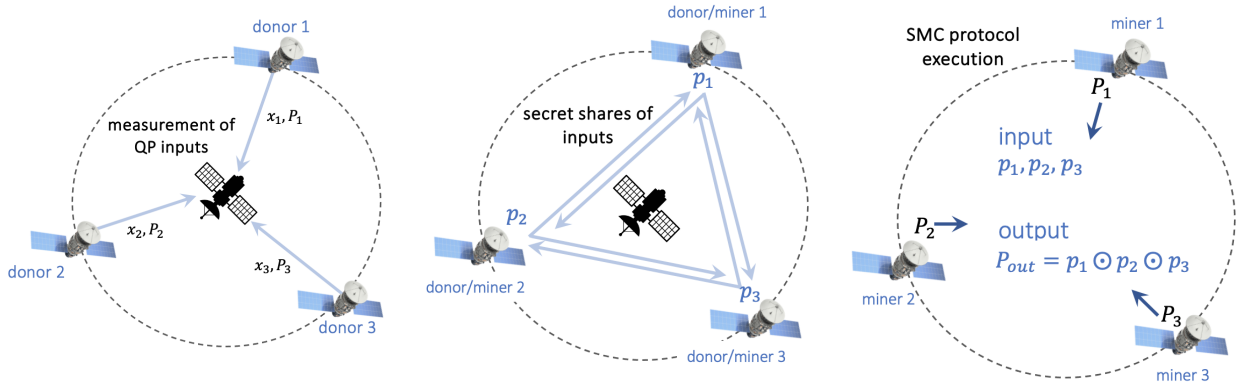
C. Attitude Optimization

The first RPO algorithm we test is an attitude optimization algorithm. This is a necessary process in many RPO scenarios, especially where formation flying or multi-point inspection is involved. In these cases, 3 or more satellites are usually involved and therefore cooperation between 3 or more organizations may be needed. This algorithm commands the torque to guide the attitude of the satellites in a system to zero relative to each other. It uses an optimization process known as fast gradient descent and a blended cost approach, where both the fuel and ending state of each satellite are optimized. Shared input parameters in this algorithm are initial states, specifically angular velocity, initial time, principal inertia, period of the algorithm (how many times it is called per second), the number of states, and the number of control parameters. The values we determined to keep private for these tests were the initial states, each satellite's angular velocity and initial time.

D. Quadratic Program Optimization

The second RPO algorithm evaluated in this paper is a joint optimization program where three parties (i.e. satellites) provide input from their sensors on the location of a fourth party (i.e. a downed or unresponsive satellite). Figure 6 illustrates how this scenario works with SMC, where the secret from donors is divided into shares distributed randomly among N miners shown in Figures 6(a) and 6(b). This is an example of a multi-point inspection requiring 3 or more data points to satisfy the relative mechanics in space and maximize the accuracy of the measurements they are taking. Then authorized subsets of N miners, all three satellites in this case, perform the computation and then return the output to the donors, as shown in Figure 6(c).

This algorithm is made up of two parts: a spacecraft propagation function, contributing simulated $\hat{x}$ and P values, and a quadratic program, a filtering program that performs a minimization of the position and uncertainty values. The quadratic program is an optimization problem with a quadratic objective function and a set of linear constraints [29]. In this scenario, the optimization produces an estimation of the true position of the downed satellite, the most likely $\hat{x}$, P, which is accepted by the contributing nodes, satellites $1, ..., n$, as the true solution. The values we privatized for the secure version of this algorithm are the covariance matrices, P. For future applications, the privacy measures could be



(a) Each satellite starting as 3 donors, measuring input data, $\{x, P\}$, to determine the position of the fourth satellite (x) and the associated uncertainty (P)

(b) Each satellite now functioning as both donor and miner, divide their secret inputs, p, into shares and distribute to each other, the other miners.

(c) Miners performing SMC on the inputs, P_i, on data shares and distributing result to all satellites.

Fig. 6 Quadratic Program: Multi-Point Inspection

expanded to other inputs, such as the position vectors, additional sensor information, state-of-health telemetry, or other values the operator deemed sensitive.

E. Experimental Setup

To gain a realistic idea of how our software would run in space, we determined what kind of processors run well and therefore would be used in space, and tested our algorithms on embedded processing boards that simulate a satellite cluster. The boards should ideally be commercially available, as there is greater accessibility and capability of commercial parts, as well as reduced financial costs for satellite stakeholders. All electronic parts running in space however must tolerate a high radiation environment [6]. According to research done by the Air Force Research Laboratory (AFRL), the current findings show that many NVIDIA boards, running ARM CPUs, and certain AMD boards running x86 architecture happen to tolerate the space environment very well [30]. Our experimental setup emulates a cluster of three satellites which we represent using three Intel NUCs. These boards are ideal for developing and optimizing the software and use an x86 CPU similar to AMD Ryzen boards which tolerate the space environment well. For research and development purposes, we use more readily accessible boards as opposed to radiation-hardened ones, though to deploy in space we would implement this work on the AMD Ryzen board or their equivalent.

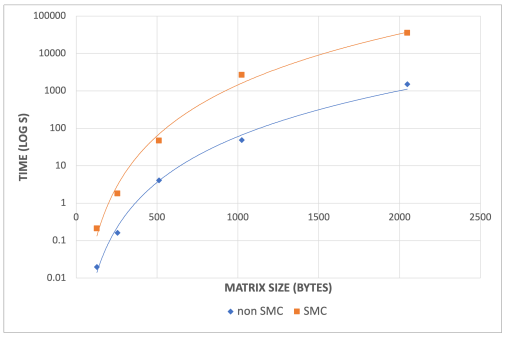
IV. Results and Analysis

We implemented secure versions of two RPO sample algorithms using Sharemind's secure computation system. The testing process involved measuring the efficiency of each secured (SMC) algorithm and comparing that to each unsecured (without SMC) algorithm. Matrix multiplication was done to gain a preliminary idea of the order of magnitude by which SMC increases the overhead of a computationally expensive RPO-related program. This benchmarking involved both versions of matrix multiplication to gain an idea of the order of magnitude by which SMC increases the overhead. As Fig. 7a shows, the SMC version of each matrix accumulates about 1 to 1.5 orders of magnitude of overhead more than the corresponding standard version.

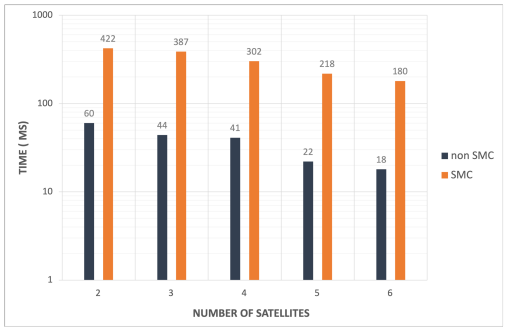
A. Attitude Optimization

The first RPO algorithm we tested was attitude optimization. The privatized inputs for the secure algorithm are the initial states, determined by the initial angular velocity of each satellite, and the initial time. To benchmark this test, we varied the number of satellites involved in the calculation and compared the time it takes the program to guide the torque of the system to zero, both unsecured and secured. Figure 7(a) shows these results, where the vertical axis is time (again logarithmic in microseconds) and the horizontal axis is the number of satellites we tested.

Our testing of the attitude optimization algorithm, as shown in Figure 7(b), shows that the secure version increased the time to perform each function by approximately 1 order of magnitude. The purposes of this algorithm require that

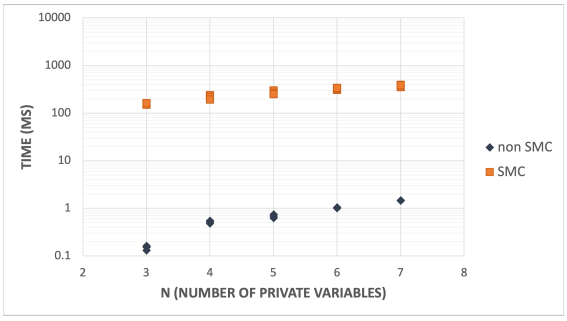


(a) Results of Matrix Multiplication benchmarking

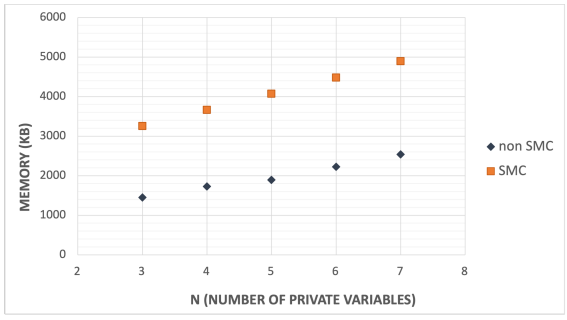


(b) Results of Attitude Optimization benchmarking

Fig. 7 Time Overhead Benchmarking for Matrix Multiplication and Attitude Optimization



(a) Quadratic Program Time Overhead



(b) Quadratic Program Memory Overhead

Fig. 8 Quadratic Program Benchmarking

this calculation not exceed 10 seconds to complete so even with this increase in overhead, the algorithm still runs in well below half a second, leading us to conclude that it is reasonable to use SMC in this RPO application.

B. Quadratic Program Optimization

To gain a realistic idea of using SMC to privatize covariance matrices, we tested a secured and unsecured version of a quadratic program. As done with the previous two algorithms, we tested the time efficiency of the two versions of the algorithm. For this algorithm, the results of using SMC to secure the covariance matrices, P, are shown in Figure 8. Figure 8(a) shows the results of this test where the vertical axis denotes time in microseconds and the horizontal axis is n, the number of satellites involved in the optimization algorithm. Additionally, we measured the overhead for this algorithm in terms of space, or memory used, as given in Figure 8(b).

The overhead accrued by the secured version of the algorithm demonstrated a $2-3$ orders of magnitude increase in time of execution and < 1 order of magnitude of memory usage. Determining if this overhead is reasonable is case-specific and depends on how rapidly the measurements need to be updated in order to maintain optimal physical safety during the RPO maneuvers. The speed at which the program needs to operate depends on how close the satellites are to each other, where the closer the distance the more rapidly the operation needs to occur. In the most rapid case, if the spacecraft are within about 10 meters of each other, this algorithm would need to operate in 30 seconds or less. Any faster rates of operation would only lead to inefficient fuel use for the satellite. We can therefore conclude that a $2-3$ order of magnitude increase in time, where the execution time remains well under 1 second, is feasible for the algorithm to still run efficiently enough for its purpose.

V. Limitations and Future Work

Our contribution is an analysis of an advanced and promising cryptographic method relevant to space computing applications. Some limitations of this research include that the algorithms have not been tested directly on radiation-

tolerant hardware. This is due to the fact that it is expensive to obtain and the hardware that we did test on was similar in function and resources to what would be deployed in space. Another area of improvement would be in the optimization of the code in each algorithm. Additionally, there are limitations in the use of Sharemind, a third-party platform, as opposed to our own SMC platform or something open-source such as MP-SPDZ [31]. The next steps of this research include further improvements to our current results using methods such as greater parallelization in the SMC code and single instruction multiple data (SIMD) vectorization to improve scalability [32]. We also plan to deploy these RPO algorithms on hardware for testing in space, specifically AMD Ryzen boards, to gain a greater understanding of the practicality of using SMC in space. Our goal is to develop cryptographic and domain-informed design optimizations for satellite-related algorithms. Additional future work includes conducting information flow analysis to ensure that privatized variables and functions do not taint other functions in the algorithm. We plan to conduct this using static and dynamic analysis techniques [33, 34].

VI. Conclusion

Computing in space is becoming more relevant and ubiquitous which makes it an attractive landscape for future hacking and malicious action in cyberspace. Security must be a leading area of research and be accounted for early on in the development of space computing technology. For this reason, space has become a leading interest in the security community but unfortunately is often accompanied by a lack of domain-specific knowledge of space and what problems are relevant to the space research community. This research addresses several concerns in space computing: the need for strong security measures for the in-space segment of satellite operations, the advancement of RPO, and need for a bridge between space dynamics and security experts, and the problem of characterization as a real threat to satellite stakeholders. SMC is a tool that we employ to address data privacy during RPO computations to protect against unnecessary information leakage leading to advanced satellite characterization. SMC is thus a viable means for assuring the satellite characterization threat and provides a promising direction for protecting space computation.

Acknowledgments

The views expressed are those of the author and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. government. Distribution Statement A: Approved for Public Release. Distribution is Unlimited. Public Affairs Release Approval #O-2102. This work is supported by the Air Force grant AFRL-FA9550-19-1-0169.

References

[1] Brandon Bailey, P. A. D. N. C. C. W. A. W., RYAN J. SPEELMAN, "Defending Satellites in the Cyber Domain," *Aerospace Corporation: Center for Space Policy and Strategy*, 2019. URL `https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf`.

[2] Reesman, R., and Rogers, A., "GettinG in Your Space : LearninG from paSt rendezvouS and proximitY operationS CENTER FOR SPACE POLICY AND STRATEGY," 2018. URL `https://api.semanticscholar.org/CorpusID:13716888`.

[3] Barnhart, D., Rughani, R., Allam, J., Weeden, B., Slane, F., and Christensen, I., "Using Historical Practices to Develop Safety Standards for Cooperative On-Orbit Rendezvous and Proximity Operations," 2018.

[4] Archer, D. W., Bogdanov, D., Pinkas, B., and Pullonen, P., "Maturity and Performance of Programmable Secure Computation," *IEEE Security & Privacy*, Vol. 14, No. 5, 2016, pp. 48–56. https://doi.org/10.1109/MSP.2016.97, URL http://ieeexplore.ieee.org/document/7676176/.

[5] "Space Launch System begins vibration testing," , Sep. 2021. URL https://www.spaceflightinsider.com/organizations/nasa/space-launch-system-begins-vibration-testing/, section: NASA.

[6] Topper, A. D., Lauenstein, J.-M., Wilcox, E. P., Berg, M. D., Campola, M. J., Casey, M. C., Wyrwas, E. J., O'Bryan, M. V., Carstens, T. A., Fedele, C. M., Forney, J. D., Kim, H. S., Osheroff, J. M., Phan, A. M., Chaiken, M. F., Cochran, D. J., Pellish, J. A., and Majewicz, P. J., "NASA Goddard Space Flight Center's Compendium of Radiation Effects Test Results," *2020 IEEE Radiation Effects Data Workshop (in conjunction with 2020 NSREC)*, IEEE, Santa Fe, NM, USA, 2020, pp. 1–12. https://doi.org/10.1109/REDW51883.2020.9325841, URL https://ieeexplore.ieee.org/document/9325841/.

[7] Hainaut, O. R., and Williams, A. P., "Impact of satellite constellations on astronomical observations with ESO telescopes in the visible and infrared domains," *Astronomy & Astrophysics*, Vol. 636, 2020, p. A121. https://doi.org/10.1051/0004-6361/202037501, URL https://www.aanda.org/10.1051/0004-6361/202037501.

[8] Banik, U., Ali, S. M. R., and Rahman, M., "Orbital debris: Threat analysis and satellite security compliances," *2017 2nd International Conference for Convergence in Technology (I2CT)*, 2017, pp. 988–992. https://doi.org/10.1109/I2CT.2017.8226277.

[9] Welser, B. H., Bill, "Cryptographers Could Prevent Satellite Collisions," , ???? https://doi.org/10.1038/scientificamerican0215-28b, URL https://www.scientificamerican.com/article/cryptographers-could-prevent-satellite-collisions/.

[10] Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Smart, N. P., and Wright, R. N., "From Keys to Databases—Real-World Applications of Secure Multi-Party Computation," *The Computer Journal*, Vol. 61, No. 12, 2018, pp. 1749–1771. https://doi.org/10.1093/comjnl/bxy090, URL https://doi.org/10.1093/comjnl/bxy090.

[11] Mood, B., Gupta, D., Carter, H., Butler, K., and Traynor, P., "Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation," *2016 IEEE European Symposium on Security and Privacy (EuroSP)*, 2016, pp. 112–127. https://doi.org/10.1109/EuroSP.2016.20.

[12] Mood, B., Gupta, D., Butler, K., and Feigenbaum, J., "Reuse It Or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values," *Proceedings of the ACM Conference on Computer and Communications Security*, 2015. https://doi.org/10.1145/2660267.2660285.

[13] Yao, A. C., "Protocols for Secure Computations," *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, USA, 1982, p. 160–164.

[14] Yao, A. C.-C., "How to generate and exchange secrets," *27th Annual Symposium on Foundations of Computer Science (FOCS 1986)*, 1986, pp. 162–167. https://doi.org/10.1109/SFCS.1986.25.

[15] Hastings, M., Hemenway, B., Noble, D., and Zdancewic, S., "SoK: General Purpose Compilers for Secure Multi-Party Computation," *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1220–1237. https://doi.org/10.1109/SP.2019.00028.

[16] Ishai, Y., Kushilevitz, E., Ostrovsky, R., and Sahai, A., "Zero-Knowledge Proofs from Secure Multiparty Computation," *SIAM Journal on Computing*, Vol. 39, No. 3, 2009, pp. 1121–1152. https://doi.org/10.1137/080725398, URL https://doi.org/10.1137/080725398.

[17] Bogdanov, D., Laur, S., and Willemson, J., "Sharemind: A Framework for Fast Privacy-Preserving Computations," *Computer Security - ESORICS 2008*, Vol. 5283, edited by S. Jajodia and J. Lopez, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 192–206. https://doi.org/10.1007/978-3-540-88313-5_13, URL http://link.springer.com/10.1007/978-3-540-88313-5_13, series Title: Lecture Notes in Computer Science.

[18] Hemenway, B., Lu, S., Ostrovsky, R., and Welser IV, W., "High-Precision Secure Computation of Satellite Collision Probabilities," *Security and Cryptography for Networks*, Vol. 9841, edited by V. Zikas and R. De Prisco, Springer International Publishing, Cham, 2016, pp. 169–187. https://doi.org/10.1007/978-3-319-44618-9_9, URL http://link.springer.com/10.1007/978-3-319-44618-9_9, series Title: Lecture Notes in Computer Science.

[19] Hemenway, B., Lu, S., Ostrovsky, R., and IV, W. W., "High-precision Secure Computation of Satellite Collision Probabilities," Cryptology ePrint Archive, Paper 2016/319, 2016. URL https://eprint.iacr.org/2016/319, https://eprint.iacr.org/2016/319.

[20] Kamm, L., and Willemson, J., "Secure floating point arithmetic and private satellite collision analysis," *International Journal of Information Security*, Vol. 14, No. 6, 2015, pp. 531–548. https://doi.org/10.1007/s10207-014-0271-8, URL https://doi.org/10.1007/s10207-014-0271-8.

[21] Foust, J., "FCC approves Starlink License Modification," , Apr 2021. URL https://spacenews.com/fcc-approves-Starlink-license-modification/.

[22] Consortium for Execution of Rendezvous and Servicing Operations, "CONFERS Recommended Design and Operational Practices," , October 2022. URL https://satelliteconfers.org/wp-content/uploads/2022/10/CONFERS_Operating_Practices_REV3_Oct2022.pdf.

[23] "INTERNATIONAL RENDEZVOUS SYSTEM INTEROPERABILITY STANDARDS CONCURRENCE," , February 2018. URL https://www.internationaldeepspacestandards.com/wp-content/uploads/sites/45/2018/02/Rendezvous_020918_R1.pdf.

[24] Staats, B., "Mitigating Security Risks and Potential Threats of Emerging Rendezvous and Proximity Operations," *Astropolitics*, Vol. 20, No. 1, 2022, pp. 64–92. https://doi.org/10.1080/14777622.2022.2080547, URL https://doi.org/10.1080/14777622.2022.2080547.

[25] Weeden, B., and Samson, V., *Global counterspace capabilities: An open source assessment*, Secure World Foundation Washington, DC, 2018.

[26] Jah, M., and Madler, R. A., "Satellite characterization: angles and light curve data fusion for spacecraft state and parameter estimation," *Proceedings of the advanced Maui optical and space surveillance technologies conference*, Vol. 49, 2007.

[27] Scott, R., and Wallace, B., "Satellite characterization using small aperture instruments at DRDC Ottawa," *Proceedings of the Advanced Maui Optical and Space Surveillance Technologies Conference*, 2008, pp. 337–347.

[28] Jagomägis, R., "SecreC: a Privacy-Aware Programming Language with Applications in Data Mining," *Master Thesis, University of Tartu*, 2010.

[29] Nocedal, J., and Wright, S. J., *Numerical Optimization*, 2nd ed., Springer, New York, NY, USA, 2006.

[30] Lovelly, T. M., Mee, J. K., Lyke, J. C., Pineda, A. C., Bole, K. D., and Pugh, R. D., "Evaluating Commercial Processors for Spaceflight with the Heterogeneous On-Orbit Processing Engine," *2019 IEEE Aerospace Conference*, 2019, pp. 1–6. https://doi.org/10.1109/AERO.2019.8741866.

[31] Keller, M., "MP-SPDZ: A Versatile Framework for Multi-Party Computation," Cryptology ePrint Archive, Paper 2020/521, 2020. https://doi.org/10.1145/3372297.3417872, URL https://eprint.iacr.org/2020/521, https://eprint.iacr.org/2020/521.

[32] Liang, X., Humos, A. A., and Pei, T., "Vectorization and Parallelization of Loops in C/C++ Code," *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)*, 2017, pp. 203–206.

[33] Palit, T., Firose Moon, J., Monrose, F., and Polychronakis, M., "DynPTA: Combining Static and Dynamic Analysis for Practical Selective Data Protection," *2021 IEEE Symposium on Security and Privacy (SP)*, IEEE, San Francisco, CA, USA, 2021, pp. 1919–1937. https://doi.org/10.1109/SP40001.2021.00082, URL https://ieeexplore.ieee.org/document/9519446/.

[34] Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B., Cox, L., Jung, J., McDaniel, P., and Sheth, A., "TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Transactions on Computer Systems*, Vol. 32, No. 2, 2014. https://doi.org/10.1145/2619091, copyright: Copyright 2014 Elsevier B.V., All rights reserved.