Privacy-Preserving Collision-Risk Assessment for LEO Satellites

Svenja Lage, Felicitas Hörmann
Communications and Navigation
German Aerospace Center (DLR)
Oberpfaffenhofen, Germany
{svenja.lage, felicitas.hoermann}@dlr.de

Felix Hanke, Michael Karl
AI Safety and Security
German Aerospace Center (DLR)
Sankt Augstin, Germany
{felix.hanke, michael.karl}@dlr.de

***Abstract*—The growing number of satellites in low Earth orbit (LEO) has increased concerns about the risk of collisions and the resulting space debris. To mitigate this risk, accurate collision risk analysis is essential. However, this requires access to sensitive orbital data, which satellite operators are often unwilling to share due to privacy concerns. This contribution proposes a Fully Homomorphic Encryption-based solution to enable secure and private collision risk analysis. In contrast to existing methods, this framework ensures that collision risk analysis can be performed on sensitive orbital data without revealing it to external parties. In our talk, we provide an in-depth description of the proposed application, derive theoretical requirements and compare them to existing schemes.**

***Index Terms*—Fully homomorphic encryption, satellite collision, multiparty computation**

I. Introduction

The substantial growth in the importance of satellites and their services is evident across various sectors, including governments, military but also private companies, as demonstrated by Starlink, which launched over 6.000 low Earth orbit (LEO) satellites within the past six years [1]. Such large-scale satellite projects have significant implications for the space environment and highly increase the probability of satellite collisions. The European space agency (ESA) underlines the increasing collision risk in their 2024 space environment report [2] as Figure 1 indicates.

Given the high costs associated with satellite production and the need for careful planning of launches, the loss of a satellite due to a collision is detrimental to the operator. Moreover, collisions often generate a large amount of space debris, which causes further collisions and hence poses a threat to other satellites and space missions.

To calculate the collision risk, it is essential to have access to precise orbital data. However, due to privacy concerns, operators are often reluctant to share detailed data, which necessitates the use of less accurate observational data instead. In our talk, we present a solution for this specific application based on Fully Homomorphic Encryption (FHE). This approach enables the computation on encrypted data without revealing any underlying information, a concept originating from Rivest, Adleman and Dertouzos' work in 1978 [3]. The issue remained an open challenge until the groundbreaking work of Gentry in 2009 [4]. Recent advancements have rendered these schemes increasingly efficient, thus bringing real-world applications within reach. In our proposed scenario, operators share their encrypted orbital data, allowing for the collision calculation to be performed without disclosing sensitive information. This approach enables operators to maintain the confidentiality of their data while still benefiting from accurate collision risk assessments.

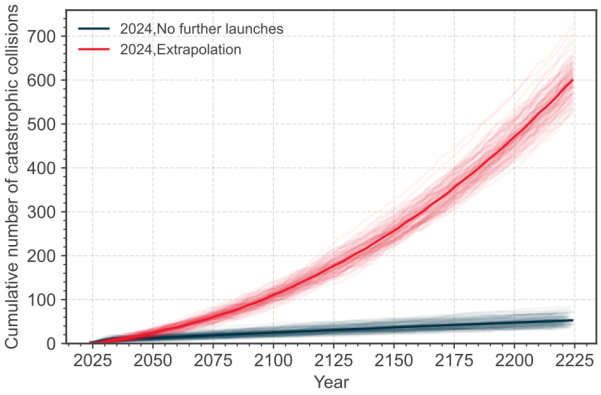

Fig. 1. Cumulative number of catastrophic collisions in the simulated scenarios of long-term evolution of the LEO environment [2].

A variety of application ideas for FHE, such as processing healthcare data, biometrics, or financial data, can be found in the literature (see e.g. [5] or [6]). Despite their potential, these applications are frequently considered under hypothetical conditions that do not accurately reflect real-world complexities, or are described in a manner that is too abstract to be directly applicable. Our proposed scenario is analyzed in detail, with the calculation broken down into individual operations for a suitable FHE scheme. In addition to specifying the type and number of operations, the application also defines the maximum duration of a collision risk analysis, taking into account both the increasing inaccuracy of operator orbit data as one looks further into the future and the need for operators to have a sufficient amount of time to take necessary actions

before a potential collision occurs. After identifying all the necessary requirements, the proposed theory is compared to existing schemes to evaluate their effectiveness and efficiency in addressing this specific application.

II. Background

We will first describe the principles of collision probability calculation based on [7], [8] and [9]. Consider two satellites, denoted by s_1 and s_2. Each satellite is modeled as a three-dimensional spherical object, with radii r_1 and r_2 for s_1 and s_2, respectively. The two satellites collide whenever the two spheres overlap. For a fixed time $t > 0$, let $\mu_1, \mu_2 \in \mathbb{R}^3$ denote the estimated position of the satellites s_1 and s_2 respectively. Due to external forces such as atmospheric influence, even the satellite operators can only estimate the position at a given time t in the future with respect to a certain error. Since the exact structure of the error is unknown, we model the distribution of the real physical location of each satellite by a normal distribution $p_i \sim N(\mu_i, C_i)$ for a given covariance matrix $C_i \in \mathbb{R}^{3\times 3}$ such that the probability density function is given by

$$g_{\mu_i,C_i}(x) = \frac{1}{\sqrt{(2\pi)^3 \det(C_i)}} \cdot \exp\left(-\frac{1}{2}(x-\mu_i)^T C_i^{-1}(x-\mu_i)\right)$$

for $x \in \mathbb{R}^3$ and $i \in \{1, 2\}$.

To simplify the calculation, it is common to attribute all mass towards one of the objects, whereas the second object is considered a point particle with combined positional uncertainty. Although both space objects are interchangeable, we go along with the usual convention and consider satellite s_1 as an object with radius $r = r_1 + r_2$, but no positional uncertainty. Consequently, satellite s_2, which we place in the origin, is considered as a point particle and its position is distributed as $\tilde{p}_2 \sim N(0, C_1 + C_2)$. Note that for simplicity, we have assumed that the positional errors are uncorrelated. However, we acknowledge that certain factors, such as drags, indeed induce correlations between positional errors but as discussed in [10, Section 2.6], these have a negligible impact on the overall analysis.

As the first object is moving through the combined covariance ellipsoid, a collision occurs at time t with a certain probability calculated by

$$P_{collision}(t) = \int_{S_r} g_{0,C_1+C_2}(x)\, dx, \tag{1}$$

where S_r is the sphere of radius r spanned by the satellite s_1 around its relative position at time t. Note that not only S_r but also $C_1 + C_2$ depend on t but we omit this dependency for readability. The probability that the two satellites collide within a given time period $[t_1, t_2]$ is finally given by

$$\int_{t_1}^{t_2} P_{collision}(t)\, dt. \tag{2}$$

Solving this integral using Monte-Carlo simulations requires a large number of samples, resulting in a computationally expensive process (compare [11] or [12]). Although there exist other analytical and numerical approaches to deal with the integral (2) (see [13] for an overview), none of these simultaneously meet the requirements of precision and computational speed in a broad range of scenarios. Hence, in recent research, collision risk analysts often differentiate between two types of scenarios: the short-term encounter scenario, which refers to a situation where the two objects have a high relative velocity and a brief approach (often lasting only a few seconds), and the long-encounter scenario, in which the relative velocity is lower and the encounter duration exceeds a few seconds. Both scenarios exhibit noticeable differences in their behaviour [10] and are thus the focus of separate research efforts.

In what follows, we will focus on the short-term encounter scenario, which is frequently applied to LEO encounters due to the high velocities of the objects involved. In this particular scenario, the encounter time is small such that, within this period, the normally curved motion of the objects can be approximated with a linear motion with a relatively small error margin. Furthermore, we can assume that the collision probability $P_{collision}$ is constant over the short encounter period which simplifies (2) to the three-dimensional case in (1). To preclude underestimation of the collision probability, the parameters are fixed at the time of closest approach (TCA).

To further simplify the calculation, we define a coordinate system with respect to the encounter plane. Therefore, let the y'-axis be along the relative velocity vector $v = v_1 - v_2$ and choose the (x', z')-plane – the so-called encounter plane – normal to v. By doing so, the distance between the two satellites is purely based on their distance in the (x', z')-plane such that the collision probability can similarly be described via the projections of the objects onto the encounter plane (compare Figure 2). As a result,

$$\begin{aligned} P_{collision} &\approx \int_{B_r} \frac{1}{2\pi\sigma_{x'}\sigma_{z'}} e^{-\frac{1}{2}\left[\left(\frac{x'}{\sigma_{x'}}\right)^2 + \left(\frac{z'}{\sigma_{z'}}\right)^2\right]}\, dx'\, dz' \\ &=: \int_{B_r} p(x', z')\, dx'\, dz', \end{aligned} \tag{3}$$

where for simplicity we assume that the x'- and z'-axes are chosen such that the covariance matrix is diagonal with elements $\sigma_{x'}^2$ and $\sigma_{z'}^2$ and B_r denotes the cross section of the two-dimensional projection in the encounter plane. In 1992, Foster and Estes expressed this integral in polar coordinates and utilized it to approximate satellite collision risks [14]. Since this model is still in use by the NASA [15] as well as by the German Aerospace Center [8], our model will be primarily based on this calculation although other approximations exist and may stimulate further research.

It is well-known that no closed-form expression exists for the solution of the integral (3) and hence, it must be solved using numerical integration. Therefore, a grid $\{(x_i', z_j') : i = 1, \ldots, N_1, j = 1, \ldots, N_2\}$ with $N_1, N_2 \in \mathbb{N}$ over the two-

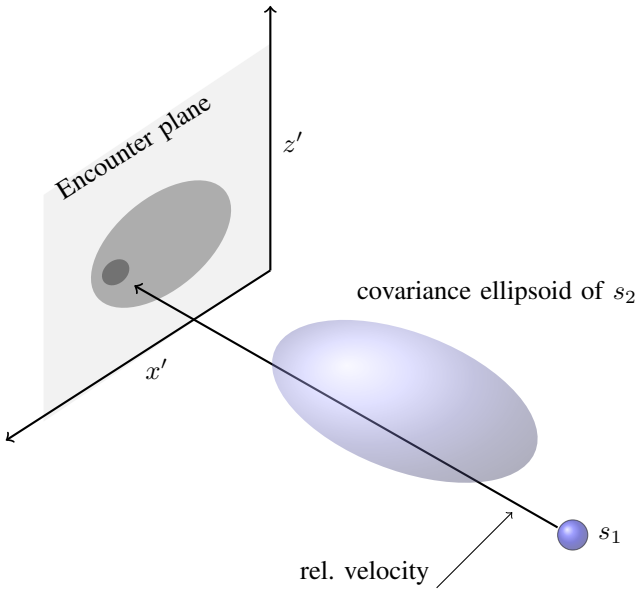

Fig. 2. Representation of satellite s_1 as sphere with combined radius $r = r_1 + r_2$ and satellite s_2 as point particle with combined covariance matrix. Additionally, the encounter plane normal to the relative velocity as well the projection of s_1 and s_2 onto the plane are displayed. Inspired by [9].

dimensional cross section B_r in (3) is defined and the integral is approximated by

$$P_{collision} \approx \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \omega_{i,j} p(x'_i, z'_j) \tag{4}$$

with suitable weights $(\omega_{i,j})_{i=1,\dots,N_1, j=1,\dots,N_2}$. From this formula we explicitly obtain the kind and number of operations needed for the whole calculation. In our talk we display the results not only for the high-order Gaussian quadrature rule used by the NASA [15] but also for other integration rules.

In certain scenarios, it may be advantageous to assume a constant probability function p within the region of integration, thereby simplifying the integral (3) to a straightforward evaluation of p without the necessity of numerical integration. However, as Aida et al. [8] have noted, this approximation introduces a non-negligible error when r is large and the combined covariance is small.

III. Current Status and Challenges

The collision risk analysis relies on accurate knowledge of the satellites' movement, necessitating the forecast of parameters μ_i, C_i, and r_i for $i \in \{1, 2\}$ across the time period of interest. While the satellite radius is typically not a sensitive parameter, due to privacy concerns (especially in the military setting) operators often hesitate to share precise trajectory data. In practice, orbit prediction is based on tracking data provided by organizations such as the 19th Space Defense Squadron (19th SDS), operated by the United States Space Force. The SDS collects tracking data for over 40.000 objects with a radius exceeding 10 cm and conducts an initial collision analysis [16]. Operators receive automatic collision warnings three times per day. However, as operators possess additional information about their satellites orbit and planned maneuvers, they reperform the analysis with more precise data for their satellites. Note that in practice, the approach outlined in Section II is not employed in isolation; rather, multiple methodologies are applied concurrently to provide a more comprehensive understanding of the data (compare [17]).

Nevertheless, the calculation of the second object's trajectory relies on observational data, which poses an ongoing challenge. Various approaches have been developed based on underlying assumptions (e.g., [18] and [19]). Despite progress in this research area, prediction accuracy is compromised by approximation errors and, most significantly, the lack of maneuver knowledge. Access to operator-provided data for predicting satellite movement would eliminate this error source, enhancing the accuracy of collision risk analysis.

IV. FHE in Satellite Collision Analysis

We now sketch how FHE can be useful in the above described use case under the assumption that the trajectory data of the involved satellites is sensitive. For simplicity, we focus on the case in which two distinct operators use a common server to compute the probability that two of their satellites collide. Hence we deal with a multiparty scenario with two parties in which both parties aim to maintain the confidentiality of their respective data.

Generally, such a scenario can be managed through either multikey FHE or threshold FHE. Within the framework of multikey FHE schemes (e.g. see [20], [21], and [22]), each party independently generates its own key, which may take the form of a secret key in symmetric-key settings or a key pair comprising a public key and a secret key in asymmetric-key settings. As a result, each operator encrypts its own data using its unique key and transmits it to a curious-but-honest server. However, as the server receives data encrypted with different keys, the computational overhead increases in proportion to the number of participants [23]. The decryption process is performed collectively by all participants.

Conversely, in the context of threshold FHE (compare for example [24], [25]), the parties engage in a collaborative process to generate a single key pair. While the public key is shared among all parties, the private key remains secret, with each party possessing only a share of it. This ensures that no single party has the capability to decrypt any data independently. Each party can encrypt its own data using the shared public key and transmit it to the curious-but-honest server. As only one single key is utilized for encryption, the server-side computational cost is comparable to that of a single-party scenario, thereby mitigating the computational costs associated with multiparty computation. Decryption, as before, is a collective process, requiring the participation

of $t + 1 \leq n$ parties, where the threshold t is a scheme parameter.
Given the involvement of only two parties, the computational overhead of multikey schemes remains sufficiently manageable when compared to threshold FHE with $t = 1 = n - 1$ (the so-called full threshold case). This feasibility allows each approach to present distinct merits, motivating our decision to examine both methodologies in detail.

Note that extending the two-party scenario to the more general case of n parties would necessitate that all parties, and not only the two operators of the considered two satellites, remain reachable throughout the entire duration, given that we are operating in the full threshold regime. This dependency introduces a potential vulnerability to the system and poses undesirable challenges in terms of risk management. Consequently, it is advantageous to adopt a pairwise approach, where the n-party system is decomposed into multiple pairs of two-party interactions. It is worth noting that multikey FHE allows for an easy integration of new parties because it only requires the new party to generate a key while the rest of the setup remains unchanged. In contrast, threshold FHE requires the regeneration of all key shares associated with the new party.

In our concrete scenario, we now assume that the operators receive a collision warning predicated on observational data (e.g. by 19th SDS) and want to verify this warning utilizing both their precise orbital knowledge without revealing it to each other. It is worth noting that we assume a preliminary filtering and analysis of publicly available data has been conducted, thereby obviating the need for unnecessary and computationally expensive calculations or an homomorphic filtering. While an intriguing extension of this work could involve integrating this filtering process within the homomorphic framework, such an exploration lies beyond the scope of the present discussion.
Both operators encrypt their respective orbital data, either utilizing their individual keys in the multikey scenario or the shared public key in the threshold scenario. The server then executes the probability calculation on the encrypted data as outlined in Section II, yielding the encrypted collision probability. This encrypted result is then collectively decrypted by both parties, thereby enabling them to access the actual collision probability and jointly determine the requisite course of action.
The quantity of data requiring encryption and processing is highly dependent upon the temporal distance between the current time and the approximate time of closest approach (TCA) obtained from the warning. When TCA is imminent, it can be reasonably assumed that the orbital data up to a point near the closest approach is relatively accurate, thereby necessitating only a verification of the data points surrounding that time. Conversely, if TCA is distant, the orbital trajectory may undergo significant changes prior to that point, rendering it essential to recalculate TCA and necessitating the processing of a substantially larger dataset.

Apart from the mathematical requirements on the FHE scheme, temporal constraints also apply. Since an operator requires a certain amount of time to initiate an evasion maneuver, all calculations must be completed 24 hours before a possible collision occurs. Furthermore, the operators steadily reappraise the situation which, due to frequent maneuvers, changes continuously. This poses an enormous restriction to the FHE scheme, as speed remains the most challenging research topic within current FHE schemes.

In our talk, we will undertake a comprehensive examination of the above scenarios, utilizing concrete numerical values to illustrate the theoretical requirements that arise from each. A comparative analysis will be conducted to juxtapose these theoretical requirements with the capabilities of existing multikey and threshold FHE schemes. Our investigation will reveal that presently, no scheme fully satisfies all of these requirements, thereby highlighting the disparities between theoretical necessities and practical implementations. These gaps will serve as a motivation for further research, underscoring the need for continued exploration and development in this area.

V. Summary

We presented the problem of assessing the collision risk of LEO satellites when the exact trajectories or planned maneuvers of the involved objects are not publicly available. As operators consider these data highly sensitive for certain missions, current state-of-the-art systems compute collision probabilities with the exact data of the owned satellite but only with estimates from ground-based observations of the second satellite.

We see a considerable potential in using FHE techniques in this scenario because they allow to use exact trajectory data for both involved satellites while still ensuring the privacy of the sensitive information. By enabling secure, encrypted computations, FHE methods could significantly enhance the precision and reliability of collision risk assessments. Furthermore, these techniques could pave the way for greater cooperation among satellite operators without compromising their competitive or security interests.

Thus, we hope that the presentation fosters the interest and discussion of the community, particularly regarding the practical implementation and optimization of FHE in real-time orbital analysis.

References

[1] satellitemap.space, accessed November 22, 2024. [Online]. Available: https://satellitemap.space

[2] ESA Space Debris Office, "ESA's annual space environment report," European Space Agency, Tech. Rep. GEN-DB-LOG-00288-OPS-SD, July 2024. [Online]. Available: https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf

[3] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," in *Foundations of Secure Computation*, R. A. DeMillo, R. J. Lipton, D. P. Dobkin, and A. K. Jones, Eds. USA: Academic Press, 1978, pp. 169–177.

[4] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, Stanford, CA, USA, 2009.

[5] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, ser. CCSW '11. New York, NY, USA: Association for Computing Machinery, 2011, pp. 113—124.

[6] A. Shahriar, T. Yang, S. Shahed, A. Mazroa, A. Attiah, and L. Mohaisen, "A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions," *Computers, Materials & Continua*, vol. 78, pp. 2087–2110, February 2024.

[7] F. Chan, *Spacecraft Collision Probability*. El Segundo, CA, USA: Aerospace Press, 2008.

[8] S. Aida, "Conjunction risk assessment and avoidance maneuver planning tools." Presented at the 6th International Conference on Astrodynamics Tools and Techniques, March 14 - 17 2016.

[9] M. Navabi and R. Hamrah, "Close approach analysis of space objects and estimation of satellite-debris collision probability," *Aircraft Engineering and Aerospace Technology: An International Journal*, vol. 87, September 2015.

[10] Y. Wen, Z. Yu, L. He, Q. Wang, and X. He, "Collision probability prediction and orbit maneuvering probability determination of non-cooperative space object orbit," *Remote Sensing*, vol. 12, no. 20, p. 3310, 2020.

[11] M. Losacco, M. Romano, P. Di Lizia, C. Colombo, R. Armellin, A. Morselli, and J. Pérez, "Advanced monte carlo sampling techniques for orbital conjunctions analysis and near earth objects impact probability computation," in *Proceedings of the 1st NEO and Debris Detection Conference*, T. Flohrer, R. Jehn, and F. Schmitz, Eds., vol. 1. ESA Space Safety Programme Office, March 2019.

[12] S. Alfano, "Satellite conjunction monte carlo analysis," *Advances in the Astronautical Sciences*, vol. 134, pp. 2007–2024, January 2009.

[13] J.-S. Li, Z. Yang, and Y.-Z. Luo, "A review of space-object collision probability computation methods," *Astrodynamics*, vol. 6, no. 2, pp. 95–120, April 2022.

[14] J. L. Foster and H. S. Estes, "A parametric analysis of orbital debris collision probability and maneuver rate for space vehicles," National Aeronautics and Space Administration, Lyndon B. Johnson Space Center, Tech. Rep. JSC-25898, August 1992. [Online]. Available: https://purl.stanford.edu/dg552pb6632

[15] F. J. Krage, "NASA spacecraft conjunction assessment and collision avoidance best practices handbook," National Aeronautics and Space Administration, Washington, DC, USA, Tech. Rep. NASA/SP-20230002470 Rev 1, February 2023.

[16] Space Force, accessed November 22, 2024. [Online]. Available: https://www.petersonschriever.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/1060278/19th-space-defense-squadron

[17] S. Aida and M. Kirschner, "Collision risk assessment and operational experiences for LEO satellites at GSOC." Presented at the 22nd International Symposium on Space Flight Dynamics (ISSFD), February 28 - March 4 2011.

[18] T. Paulet and B. Cazabonne, "An open-source solution for TLE-based orbit determination," in *Proceedings of the 8th European Conference on Space Debris*, April 2021.

[19] M. Thammawichai and T. Luangwilai, "Data-driven satellite orbit prediction using two-line elements," *Astronomy and Computing*, vol. 46, p. 100782, 2024.

[20] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, May 2012.

[21] ——, "Multikey fully homomorphic encryption and applications," *SIAM Journal on Computing*, vol. 46, no. 6, pp. 1827–1892, 2017.

[22] M. Clear and C. McGoldrick, "Multi-identity and multi-key leveled FHE from learning with errors," in *Advances in Cryptology – CRYPTO 2015*, R. Gennaro and M. Robshaw, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 630–656.

[23] H. Chen, W. Dai, M. Kim, and Y. Song, "Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 395—412.

[24] G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs, "Multiparty computation with low communication, computation and interaction via threshold FHE," in *Advances in Cryptology – EUROCRYPT 2012*, D. Pointcheval and T. Johansson, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 483–501.

[25] K. Boudgoust and P. Scholl, "Simple threshold (fully homomorphic) encryption from LWE with polynomial modulus," in *Advances in Cryptology – ASIACRYPT 2023*, J. Guo and R. Steinfeld, Eds. Singapore: Springer Nature Singapore, 2023, pp. 371–404.