

# CSUM: A Novel Mechanism for Updating CubeSat while Preserving Authenticity and Integrity

Ankit Gangwal, Aashish Paliwal\*

International Institute of Information Technology Hyderabad, India  
gangwal@iiit.ac.in, aashish.paliwal@research.iiit.ac.in

**Abstract**—The recent rise of CubeSat has revolutionized global space explorations, as it offers cost-effective solutions for low-orbit space applications (including climate monitoring, weather measurements, communications, and earth observation). A salient feature of CubeSat is that applications currently on-boarded can either be updated or entirely replaced by new applications via software updates, which allows reusing in-orbit hardware, reduces space debris, and saves cost as well as time. Securing software updates employing traditional methods (e.g., encryption) remains impractical mainly due to the low-resource capabilities of CubeSat. Therefore, the security of software updates for CubeSats remains a critical issue.

In this paper, we propose CubeSat Update Mechanism (CSUM), a lightweight scheme to provide integrity, authentication, and data freshness guarantees for software update broadcasts to CubeSats using a hash chain. We empirically evaluate our proof of concept implementation to demonstrate the feasibility and effectiveness of our approach. CSUM can validate 50,000 consecutive updates successfully in less than a second. We also perform a comparative analysis of different cryptographic primitives. Our empirical evaluations show that the hash-based approach is at least  $61\times$  faster than the conventional mechanisms, even in resource-constrained environments.

**Index Terms**—Authentication, CubeSat, Data Freshness, Integrity, Secure Software Update.

## I. INTRODUCTION

Space exploration and deployment of satellites have become an indispensable part of modern science. These satellites serve various purposes, including navigation [1], weather forecast [2], and data collection [3]. In the past few years, CubeSat (CS) - a novel type of miniature satellite - has attracted significant interest from researchers in academia as well as industry [4]. Each CS unit measures  $10 \times 10 \times 10$  cubic centimeters ( $10 \text{ cm}^3$ ). The rise of CS has significantly reduced the cost associated with satellite deployment, consequently democratizing the field. In particular, the reduction in satellite deployment cost has enabled small to mid-sized companies, universities, research institutes, and even developing nations [5] to participate in space expeditions.

While CS provides a cost-effective means for entering the satellite playground, it also introduces a new array of challenges that do not apply to traditional satellites. The fundamental reason for such unprecedented challenges is the limited availability of resources (including computing power, memory, and communication bandwidth) in CS. One such challenge within resource-constrained environments is the

software update process [6], and CSs are no different. In fact, it is even more crucial to secure the software update process for CSs as they are mission-critical, where even a minute error can lead to mission failure or the complete loss of a satellite. Furthermore, it is essential for CS's software to be modular and reusable [7].

Malicious software updates can lead to unauthorized control, data manipulation, and communication interference, which can lead to severe consequences (e.g., increased risk for mission failure, lack of data integrity, even complete loss of control over CS). Moreover, unauthorized access to a satellite poses a significant risk not just to its owners, but to the broader space environment as well. As a representative example, an attacker taking control of a satellite and activating its thrusters could lead to the Kessler Syndrome [8]. Kessler Syndrome is a scenario where debris from one satellite collision spreads and hits other satellites, creating more debris in a domino effect. Such a chain reaction could potentially block access to space for decades, as observed in different simulations [9, 10]. CS commonly utilizes amateur radio frequencies for communication (i.e., UHF/VHF [11]), resulting in relatively low data rates (typically ranging from 9.6 Kbps to 100 Kbps). For instance, the daily throughput of ThingSat [12] is approximately 1500 KB [11]. Furthermore, utilizing standard cryptographic schemes to handle malicious updates is impractical since cryptographic operations tend to be expensive in terms of computational resources; making them unsuitable for CS's resource-constrained environment.

The on-board software is one of the most critical components of any space mission. It encompasses the core capabilities of the space system, ranging from daily activities within the system (like navigation, communication, and energy management) to more specialized tasks (like data collection and processing). The effectiveness of a space system relies heavily on the correct functioning of on-board hardware and software. Post-launch, satellites may face unexpected events and operating conditions. While some issues can be mitigated via exception handling (if anticipated during initial software development), others may be fixed through software updates.

Over-the-Air (OTA) updates have overwhelmingly affected various user-centric domains, e.g., smartphones, smart TVs, automobiles, and IoT devices. OTA enables manufacturers to deliver software updates remotely, eliminating the need for physical access to a device. For the end users, OTA updates offer a convenient way to receive the latest functionality without

\*Corresponding author

visiting the service center. For manufacturers, it provides a way to improve their products' value by delivering new features, bug fixes, and security patches on time. The importance of OTA updates extends beyond convenience. OTA updates are critical for the lifecycle management of modern devices to ensure they remain efficient, secure, and up-to-date with minor user intervention.

Nilchiani [13] argues that the capability of remote modification and enhancement of on-board software is crucial for space systems due to the uncertain nature of space. This capability can help preserve system functionality, adapt to emerging requirements, or improve performance without needing physical upgrades (which are often impossible after launch). In-orbit software updates are now standard practice for small satellites [14]. Even nano-satellites (e.g., PlanetLabs Dove nanosatellite constellation [15]) acknowledge support for in-orbit firmware updates without disclosing the details.

In this paper, we introduce CSUM, a lightweight scheme designed to enhance the security of software updates in CS. CSUM is designed to take into account the constrained hardware capabilities of CS and the limited communication bandwidth between Ground Station (GS) and CS. It aims to preserve software updates' integrity, authenticity, and freshness, thereby safeguarding CS from adversaries attempting to tamper with in-transmission software updates. Our approach advocates for using lightweight hash functions because a single public-key computation is roughly equivalent to hundreds of hash computations in processing time [16].

The major contributions of our paper are as follows:

- 1) We propose CSUM, a novel and lightweight scheme that utilizes hash chains to ensure authentication, integrity, and freshness for CS software update broadcasts.
- 2) We validate the effectiveness of CSUM via empirical evaluations of its proof of concept implementation. Our results show that CSUM can validate 50,000 consecutive updates in just 0.81 seconds.
- 3) Furthermore, we perform a comparative analysis of different cryptographic primitives. Our analyses show that the hash-based approach outperforms the traditional mechanisms even in resource-constrained environments. In particular, encryption, decryption, signing, and signature verification operations are over 155, 126, 64, and 61 times slower than the hash-based approach, respectively.

*Organization:* Section II provides an overview of the related research works and background knowledge. We discuss our system and adversary model along with security requirements in Section III, elaborate CSUM in Section IV, and discuss our results in Section V. Finally, Section VI concludes the paper and highlights the possible future research directions.

## II. RELATED WORKS

The security of space-based assets (like CS) has not been extensively researched as their terrestrial counterparts (like connected vehicles), especially concerning OTA software updates. Recently, researchers have been looking into CS security, focusing on the unique challenges posed by the limited

resources available on such platforms. Halder et al. [17] underlines the significance of OTA updates and categorizes existing OTA update techniques for connected vehicles. Various secure update techniques for connected vehicles have been developed to address integrity, authenticity, and confidentiality. These techniques include Uptane [18], a secure software repository framework that enhances compromise resilience by distributing responsibilities across distinct roles. Blockchain-based schemes [19] eliminate cloud involvement and utilize smart contracts to ensure update integrity and authenticity, while hash function-based protocols [20] safeguard the transmission integrity of software updates. Frameworks, such as SecUp [21], utilize a combination of symmetric and asymmetric key cryptography to ensure secure and efficient OTA updates. Moreover, hardware-based solutions leveraging Hardware Security Modules (HSM) [22] and Trusted Platform Modules (TPM) [23] provide robust security at hardware-level.

Souza et al. [24] emphasize the difficulties in implementing secure software updates due to these resource constraints, proposing a multi-layered mission software approach for CS. Similarly, Bellissimo et al. [6] highlights the challenges in securing software updates in deployed systems, complexities in safeguarding against known attacks, and the challenges of applying secure content distribution methods in resource-limited devices. Willbold et al. [25] offers a comprehensive threat taxonomy against satellite firmware, including an analysis of real-world satellite firmware security issues and a survey among professional satellite developers to shed light on the satellite security landscape.

The authors in [11, 26, 27] discuss different firmware update mechanisms for an in-orbit CS. Sünter et al. [27] explore firmware updating systems for nano-satellites using the ESTCube-1 mission [28] to compare four distinct update procedures, highlighting their implementation complexities and error recovery mechanisms for in-orbit satellite software management. Fitzsimmons [26] improves CS robustness through a software update mechanism, focusing on update usability, validation, and system recovery to extend mission capabilities and safeguard against operational anomalies. The author utilizes MD5 for integrity, but the scheme does not address authentication. Bezem and Fjellby [29] tackle the absence of inherent security features in satellite communications by enhancing the CS Space Protocol with HMAC and sequence numbers to prevent replay attacks. However, apart from focusing exclusively on replay attacks, the scheme also requires secure infrastructure, which is comparatively costly. Molina et al. [11] addresses secure software updates for multi-tenant CS through Cubedate, a framework designed for continuous software deployment to orbiting CS. Despite its innovative approach, the framework relies on digital signatures and encryption, raising concerns about computational feasibility in the constrained environment, alongside its dependence on a single trust anchor. Challa et al. [30] proposed CubeSec and GndSec, lightweight security solutions for CS communications, acknowledging the need for efficient security measures in resource-constrained environments. However, the

security of their approach relies heavily on pre-shared keys as they utilize symmetric encryption.

In traditional pre-shared key systems, all security properties are lost once the key (or trust anchor) is compromised. In our approach, even if a CS is compromised, adversaries can only validate tokens and read the next one when it comes; they cannot create the next key due to the pre-image resistance of cryptographic hash functions. This significantly limits the damage an adversary can do as long as they can only read the trust anchor and not replace it.

To summarize, using standard cryptographic primitives (i.e., encryption in CubeSec [30], CubeDate [11], and GndSec [30] as well as digital signatures in CubeDate [11] and NUTS [29]) make state-of-the-art CS security solutions computationally expensive. **CSUM overcomes computational overheads by limiting the use of public-key operations to just one instance (i.e., to create a one-time trust anchor) and utilizing lightweight hash function in subsequent operations.**

*Hash chain:* Hash chain utilizes a cryptographic hash function to create a linked chain of hashes. A hash chain is constructed by recursively applying a cryptographic hash function to a randomly generated seed as shown in Fig. 1. Hash chains inherently inherit the properties of cryptographic hash functions while also exhibiting their own unique characteristics due to their iterative structure.

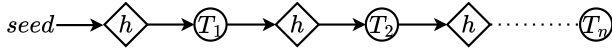


Fig. 1. Representation of a hash chain starting from seed to  $T_n$ .

### III. SYSTEM ARCHITECTURE AND THREAT MODEL

In this section, we outline the system model (cf. Section III-A), describe the adversary model for CSUM (cf. Section III-B), and specified the security requirements for CS (cf. Section. III-C).

#### A. System model

CSUM focuses on ensuring the secure delivery of Software Update Package (*SUP*) from GS to CS while considering the inherent vulnerabilities of the communication systems linking them. Our system model comprises three primary entities: administrator, GS, and CS. The administrator plays a pivotal role in the initial setup by generating a seed to create a hash chain, which acts as a trust anchor and lays the foundation for secure communication. The administrator is also responsible for creating *SUP*s and corresponding Transmission Token (*TT*), which are essential for authorizing updates. GS is responsible for transmitting *SUP*s and its corresponding *TT*s received from the administrator to CS. CS is tasked with the reception and verification of *SUP* and their accompanying *TT*s, ensuring the security of the deployment process. CS is equipped to perform critical cryptographic operations despite its limited resources.

The communication link between GS and CS is inherently insecure but reliable and susceptible to threats such

as replay attacks, message alteration, and injection. Despite these challenges, both the administrator and CS are considered secure entities with secure internal storage capabilities to resist direct attacks. Operating within a constrained environment, CS must efficiently manage its limited bandwidth, processing capabilities, and storage, highlighting the need for streamlined and lightweight security solutions. A reliable transfer protocol, like Saratoga protocol [31], can mitigate issues related to packet losses and propagation delay. Our proposed scheme is agnostic to transport mechanisms as long as we transmit both *SUP* and the corresponding *TT*.

Fig. 2 illustrates a communication system where the administrator interacts with the Ground Station over the Internet, with the potential for both secure and insecure data transmission. However, the communication between the Ground Station and the CS is insecure.

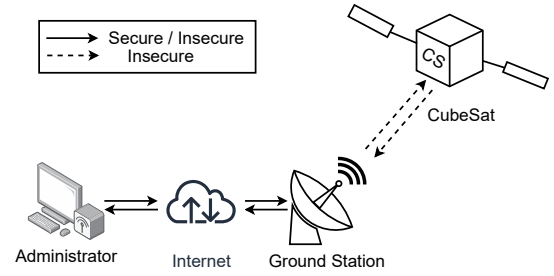


Fig. 2. A simplified communication architecture of CS.

#### B. Adversary model

Our adversary model considers a highly capable adversary with computational resources surpassing those typically available in a CS environment. The adversary operates within Probabilistic Polynomial Time (PPT) and targets vulnerabilities primarily within the communication framework connecting GS and CS. We assume that the trusted components in the overall CS infrastructure, including the administrator, CS, and GS, remain secure throughout the system's operational life.

The adversary possesses a diverse array of attack capabilities to compromise software updates between GS and CS. These capabilities include passive eavesdropping on the communication channel, active interception and data manipulation to facilitate Man-in-the-Middle attacks, executing replay attacks by re-transmitting legitimate *SUP*, injecting malicious *SUP*, and overwhelming CS (and its verification capacity) by flooding CS with fake *SUP* and *TT*.

The adversary's objectives include disrupting genuine communication, deceiving CS into accepting malicious *SUP*s, extracting sensitive information from transmitted messages, and wasting CS resources. Despite these capabilities, the adversary is bound by PPT, which restricts its ability to break strong cryptographic systems within a reasonable time frame. Additionally, the adversary is incapable of altering the initially trusted data placed in a CS (e.g., trust anchor).

### C. Security goals

The primary objective of CSUM is to secure the transmission of *SUPs* from GS to CS against threats on insecure channels. We aim to achieve the following security goals [32]:

- 1) *Authentication*: To ensure that *SUPs* originate from a verified source, CSUM incorporates the use of authentication tokens. This mechanism ensures that only authorized entities can initiate software updates.
- 2) *Integrity*: CSUM is designed to detect any unauthorized modifications in *SUPs* received by CS. Thereby safeguarding the integrity of the transmitted data.
- 3) *Data freshness*: It is crucial that CS receives the most recent *SUP*. CSUM mitigates the risk of replayed attacks by adversaries, ensuring that only the latest valid *SUP* are installed.

## IV. PROPOSED SCHEME - CSUM

CS is designed to operate under limited resources, e.g., extremely low bandwidth, constrained memory, and minimal processing power. Formulating effective security strategies within these constraints is non-trivial and presents a significant challenge. These constraints force us to move away from traditional cryptographic mechanisms that are robust but resource-intensive. Thus, such mechanisms are impractical for low-resource environments, like CS. In contrast, cryptographic hash functions emerge as a better solution due to their significantly lower computational overheads [16]. CSUM utilizes a lightweight hash function to ensure the authentication and integrity of *SUPs* sent from GS to CS.

CSUM aims to minimize reliance on resource-intensive public-key operations and replace them with efficient hash operations instead. This approach holds significant advantages for CS due to the lightweight nature of hash functions compared to encryption and signature schemes. The proposed scheme aims to achieve authentication, integrity, and freshness with constant network overhead (i.e., output length of a single hash function). Now we elucidate different phases (cf. Section IV-A) and operations (cf. Section IV-B) in CSUM.

### A. Phases

CSUM involves setup, key encapsulation, and authentication and integrity phases. We utilize several symbols as defined in TABLE I while explaining CSUM.

TABLE I  
SYMBOL DEFINITIONS.

| Symbol      | Description                            |
|-------------|----------------------------------------|
| $TA$        | Trust Anchor                           |
| $TT$        | Transmission Token                     |
| $DT$        | Derived Token (from transmission)      |
| $PT$        | Partial Token                          |
| $AT$        | Authentication Token                   |
| $AT_{curr}$ | Current Authentication Token           |
| $AT_{prev}$ | Previous Authentication Token          |
| $h(x)$      | Hash function applied on $x$           |
| $h^n(x)$    | Hash function applied on $x$ $n$ times |

1) *Setup phase*: The setup phase initializes the system, where the administrator employs a hardware random number generator [33] to produce a random seed. The generated seed undergoes iterative hashing to form a hash chain [34]. The resulting tip,  $h^n(seed)$ , is stored in CS memory as a Trust Anchor ( $TA$ ) for subsequent operations.

Prior to launch, storing  $TA$  in CS is straightforward. Post-launch introduces considerations for secure transmission. Confidentiality is ensured through pre-existing mechanisms supporting confidentiality, allowing direct transfer of  $TA$  without additional security layers. Encryption becomes necessary only when the default mechanism lacks confidentiality support despite the additional overhead.

2) *Key encapsulation phase*: The key encapsulation phase conceals a one-time Authentication Token ( $AT$ ) without utilizing encryption techniques. Our key encapsulation involves a bitwise XOR operation ( $\oplus$ ) between the current  $AT$  (i.e.,  $AT_{curr}$ ) and the result of applying a cryptographic hash function ( $h$ ) to the concatenation of  $SUP$  and the previous  $AT$  (i.e.,  $AT_{prev}$ ) as shown in Eq. (1).

$$TT := AT_{curr} \oplus h(SUP \parallel AT_{prev}) \quad (1)$$

Basically, we combine  $AT_{curr}$  with a hashed value derived from the concatenation of  $SUP$  and  $AT_{prev}$  to generate  $TT$ . Fig. 3 shows interconnection between subsequent  $TT$ s.

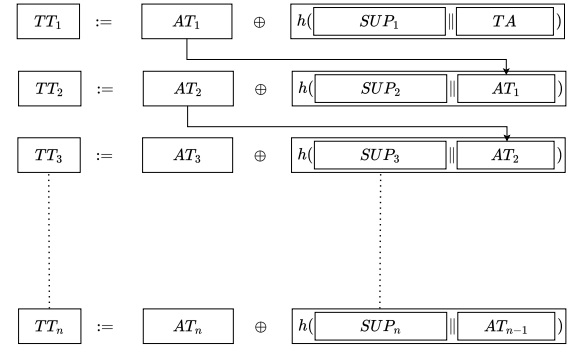


Fig. 3. Protocol describing secure software update procedure.

3) *Authentication and integrity phase*: The authentication and integrity phase is crucial in ensuring the secure transmission of *SUPs* from GS to CS. This phase links  $TT$  to  $AT_{curr}$ ,  $SUP$ , and  $AT_{prev}$  (previous state of hash chain) while confirming the validity of  $AT_{curr}$ . CSUM ensures integrity by associating the hash of  $SUP$  to  $TT$  as shown in Eq. (1). Any attempt by an adversary to alter  $SUP$  results in CS failing to extract the correct  $AT_{curr}$  from  $TT$ , leading to the rejection of  $SUP$ .  $AT_{curr}$  verification requires a single hash operation, as shown in Eq. (2).

$$h(AT_{curr}) = AT_{prev} \quad (2)$$

Overall, the proposed scheme leverages hash functions to ensure authentication and integrity in a resource-constrained environment, making it suitable for CS with limited bandwidth, processing power, and memory. The hash chain and  $TT$

mechanisms provide a lightweight yet effective approach to secure software updates in the presence of potential adversaries and insecure communication channels.

## B. Operations

This section explains the tasks executed by the administrator, GS, and CS within the proposed scheme. Fig. 4 presents a sequence diagram that illustrates CSUM for securely installing software updates on CSs.

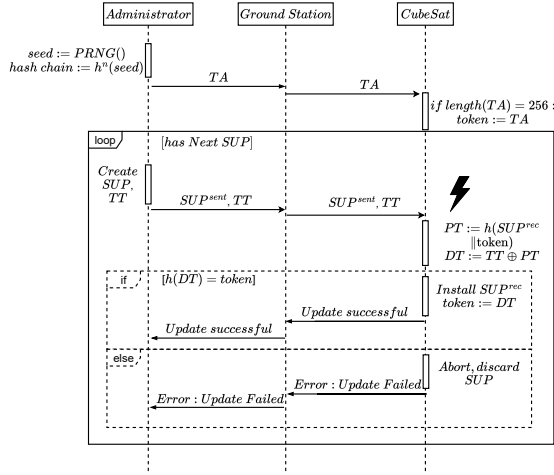


Fig. 4. Sequence diagram illustrating CSUM for secure software update.

1) *Administrator operation*: Several crucial tasks are undertaken to ensure the proper functioning of CSUM at the administrator's end. These tasks include generating a hash chain and creating a  $SUP$  with the corresponding  $TT$ . The administrator initializes the scheme by generating a random seed; the generated seed is hashed iteratively to create a hash chain. Each  $SUP$  sent to CS is accompanied by its corresponding  $TT$ , formulated as shown in Eq. (1). Algorithm 1 presents the pseudocode for  $TT$  generation by the administrator for each  $SUP$ .

The administrator and GS can communicate in an encrypted or plain text manner. However, we require an integrity mechanism while sending  $SUP$ s without encryption. We especially require an encrypted connection between the administrator and GS only while sending  $TA$  during the initial setup phase. For regular  $SUP$ s, the administrator creates and sends  $SUP$  and the corresponding  $TT$  to the GS. Algorithm 1 details the pseudocode for this case.

2) *Ground station operations*: GS receives  $SUP$  and  $TT$  from the administrator. It forwards both  $SUP$  and  $TT$  to CS in unencrypted form. GS has more resources than CS in terms of computational power. It enables GS to manage communication links with multiple satellites simultaneously and process large amounts of data transmitted from such satellites.

3) *CubeSat operations*: CS extracts both  $SUP$  and its corresponding  $TT$  from a transmission received from the GS.

Subsequently, CS deciphers  $AT_{curr}$  using received  $SUP$ ,  $TT$  and  $AT_{prev}$ , using Eq. (3).

$$AT_{curr} := TT \oplus h(SUP \parallel AT_{prev}) \quad (3)$$

Following token extraction, CS verifies the authenticity of deciphered  $AT_{curr}$  by comparing its hash with  $AT_{prev}$  as shown in Eq. (2). Successful verification confirms the integrity and authenticity of  $SUP$ , and thus, CS installs  $SUP$  and updates  $AT_{prev}$ . Algorithm 2 provides pseudocode for  $AT$  extraction,  $AT$  verification, and  $SUP$  installation at CS.

### Algorithm 1 $TT$ generation by administrator.

**Input:**  $SUP$ ,  $AT_{curr}$ ,  $AT_{prev}$

**Output:**  $TT$

```

1: if  $h(AT_{curr}) = AT_{prev}$  then                                ▷ Validate AT
2:    $PT = h(SUP \parallel AT_{prev})$ 
3:    $TT := AT_{curr} \oplus PT$ 
4:   return  $TT$ 
5: else
6:   Invalid  $AT_{curr}$  and  $AT_{prev}$  combination
7: end if

```

### Algorithm 2 $AT$ extraction and verification by CS.

**Input:**  $SUP^{rec}$ ,  $TT$

**Output:** True/False

```

1: while hasNextUpdate() do
2:    $PT := h(SUP^{rec} \parallel token)$ 
3:    $DT := TT \oplus PT$ 
4:   if  $h(DT) = token$  then                                ▷ Validate DT
5:     Install  $SUP^{rec}$  on CS
6:      $token := DT$ 
7:     Send "Update successful" message to GS
8:     return True
9:   else
10:    Abort update
11:    Send "Error: Update Failed" message to GS
12:    return False
13:   end if
14: end while

```

Fig. 5 outlines the verification procedure for  $TT$  at CS. If CS receive  $SUP^{sent}$  and  $TT$  without any modification to  $SUP$  or  $TT$  during transmission then  $SUP^{sent} = SUP^{rec}$ ,  $DT = AT_{curr}$ . Here,  $token$  is a local variable stored in CS such that other parties are unable to access it.

## V. EXPERIMENTAL EVALUATION

We performed experiments on a Lenovo ThinkPad P14s Gen 2 machine. We implemented our proposed scheme using python 3.7 and utilized four common open-source packages including Putty, Notepad++, FileZilla, and Audacity with sizes  $< 16$  MB to simulate  $SUP$  being sent to CS.

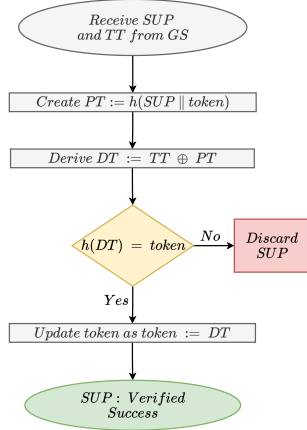


Fig. 5. Flowchart describing software verification procedure at CS.

Encryption/decryption-based schemes are traditionally employed to provide authentication, confidentiality, and integrity. However, they may not inherently guarantee data freshness. Moreover, decryption operations at CS can impose a significant computational burden. Signature-based schemes primarily focus on ensuring authentication and integrity with the potential to provide freshness depending on the specific implementation. However, signature verification operations at CS can also introduce computational overhead.

To this end, we designed an experiment with different commonly used software applications, including Putty v0.80 [35], NotePad++ v8.6 [36], FileZilla v3.66.4 [37], and Audacity v3.4.2 [38]. We performed the following cryptographic operations: encryption, decryption, signature generation, signature verification, and hashing on these open-source software packages to collect timing data. We utilize RSA with a 2048-bit key with PSS padding [39] for signing, AES with a 256-bit key in CBC mode for encryption, and SHA-256 for hashing. We used *hazmat* layer from the Python cryptography library [40] to implement cryptographic primitives. The results are shown in Fig. 6. Encryption, signature generation, and hashing operations are performed at administrator (without any resource limitation) while decryption, signature verification, and hashing operation are done at CS (with limited resources).

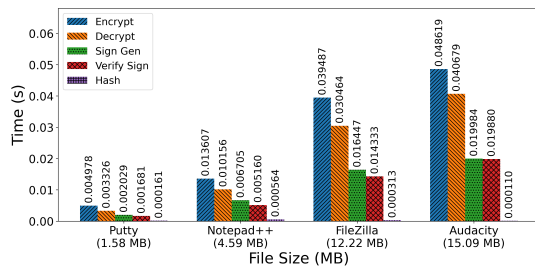


Fig. 6. Timing information for various software of cryptographic primitives.

As shown in Fig. 6, we observe that hashing operations are consistently the fastest across various file sizes, taking only 0.000161s for a 1.58 MB file, 0.000564s for a 4.59 MB

file, 0.000313s for a 12.22 MB file, and 0.000110s for a 15.09 MB file. Signature verification, a process that ensures data integrity and authenticity, is more time-consuming than hashing, with times ranging from 0.001681s for the smallest file to 0.019880s for the largest file. Decryption times, which ensures confidentiality, data integrity and authenticity, is even more expensive than signature verification, requiring 0.003326s for the smallest file and scaling up to 0.040679s for the largest tested file.

CSUM inherently assures authentication, integrity, and freshness by using a hash chain. Freshness is assured by the sequential nature of the hash chain, which prevents the reuse of old hashes. CSUM simplifies the verification process by requiring only a single hash operation at CS, significantly reducing computational overhead.

**Performance:** TABLE II shows the performance analysis of the hash chain, particularly, the time taken to generate the hash chain and the verification time. CSUM takes less than 0.01s to generate a hash chain for 10,000 updates, and it gradually increases to 0.056s for 50,000 updates. This rise indicates a proportional increment in the computational load associated with a larger number of targeted updates. On another side, verifying 10,000 updates requires about 0.18s, which increases to 0.805s for 50,000 updates. This increase is steeper since more operations are involved in verifying *SUPs* than in generating a hash chain. Overall, both the hash chain generation time and verification of *SUPs* grow linearly with the number of *SUPs*.

TABLE II  
PERFORMANCE ANALYSIS OF HASH CHAINS.

| Number of <i>SUPs</i> | Time taken to generate hash chain (s) | Verification by our approach for every single <i>SUP</i> in chain (s) |
|-----------------------|---------------------------------------|-----------------------------------------------------------------------|
| 10,000                | <0.01                                 | 0.179558                                                              |
| 20,000                | 0.019748                              | 0.316285                                                              |
| 30,000                | 0.031258                              | 0.509595                                                              |
| 40,000                | 0.040098                              | 0.635965                                                              |
| 50,000                | 0.055507                              | 0.805479                                                              |

**Network overhead:** The network overhead in our approach is independent of the size of a *SUP*, and it is determined by the fixed output length of the utilized hash function, i.e., 256 bits in our implementation. Therefore, our proposed scheme has a constant network overhead.

## VI. CONCLUSION AND FUTURE WORK

In this paper, we propose a lightweight scheme that ensures authentication, integrity, and data freshness for CS software updates, providing a practical solution specifically tailored to the resource-constrained environment of CS. We validate the practical feasibility and efficacy of our proposed approach by developing a proof of concept. Our results indicate that CSUM significantly improves the performance of the software update procedure for CS. In the future, we will explore a scalable and secure group update scheme for a cluster of CSs, eliminating the need for unique *AT* per satellite/update.

## REFERENCES

- [1] W. Lechner and S. Baumann, "Global Navigation Satellite Systems," *Computers and Electronics in Agriculture*, vol. 25, no. 1-2, pp. 67–85, 2000.
- [2] S. Kalsi, "Satellite based Weather Forecasting," *Satellite remote sensing and GIS applications in agricultural meteorology*, vol. 331, 2002.
- [3] M. Antonini, A. De Luise, M. Ruggieri, and D. Teotino, "Satellite Data Collection & Forwarding Systems," *IEEE Aerospace and Electronic Systems Magazine*, vol. 20, no. 9, pp. 25–29, 2005.
- [4] M. Swartwout, "The First One Hundred Cubesats: A Statistical Look," *Journal of Small Satellites*, vol. 2, no. 2, pp. 213–233, 2013.
- [5] K. Woellert, P. Ehrenfreund, A. J. Ricco, and H. Hertzfeld, "Cubesats: Cost-effective Science and Technology Platforms for Emerging and Developing Nations," *Elsevier Advances in Space Research*, vol. 47, no. 4, pp. 663–684, 2011.
- [6] A. Bellissimo, J. Burgess, and K. Fu, "Secure Software Updates: Disappointments and New Challenges," in *USENIX Workshop on Hot Topics in Security*, 2006.
- [7] M. Eshaq, I. Al-Midfa, Z. Al-Shamsi, S. Atalla, S. Al-Mansoori, and H. Al-Ahmad, "Flight Software Design and Implementation for a CubeSat," in *IEEE Advances in Science and Engineering Technology International Conferences*, 2023, pp. 1–6.
- [8] D. J. Kessler, N. L. Johnson, J. Liou, and M. Matney, "The Kessler Syndrome: Implications to Future Space Operations," *Advances in the Astronautical Sciences*, vol. 137, no. 8, 2010.
- [9] J. Pavur and I. Martinovic, "The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space," in *IEEE Int. Conf. on Cyber Conflict*, 2019, pp. 1–18.
- [10] J. Drmola and T. Hubik, "Kessler Syndrome: System Dynamics Model," *Space Policy*, pp. 29–39, 2018.
- [11] F.-X. Molina, E. Baccelli, K. Zandberg, D. Donsez, and O. Alphand, "Cubedate: Securing Software Updates in Orbit for Low-Power Payloads Hosted on CubeSats," in *IFIP/IEEE Int. Conf. on Performance Evaluation and Modeling in Wired and Wireless Networks*, 2023, pp. 1–6.
- [12] (2022) Thingsat project. CSUG - Grenoble University Space Center. [Online]. Available: <https://www.csug.fr/projects/thingsat-project/>
- [13] R. Nilchiani, "Valuing Software-based Options for Space Systems Flexibility," *Acta Astronautica*, vol. 65, no. 3-4, pp. 429–441, 2009.
- [14] B. Garrido, A. Garcia, N. Alfaro, and J. Asensio, "MINISAT01 on-board Software Maintenance," in *Data Systems in Aerospace*, vol. 422, 1998, p. 65.
- [15] W. Marshall and C. Boshuizen, "Planet Labs' Remote Sensing Satellite System," 2013.
- [16] C.-S. Park, "One-time Password based on Hash Chain without Shared Secret and Re-registration," *Computers & Security*, vol. 75, pp. 138–146, 2018.
- [17] S. Halder, A. Ghosal, and M. Conti, "Secure Over-The-Air Software Updates in Connected Vehicles: A Survey," *Computer Networks*, vol. 178, p. 107343, 2020.
- [18] T. Karthik, A. Brown, S. Awwad, D. McCoy, R. Bielawski, C. Mott, S. Lauzon, A. Weimerskirch, and J. Capps, "Uptane: Securing Software Updates for Automobiles," in *International Conference on Embedded Security in Car*, 2016, pp. 1–11.
- [19] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles," in *IEEE Wireless Communications & Networking*, 2019, p. 7.
- [20] D. K. Nilsson and U. E. Larson, "Secure Firmware Updates over the Air in Intelligent Vehicles," in *IEEE International Conference on Communications Workshops*, 2008, pp. 380–384.
- [21] M. Steger, C. A. Boano, T. Niedermayr, M. Karner, J. Hillebrand, K. Roemer, and W. Rom, "An Efficient and Secure Automotive Wireless Software Update Framework," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2181–2193, 2017.
- [22] M. S. Idrees, H. Schwappe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger, "Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates," in *Springer Communication Technologies for Vehicles. Nets4Cars/Nets4Trains*, 2011, pp. 224–238.
- [23] R. Petri, M. Springer, D. Zelle, I. McDonald, A. Fuchs, and C. Krauß, "Evaluation of Lightweight TPMs for Automotive Software Updates over the Air," in *International Conf. on Embedded Security in Car*, 2016, pp. 1–15.
- [24] K. V. de Souza, Y. Bouslimani, and M. Ghribi, "Flight Software Development for a CubeSat Application," *IEEE Journal on Miniaturization for Air and Space Systems*, vol. 3, no. 4, pp. 184–196, 2022.
- [25] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abasi, "Space Odyssey: An Experimental Software Security Analysis of Satellites," in *IEEE Symposium on Security and Privacy*, 2023.
- [26] S. Fitzsimmons, *Reliable Software Updates for On-orbit Cubesat Satellites*. California Polytechnic State University, 2012.
- [27] I. Sünter, A. Slavinskis, U. Kvell, A. Vahter, H. Kuuste, M. Noorma, J. Kutt, R. Vendt, K. Tarbe, M. Pajusalu et al., "Firmware Updating Systems for Nanosatellites," *IEEE Aerospace and Electronic Systems Magazine*, vol. 31, no. 5, pp. 36–44, 2016.
- [28] A. Slavinskis, M. Pajusalu, H. Kuuste, E. Ilbis, T. Eenmäe, I. Sünter, K. Laizans, H. Ehrpais, P. Liias, E. Kulu et al., "ESTCube-1 In-Orbit Experience and Lessons Learned," *IEEE Aerospace and Electronic Systems Magazine*, vol. 30, no. 8, pp. 12–22, 2015.
- [29] B. Bezem and P. K. J. Fjellby, "Authenticated Uplink for the Small, Low Orbit Student Satellite NUTS," *Department of Telematics, NTNU*, 2012.
- [30] O. Challa, G. Bhat, and J. Mcnair, "CubeSec and GndSec: A Lightweight Security Solution for CubeSat Communications," 2012.
- [31] L. Wood, W. M. Eddy, W. Ivancic, J. McKim, and C. Jackson, "Sarotoga: A Delay-Tolerant Networking Convergence Layer with Efficient Link Utilization," in *IEEE International Workshop on Satellite and Space Communications*, 2007, pp. 168–172.
- [32] C. Boyd, A. Mathuria, and D. Stebila, *Protocols for Authentication and Key Establishment*. Springer, 2020.
- [33] R. Davies, "Hardware Random Number Generators," in *15th Australian Statistics Conference*, 2000.
- [34] L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
- [35] (2023) Putty v0.80. [Online]. Available: <https://the.earth.li/~sg-tatham/putty/0.80/w64/putty.exe>
- [36] (2023) Notepad++ v8.6. [Online]. Available: <https://github.com/notepad-plus-plus/notepad-plus-plus/releases/download/v8.6/npp.8.6.Installer.x64.exe>
- [37] (2023) FileZilla v3.66.4. [Online]. Available: [https://download.filezilla-project.org/client/FileZilla\\_3.66.4\\_win64\\_sponsored2-setup.exe](https://download.filezilla-project.org/client/FileZilla_3.66.4_win64_sponsored2-setup.exe)
- [38] (2023) Audacity v3.4.2. [Online]. Available: <https://github.com/audacity/audacity/releases/download/3.4.2/audacity-win-3.4.2-64bit.exe>
- [39] M. Bellare and P. Rogaway, "PSS: Provably Secure Encoding Method for Digital Signatures," 1998.
- [40] (2023) Cryptography. [Online]. Available: <https://pypi.org/project/cryptography/>