Cybersecurity and Privacy in Space and Associated Domains: Update

Space is a Contested Environent

Many aspects of the space infrastructure need to be considered from a security perspective

The New York Times

U.S. Warns Allies Russia Could Put a Nuclear Weapon Into Orbit This Year

The American assessments are divided, however, and President Vladimir Putin denied having such an intention, saying that Russia was "categorically against" it.

Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service

Russia has deployed advanced tech to interfere with Elon Musk's satellite internet service, Ukrainian officials said, leading to more outages on the northern front battle line.

UF UNIVERSITY of FLORIDA | Duke UNIVERSITY | TEXAS The University of Texas at Austin | UC SANTA CRUZ

Recent Research in Space Security

Communication & Network security

Don’t Shoot the Messenger: Localization Prevention of Satellite Internet Users

The Dark Side of Scale: Insecurity of Direct-to-Cell Satellite Mega-Constellations

System security

Orbital Shield: Rethinking Satellite Security in the Commercial Off-the-Shelf Era

Recent Work in Related Areas

- Preliminary discussion of privacy-preserving computing for satellites (AIAA SciTech Forum'24)
- Directed energy (acoustic) attacks in underwater environments (IEEE S&P'24)
- Resilience of terrestrial communication infrastructure:
  - Overprivilege in 5G network functions (ACM WiSec'24)
  - Randomness and cryptography failures in 5G network cores (ACM CODASPY'24)
  - Fuzzing of cellular cores and RAN interfaces (ACM CCS'24)

Holistically Assessing Privacy-Preserving Satellite Computation for RPO and ISM

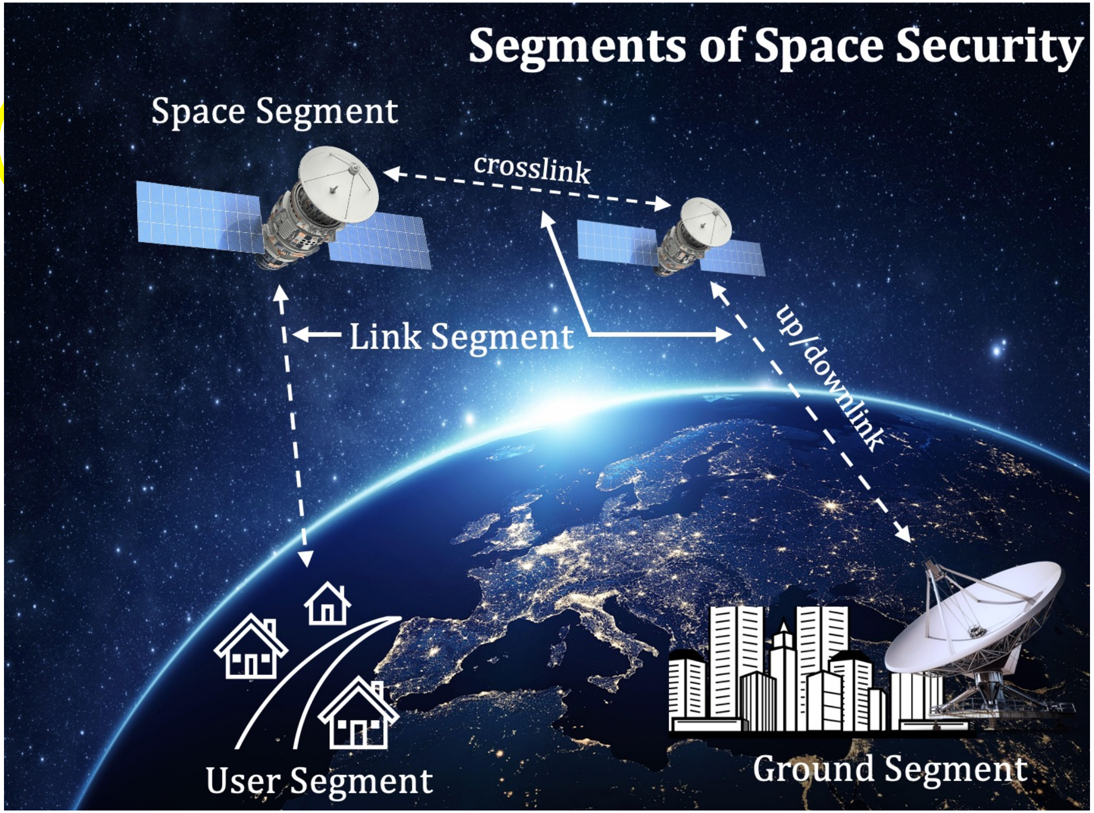
Caroline Fedele, **Carson Stillman**, Tyler Lovelly*, Christopher Peterson, and Kevin Butler

University of Florida, *University of New Mexico

May 2024

(In submission)

Security in Space



The Aerospace Corporation, 2019

- **Needs for both privacy and security in space**

IN-SPACE Cybersecurity

- **Growing number of satellites & expanding private sector**
- **Motivates autonomy needs**
- **Rendezvous & Proximity Operations (RPO)**
- **Near-field collision avoidance and characterization**

Project Overview

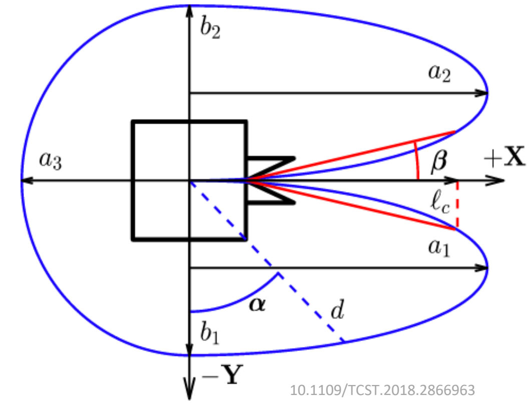
General goal: address security and privacy challenges in satellite rendezvous and proximity operations (RPO) and in-space manufacturing (ISM)

- Examining existing limitations of secure multiparty computation (SMC) in space applications
  - Limited existing research on *space segment* and in-space operation security
- Implementation and evaluation of in-space RPO and ISM algorithms on space-certified hardware
  - Categorized mission scenarios and associated security requirements
  - Detailed adversarial scenarios and solutions
- Feasibility assessment of SMC in RPO/ISM given satellite operational constraints
  - characterize use of SMC protocols considering propagation, transmission, local execution time

Rendezvous and Proximity Operations (RPO):

- On-board trajectory operation and replanning
  - E.g. docking, on-orbit servicing/refueling, formation flying
- RPO occurs on-board, autonomously
  - housed in guidance navigation and control (GNC) unit
- Needed at scales of < 500km between satellites

RPO example: docking



10.1109/TCST.2018.2866963

Ground station vs On-board Control

	Ground station	On-Board
Distance between satellites	1-10 Mm	< 500 km
Time needed	Days-weeks	< 1 day
Speed	km /sec	m /sec
Approach	conjunction analysis	RPO

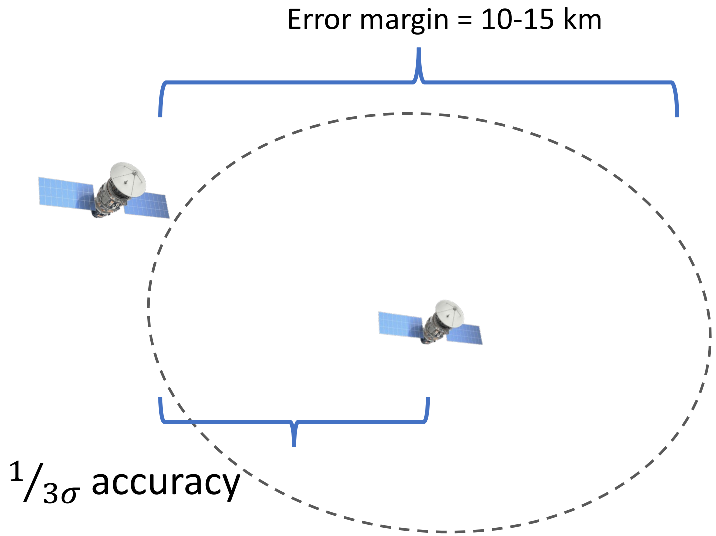
Problem: Capability Inference

Example: Collision Avoidance in RPO

- Minimum data to share with other satellites
  - position, velocity, ***covariance***

Stochastic systems

- Probabilistic, not deterministic
- Covariance matrices = quantify uncertainty
  - Calculated using intrinsic sensor variance
- Measure of TRUST, decisions based on accuracy



Problem: knowledge of error margins (covariance matrices) can lead to inferences on satellite capabilities, purpose, etc. through knowledge of sensors on board

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ

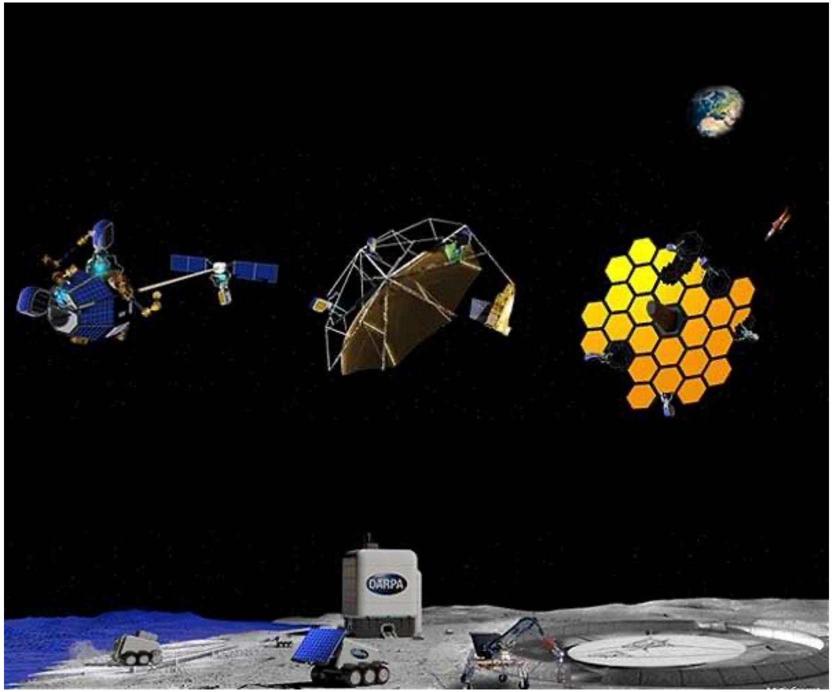
Motivation: In-Space Manufacturing

Example: In-Space Manufacturing

- Integrated circuits, advanced materials, bioengineering, large assembly (Luvoir telescope)

Sensitive Values*	Threat Assumptions
Covariance matrices	Infer proprietary sensor info
Fuel levels	May infer satellite capacity/mission objectives
State-of-health telemetry (e.g. power, heat use)	Infer propulsion system,
Installation/servicing technology parameters	Infer IP (e.g. IC design, robotic arm capability)

*not exhaustive list, values are mission dependent



Solution: protect sensitive values using privacy-preserving computation

Privacy-Preserving Computation

Privacy-Preserving Computation (PPC)

- Allows for data to remain encrypted during computation
- Protects **physical integrity** of satellite during RPO and **data privacy** keeping data encrypted

Secure Multiparty Computation (SMC):

- Cryptographic protocol that allows set of mutually-distrusting parties to jointly compute a function on their inputs, without revealing information about inputs (millionaire's problem)
    1. *2-Party Computation (2PC):* e.g. Yao's garbled or BMR, binary circuit representation
    2. *Secret sharing*: 3+ parties, arithmetic circuit representation

Secure Multiparty Computation Tool

Security Models

- Honest vs. dishonest majority – assumption of behavior of parties
- Semi-honest vs. malicious corruption – passive vs. active adversary

Computation Domain

Mathematical structure of secret info

- Usually ring structure defined by integer operation with modulus or Galois (finite) field
- Binary circuits or arithmetic circuits
  - Mod prime, mod power 2

Underlying Primitives

- Secret Sharing
- Garbled Circuits
- Oblivious Transfer
- Homomorphic Encryption

Security model	Mod prime / GF(2^n)	Mod 2^k	Bin. SS	Garbling
Malicious, dishonest majority	MASCOT / LowGear / HighGear	SPDZ2k	Tiny / Tinier	BMR
Semi-honest, dishonest majority	Semi / Hemi / Temi / Soho	Semi2k	SemiBin	Yao's GC / BMR
Malicious, honest majority	Shamir / Rep3 / PS / SY	Brain / Rep3 / PS / SY	Rep3 / CCD / PS	BMR
Semi-honest, honest majority	Shamir / ATLAS / Rep3	Rep3	Rep3 / CCD	BMR
Malicious, honest supermajority	Rep4	Rep4	Rep4	N/A
Semi-honest, dealer	Dealer	Dealer	Dealer	N/A

Table of supported protocols

Sharemind vs.MP-SPDZ

Sharemind	MP-SPDZ
Ease of use for industry & non-security professionals	Prominent tool for academic research uses
C++ and proprietary SecreC code	Python
1 SMC approach – linear secret sharing (3+ parties)	Over 30 SMC variants (GC, OT, FHE, SS)
1 security model (semi-honest)	3 security models (semi-honest, malicious, covert)
1 trust option (honest majority)	2 trust options (honest or dishonest majority)
Black box – cannot see or modify source code	White box – can see and modify source code

MP-SPDZ and Python

- MP-SPDZ can execute python code but only at compile time
  - This means we lose access to the large library of python math functions for any values that are secret
- We implemented many custom functions in MP-SPDZ including
  - Eigenvalues and Eigenvector solver
  - Integration Approximation using Simpson's Rule
  - An Error Function Approximation
  - Cross Products

```
def simpsons_rule(f, a, b, n):
    if n % 2 != 0:
        raise ValueError("Number of subintervals (n) must be even.")
    h = (b - a) / n
    x_values = [a + i * h for i in range(n + 1)]
    sum = f(a) + f(b)
    for i in range(1, n, 2):
        sum += 4 * f(x_values[i])
    for i in range(2, n-1, 2):
        sum += 2 * f(x_values[i])
    sum *= h / 3
    return sum
```

Program Selection

- We investigated three programs for test
  i. Alfano's Algorithm for Conjunction Analysis
  ii. Artificial Potential Function
  iii. Quadratic Program

```
P1_inverse = ml.mr(P1,1)
P2_inverse = ml.mr(P2,1)
P3_inverse = ml.mr(P3,1)

M = P1_inverse + P2_inverse + P3_inverse
V = P1_inverse*xhat1 + P2_inverse*xhat2 + P3_inverse*xhat3
M_inverse = ml.mr(M,1)
e = M_inverse*V
```

- We found Alfano's method required higher accuracy for float representations than the default value for MP-SPDZ
  - To achieve accurate results we had to raise the number of bits for the floating point representation
  - This severely impacted the execution time so we excluded Alfano's from our later tests

Methodology: hardware

Finding hardware for deployment in space

- Considerations:
  - Commercial off-the-shelf (COTS)
  - Sufficient radiation tolerance
  - Sufficient power & efficiency with limited resources

- Current findings:
  - NVIDIA Jetson Nano boards (ARM processors)

Emulate satellite cluster

- Prototype with 3 NVIDIA nano boards
- Networked to communicate with each other
- 3 satellites minimum needed for secret sharing

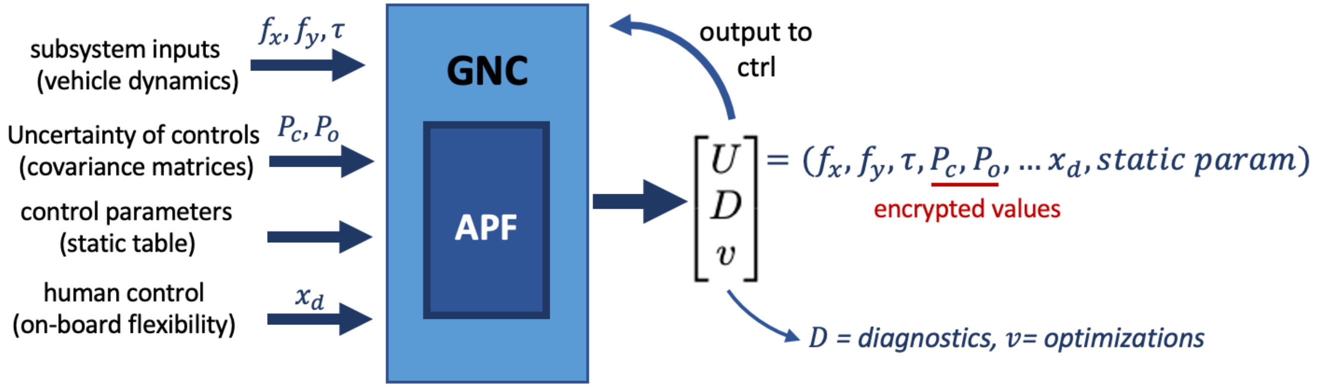
Algorithm 1: Artificial Potential Function

Artificial Potential Function (APF): conjunction analysis

- Autonomous Robotic Control algorithm
- Docking, service, collision avoidance
  - On-board trajectory control
- Assume linear orbital dynamics: one satellite stationary relative to other

Shared parameters

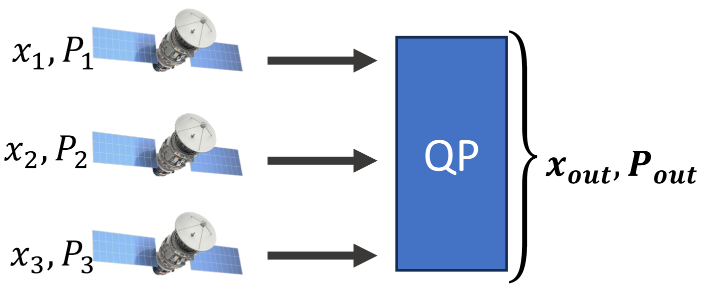
- Control forces : f_x, f_y, τ → **Public**
- Vehicles' covariance: P_c, P_o → **Private**

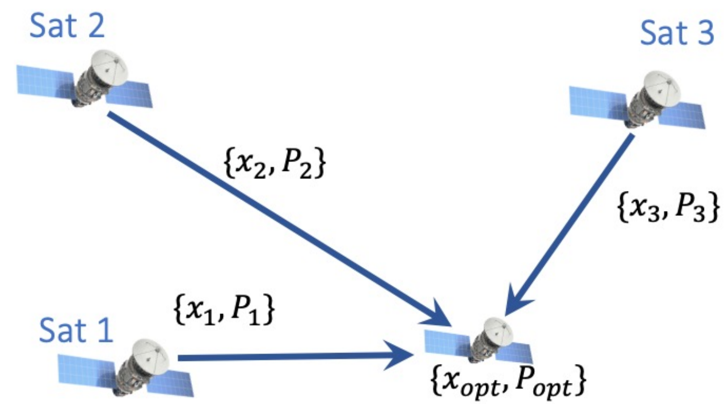


10.1007/978-981-10-2963-9_5

Quadratic Program: multi-point inspection

- Sensor Fusion optimization algorithm
- Need 3+ parties for 3 dimensional accuracy (secret sharing or homomorphic encryption)





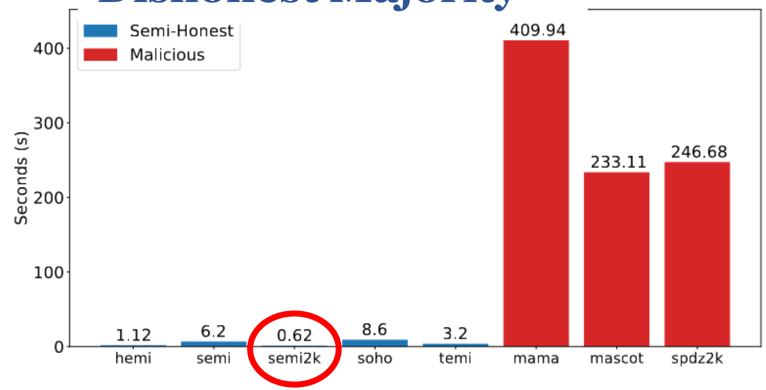
Shared parameters

- Measured positions: x_1, x_2, x_3 → **Public**
- Position covariance: P_1, P_2, P_3 → **Private**

Evaluation – APF Initial Benchmarks

Dishonest Majority

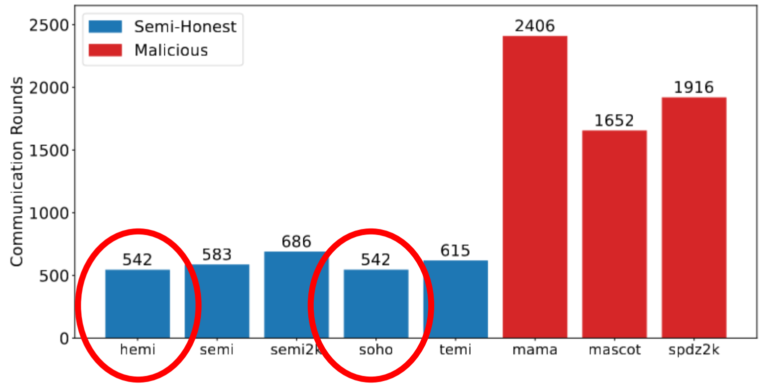
Local execution time



(a) Execution time comparison for the two-party MPC protocols running APF

BEST → semi2k

Communication rounds



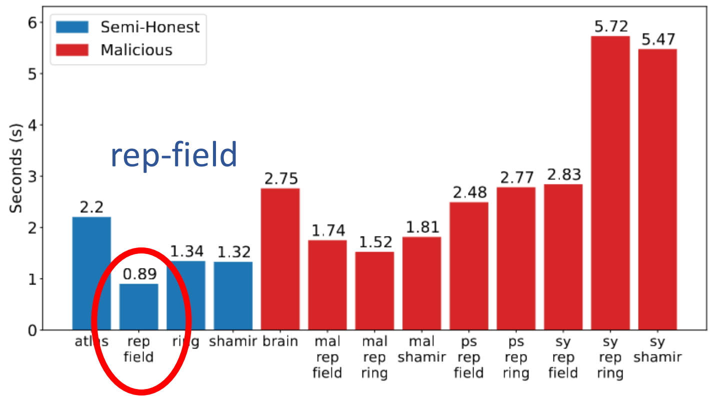
(b) Communication rounds comparison for the two-party MPC protocols running APF

BEST → hemi, soho

Evaluation: QP Initial Benchmarks

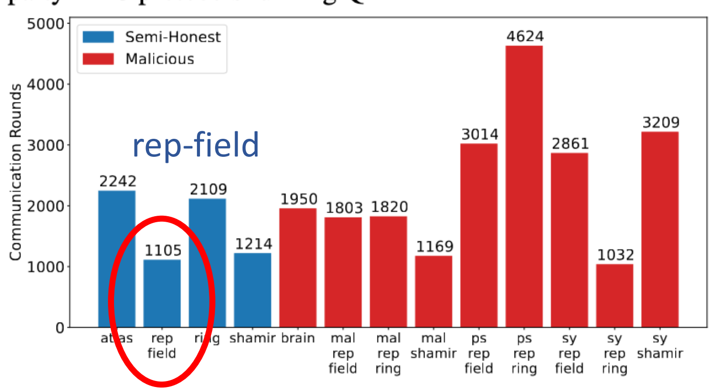
Honest Majority

Local exec time



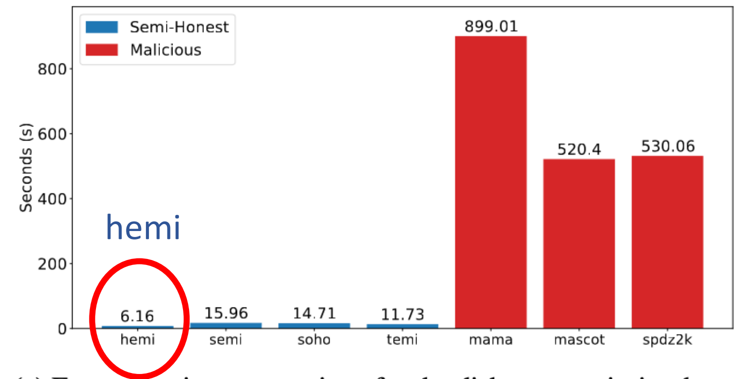
(a) Execution time comparison for the honest majority three-party MPC protocols running QP

Comm rounds

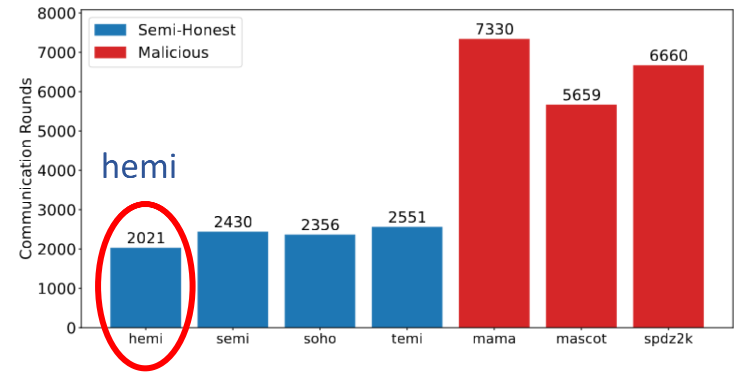


(b) Communication rounds comparison for the honest majority three-party MPC protocols running QP

Dishonest Majority



(a) Execution time comparison for the dishonest majority three-party MPC protocols running QP



(b) Communication rounds comparison for the dishonest majority three-party MPC protocols running QP

Total Execution Time

$$t_{tot} = t_{exec} + t_{prop} + t_{trans}$$

t_{exec}: The local execution time of the protocol

t_{prop}: The propagation time of the signal.

$$t_{prop} = comm\ rounds * \frac{500\ km}{c}$$

t_{trans}: The transmission time governed by the radios.

$$t_{trans} = \frac{data\ overhead\ (Mb)}{10\ \left(\frac{Mb}{s}\right)}$$

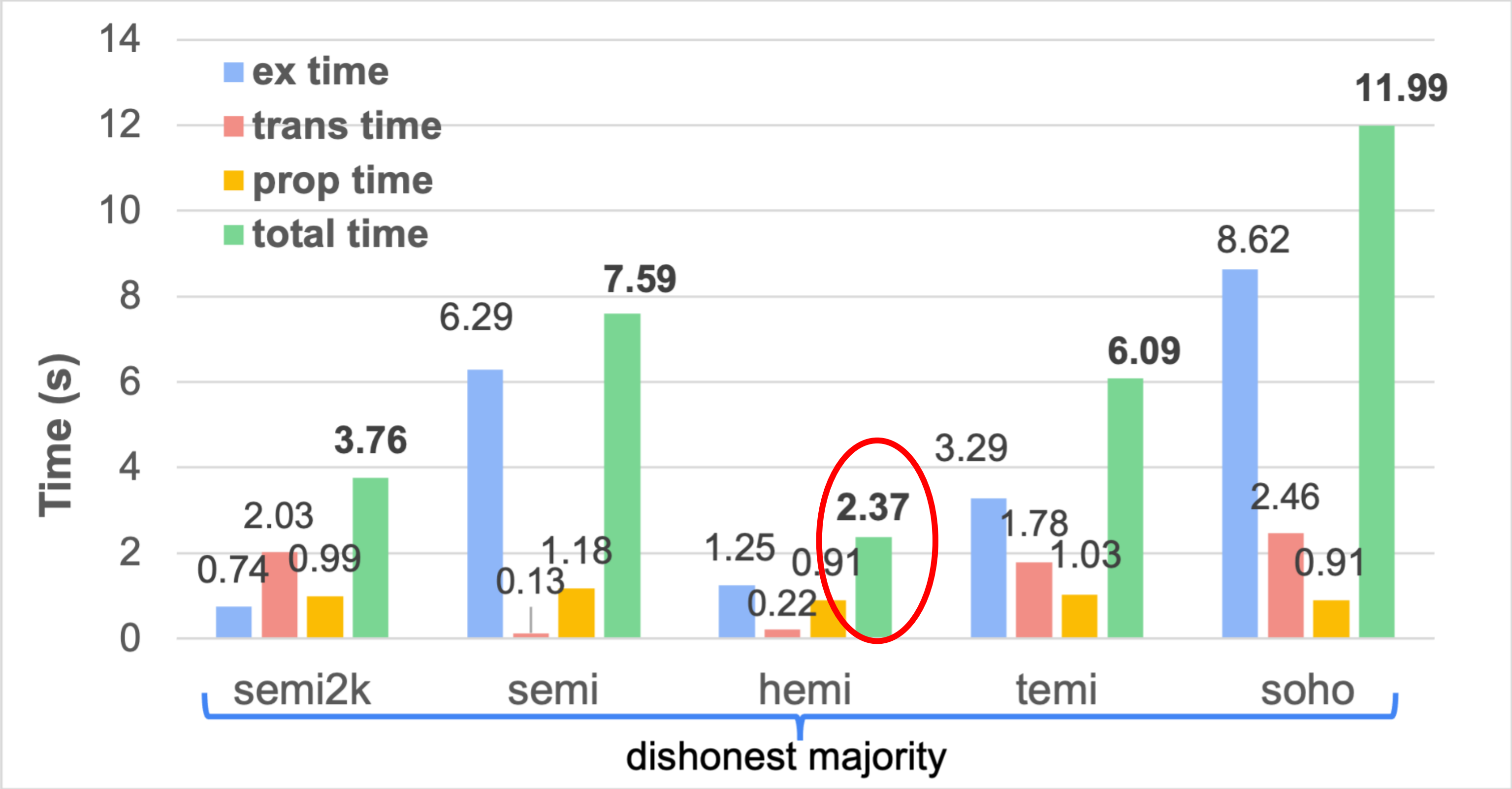
Evaluation: APF Space Factors

Semi-honest model

Semi2k no longer the most efficient

BEST → hemi

Why?
Comm rounds

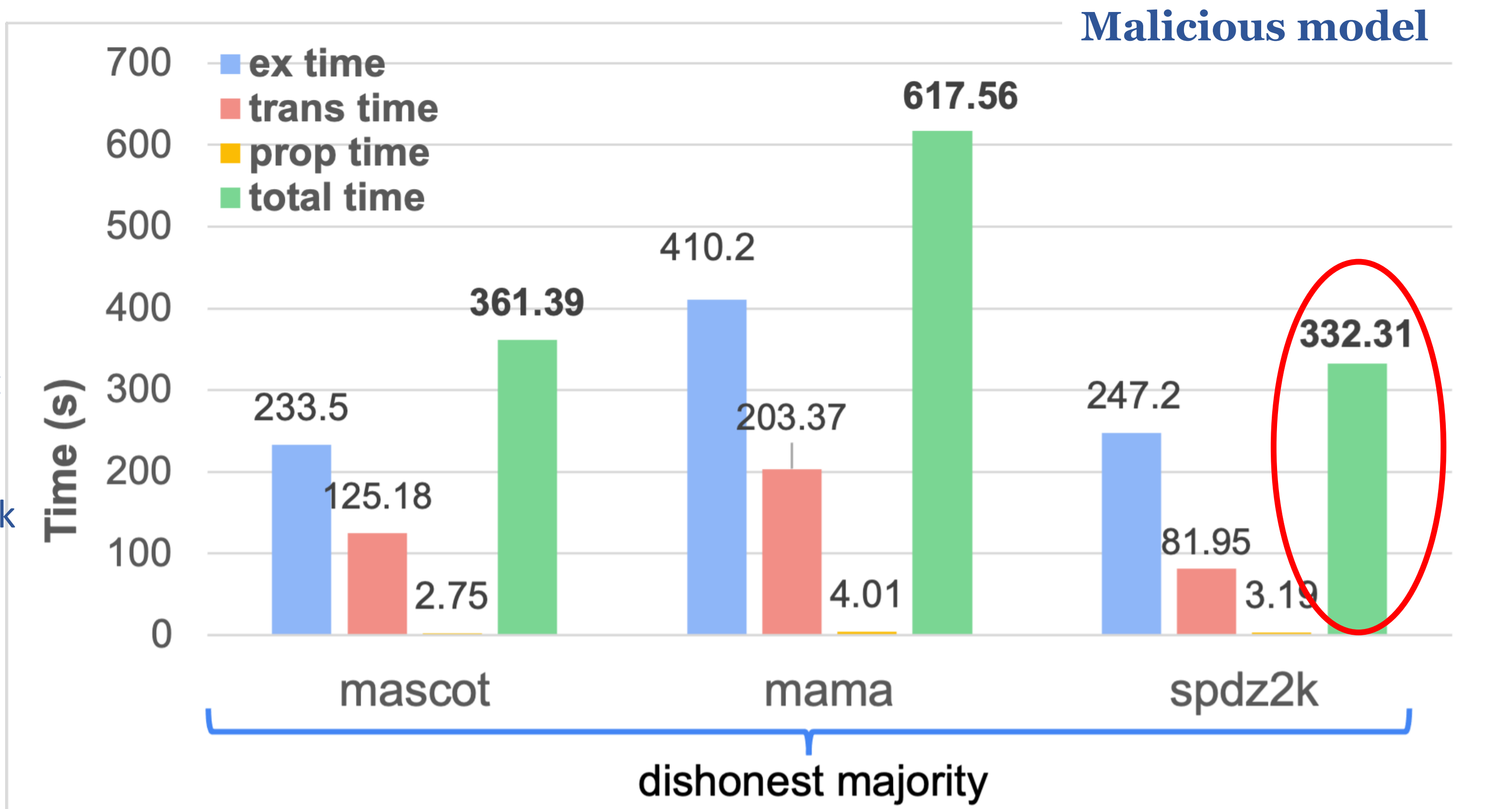


Evaluation: APF Space Factors

Mascot no longer the most efficient

BEST → spdz2k

Why?
Comm rounds

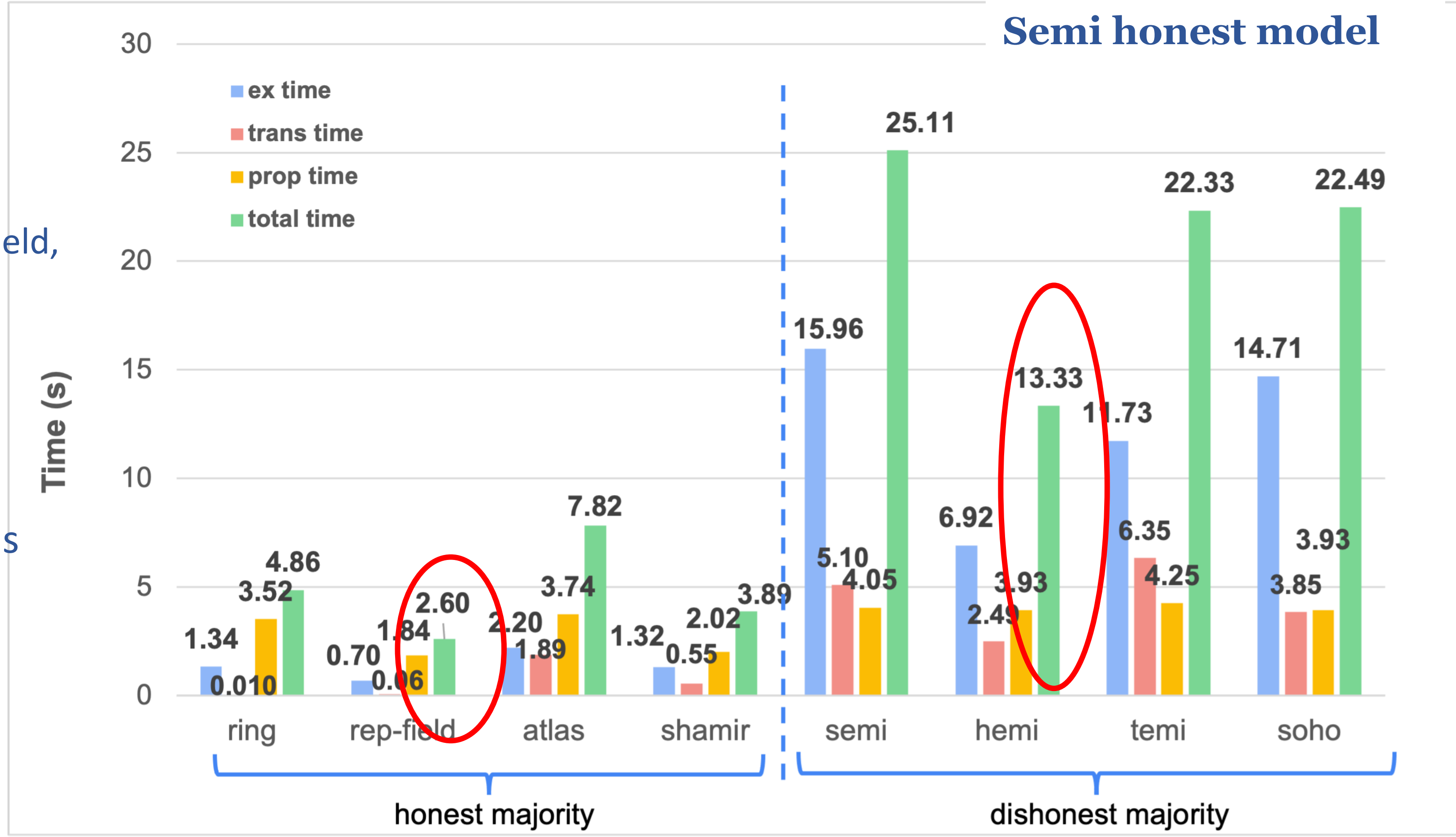


UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ

Evaluation: QP Space Factors

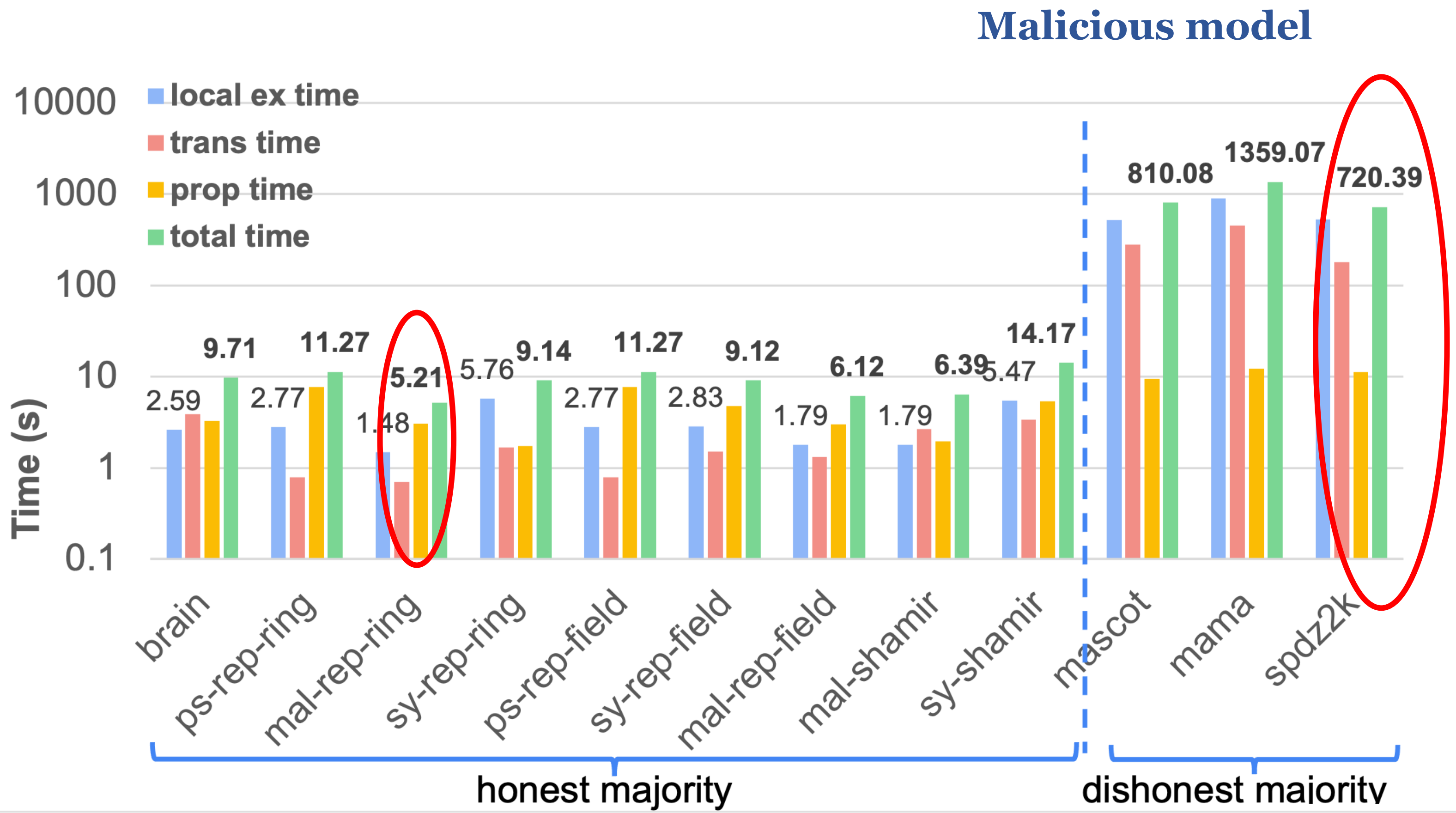
BEST → rep-field, hemi

Also lowest comm rounds



Evaluation: QP Space Factors

BEST → mal-rep-ring, spdz2k



UF UNIVERSITY of FLORIDA
Duke UNIVERSITY
TEXAS The University of Texas at Austin
UC SANTA CRUZ

Conclusion:

- Communication rounds play a large role, but not sufficient themselves (sy-rep ring)

APF Program

Semi-Honest Model, Dishonest Majority	semi	2.05 s
Malicious Model, Dishonest Majority	spdz2k	332 s

Quadratic Program

Semi-Honest Model, Dishonest Majority	hemi	13.3 s
Malicious Model, Dishonest Majority	spdz2k	720 s
Semi-honest Model, Honest Majority	rep-field	2.6 s
Malicious Model, Honest Majority	mal-rep-ring	5.21 s

Takeaway

Conclusion:

- Communication rounds play a large role, but not sufficient themselves (sy-rep ring)
- Malicious, dishonest majority protocols may require further optimization to meet certain mission criteria

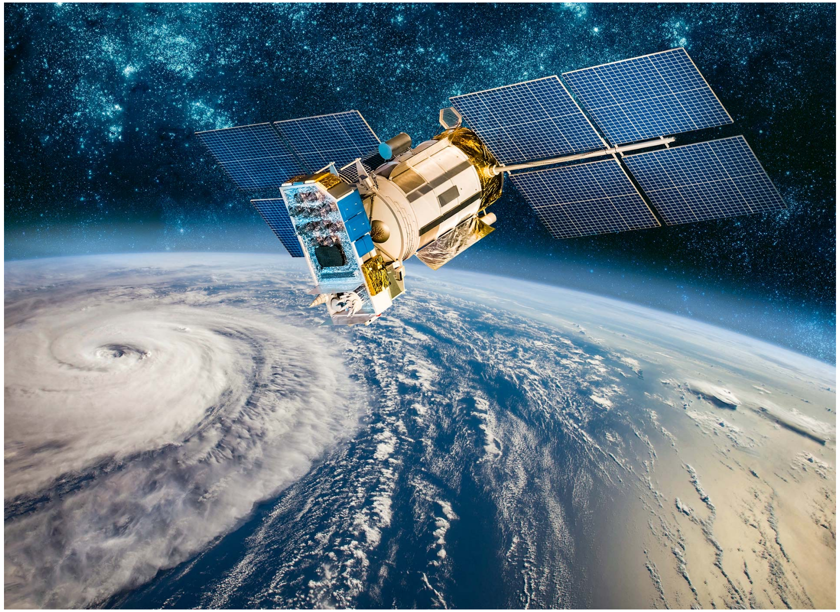
APF Program

Malicious Model, Dishonest Majority	spdz2k	332 s

Quadratic Program

Malicious Model, Dishonest Majority	spdz2k	720 s

Current and Future Work



Source: verdict.co.uk

Current:

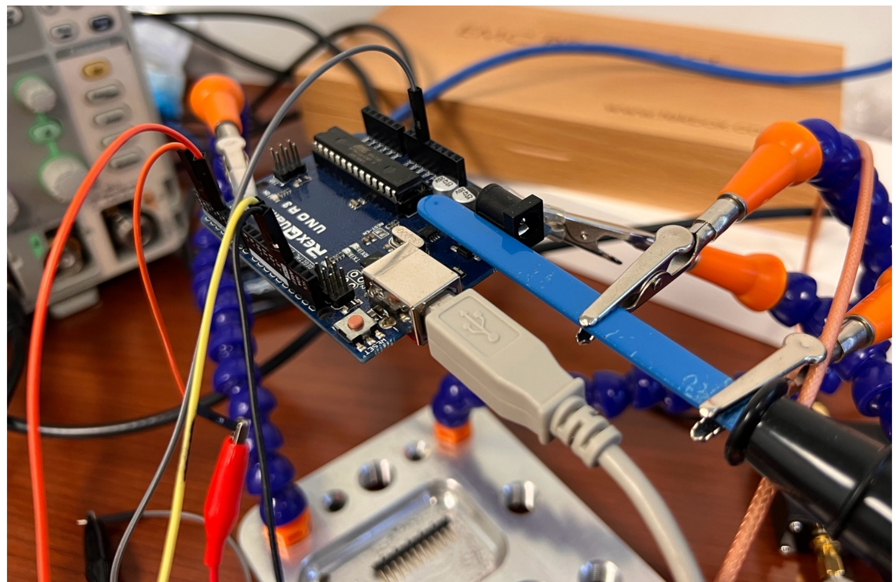
- ACSAC '24 Conference paper – in review

Future Work:

- Evaluate sensor robustness against EMI injection
- Perform an electromagnetic analysis to validate the correct execution of critical operations on on-board MCUs
- Explore other areas for in-space privacy and security applications

Current and Future Work

- EM emissions from microprocessors can be used to validate operations in Microcontrollers such as those used to control actuators for thrusters or reaction wheels



Questions?