StarCast: A Secure and Spectrum-Efficient Group Communication Scheme for LEO Satellite Networks

Chaoyu Zhang, Hexuan Yu, Shanghao Shi, Shaoyu Li, Yi Shi, Eric Burger, Y. Thomas Hou, and Wenjing Lou

Virginia Tech, VA, USA

Abstract—**Low Earth Orbit (LEO) satellite networks serve as a cornerstone infrastructure for providing ubiquitous connectivity in areas where terrestrial infrastructure is unavailable. With the emergence of Direct-to-Cell (DTC) satellites, these networks can provide direct access to mobile phones and IoT devices without relying on terrestrial base stations, leading to a surge in massive connectivity demands for the serving satellite. To address this issue, group communication is an effective paradigm that enables simultaneous content delivery to multiple users and thus optimizes bandwidth reuse. Although extensive research has been conducted to improve group communication performance, securing this communication without compromising its inherent spectrum efficiency remains a critical challenge. To address this, we introduce StarCast, a secure group encryption scheme for LEO satellite networks. Our solution leverages ciphertext-policy attribute-based encryption (CP-ABE) to implement fine-grained access control by embedding access policies directly within the ciphertext. Unlike standard secure communication approaches that require dedicated per-user channels and significantly deplete limited satellite spectrum resources, StarCast maintains efficient spectrum reuse within user groups while ensuring that only authorized users can access transmitted data. Additionally, it significantly reduces the costly key management overhead associated with conventional encryption schemes.**

Index Terms—**LEO Satellites, Spectrum Efficiency, Ciphertext-Policy Attribute-Based Encryption, Group Encryption**

I. INTRODUCTION

LEO satellite networks have emerged as the key infrastructure for bridging connectivity gaps in remote and underserved regions. These networks support various applications, including remote access for mobile phones and IoT devices, disaster recovery efforts, and military communication. The integration of LEO satellite networks into the 3GPP ecosystem began with Release 17, which established global standards for NT networks, enabling satellite-based New Radio and IoT access for seamless service continuity [1]. With further enhancements planned in Release 18, LEO satellite networks are expected to play a central role in the evolution of 6G [2]. The rise of DTC LEO satellites, such as Starlink V2, AST BlueWalker 3, and Lynk, has exponentially expanded user access [3]. By enabling direct connectivity between satellites and devices, these systems eliminate the reliance on traditional ground infrastructure, extending connectivity to billions of users. This increasing demand underscores the urgent need to optimize spectrum efficiency to support the growing number of user connections while maintaining reliable, high-quality service.

However, LEO satellite communication systems face several critical constraints that limit their scalability in accommodating a massive number of user accesses. First, the onboard communication resources of LEO satellites are inherently limited due to restricted spectrum availability and the finite number of beams available for simultaneous connections, particularly in high-density areas [4]. The emergence of DTC LEO satellites exacerbates the issue of limited licensed spectrum. Satellite network operators (SNOs) must share the already allocated 4G/5G bands with terrestrial mobile network operators (MNOs) under FCC/ITU regulations (Tab. I). Additionally, the scarcity of orbital slots, which require approval from the ITU/FCC, imposes further constraints on the deployment of new satellites. Furthermore, the high capital investment required for developing, launching, and maintaining constellations presents a significant barrier to scaling these networks in a timely manner to meet sudden spikes in connectivity demand [5], [6].

Motivation. To address the critical challenge of sending data to multiple users, group communication plays a crucial role. Modern LEO satellites, such as Starlink [7], increase their user access capacity by utilizing narrow spot beams, enabling them to serve multiple users simultaneously and reuse the same spectrum across different beams. Another technique to improve satellite spectrum efficiency is to use a broader beamwidth to enable multiuser coverage while using a single beam's spectrum to deliver the same content to many different users, such as multicast and broadcast communication. These approaches not only achieve high throughput, but also considerably increase an individual satellite's connectivity capacity. For example, the digital satellite television broadcast standard (DVB-S2X [8]) allows each spot beam to serve numerous customers simultaneously by broadcasting a single coded frame, thus optimizing resource allocation.

Multi-beam satellite systems have recently garnered considerable research interest, with extensive studies dedicated to improving satellite group communication performance [9]–[12]. Despite these advancements, there remains a critical need to develop security solutions for LEO satellites in group communication scenarios while preserving the inherent spectrum efficiency. To protect information confidentiality, encryption is essential. If all receivers use the same secret key to decrypt the broadcasted ciphertext from the satellite, a single device compromise could lead to information leakage. Standard end-to-end encryption (E2EE) secures data and facilitates access control by employing a unique pair of cryptographic keys for each receiver [13], [14]. However, this approach requires individual encrypted communication channels for each user, which hinders spectrum reuse within the group and undermines the

efficiency expected from group communication. In a broadcast encryption system [15], [16], a ciphertext is protected by encrypting the group key using each group member's public key, thereby involving different keys for every user. However, scalability becomes a bottleneck as the number of system participants increases or as group membership changes dynamically. This significantly increases the number of required keys, complicating key distribution, management, and revocation.

Our Solution. To address these concerns, we propose StarCast, a secure and efficient group encryption scheme for LEO satellite networks that preserves the inherent spectrum efficiency of group communication. StarCast secures data and enables simultaneous transmission to all users covered by the same beam while ensuring that only legitimate users can decrypt the information.

StarCast utilizes CP-ABE [17]–[23] as its cryptographic foundation, employing an attribute-based policy to facilitate scalable, fine-grained access control for a group of legitimate users. StarCast allows the server to encrypt data and specify an access policy for this information. The ciphertext, embedded with the access policy, is broadcast to various users within the beam but can only be decrypted by those whose attributes satisfy the access policy, eliminating the need for multiple individually encrypted channels for each user. StarCast significantly reduces the overhead associated with key management in large-scale systems, as users no longer require individual keys for each communication session. This attribute-based design enables our system to scale dynamically and efficiently. Furthermore, StarCast supports backward secrecy and revocability, and is resistant to collusion attacks, preventing adversaries from combining attribute keys from multiple non-members to access information that neither could access individually. StarCast ensures security while optimizing the utility of limited satellite spectrum resources by effectively combining multiple unicast communications with a physical-layer broadcast wireless signal for a group of users. Using this approach, the satellite can leverage phased array antennas to generate optimized and flexible beam directions and beamwidths tailored to group members, providing better signal strength compared to a large beam used for broadcasting to all users.

Our Contribution:

- We propose StarCast, a secure and efficient group encryption scheme designed specifically for LEO satellite networks, addressing the critical need for enhanced connectivity capacity.
- StarCast leverages CP-ABE to provide fine-grained and scalable access control, significantly reducing the complexity of key management in dynamically changing and large-scale user systems.
- StarCast enhances both performance and efficiency in secure LEO satellite networks by enabling simultaneous ciphertext transmission to multiple users within the same beam and maximizing spectrum reuse.
- We prototype StarCast using the Starlink Standard Kit and conduct comparative evaluations against secure uni-
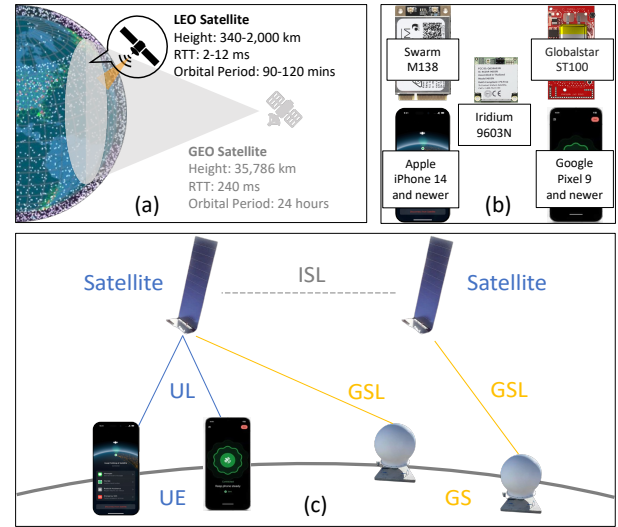

Fig. 1. (a) Starlink Coverage Map; (b) DTC Supported Mobile Phone and IoT Devices; (c) DTC LEO Satellite Network

TABLE I
COMPARISON OF SATELLITE COMMUNICATION PROVIDERS AND SPECIFICATIONS

SNO/Partner	# of Satellites	Spectrum/Band	Standard
SpaceX/T-Mobile	2016	MNO-band	3GPP
AST/AT&T	243	MNO-band	3GPP
Kuiper/Verizon	3236	Ka-band	Proprietary
Globalstar/Apple	24	L-band, S-band	Proprietary
Iridium/Qualcomm	66	L-band	Proprietary

cast and broadcast frameworks, demonstrating the spectrum efficiency of our design.

II. PRELIMINARY AND RELATED WORK

A. LEO Satellite Constellation

LEO satellite constellations orbit below 2000 km above the Earth [24], offering low-latency, high-speed connectivity compared to geostationary satellites (Fig. 1(a)). One transformative feature of LEO satellites is their DTC capability, which enables mobile phones and IoT devices to connect directly to satellites without relying on terrestrial base stations. For instance, satellite network operators like Starlink V2 and other DTC-enabled systems seek to connect the roughly 2.6 billion people who do not have access to dependable internet [25] (Tab. I). To achieve this, terminal devices that support the DTC satellite communication function (Fig. 1(b)) can connect directly to an accessible LEO satellite via a User Link (UL). The satellite operates as an onboard radio access network (RAN) and transmits signals to a Ground Station (GS) via a GS-to-Satellite Link (GSL), which connects to the terrestrial core network (Fig. 1(c)). Additionally, Starlink satellites utilize inter-satellite links (ISLs) powered by space laser communication, enabling direct satellite-to-satellite data transfer without the need for intermediate GS relays.

B. Group Communication in Satellite Network

The DTC capability of LEO satellites dramatically increases the number of users and devices accessing the network, leading to massive connectivity demands. Recent literature has focused on utilizing beams generated by phased array antennas to enhance spectrum efficiency, improve power density, and support higher data rates [26]. User grouping and beamwidth optimization have been proposed to address the trade-offs between serving more users simultaneously and maintaining adequate signal strength [9], [10] for downlink multicast communications. Various beamforming and pre-coding strategies have also been explored, including optimization algorithms that minimize power consumption while maintaining the quality of service [27]–[29].

C. Secure Group Communication

Despite extensive research to enhance group communication efficiency, the challenge of ensuring secure communication without compromising spectrum efficiency remains. As next-generation communication systems evolve, the security and privacy of upcoming 6G networks are increasingly critical [30]–[35]. Secure group communication can be achieved through centralized key management and end-to-end session encryption [36]–[38]. Another approach, broadcast encryption, ensures communication security and access control by encrypting the group key using each member's public key. Various broadcast encryption schemes embed these encrypted keys in the ciphertext [13]–[16]. Additionally, several efforts focus on improving protection scheme efficiency [39]–[41]. Attribute-based encryption originated as a fuzzy variant of identity-based encryption [42]. In CP-ABE schemes [17]–[23], a user's private key is associated with specific attributes, and ciphertexts are encrypted according to an access policy. Decryption is only possible if the user's attributes meet the policy requirements.

D. Cryptographic Preliminaries

1) Bilinear map or pairing e: The cryptographic design of StarCast is based on CP-ABE. This scheme leverages bilinear maps as the mathematical foundation to enable efficient cryptographic operations, fine-grained access control, and provable security. For all $u, v \in \mathbb{Z}$, $x \in \mathbb{G}_1$, and $y \in \mathbb{G}_2$, it holds that $e(x^u, y^v) = e(x, y)^{uv}$. Besides, e is non-degenerate, i.e., $e(x, y) \neq 1$. We define **Gen** as an asymmetric pairing group generator that, on input 1^λ, outputs three groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ of prime order $p = \Theta(\lambda)$. These groups come with a non-degenerate and efficiently computable bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. g and h are the group generators for $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The CP-ABE scheme utilized in StarCast is based on Type-III pairings (i.e., asymmetrical prime order pairings).

2) Access Policy and Attributes: An access policy $\mathcal{A}$ specifies how attributes are managed to control access to the encrypted secret [21], and it is typically embodied in a policy that specifies which combinations of user attributes are required to decrypt a ciphertext. Access policy $\mathcal{A}$ is a collection of non-empty subsets of $\mathcal{U}$, $\mathcal{A} \subseteq 2^{\mathcal{U}} \setminus \{0\}$, where $\mathcal{U}$ denotes the universe of attributes. $\mathcal{A}$ can be effectively modeled using Boolean formulas involving AND and OR gates. If all inputs corresponding to attributes in S are set to true and all other inputs are set to false, then a set of attributes $S \subseteq \mathcal{U}$ meets a formula.

A generalization of the Boolean formula can be achieved by monotone span programs (MSPs), also known as a liner secret sharing scheme [43], [44]. The *monotonicity* is defined as for all $\mathcal{P}, \mathcal{Q} \subseteq \mathcal{U}$ that $\mathcal{P} \subseteq \mathcal{Q}$, $\mathcal{P} \in \mathcal{U}$ implies $\mathcal{Q} \in \mathcal{U}$. *Monotonicity* implies that if an authorized user has additional attributes, their access remains valid and their privilege remains true.

An MSP is given by a matrix $\mathbf{M}$ of size $n_1 \times n_2$ over $\mathbb{Z}_p$ and a mapping $\pi : \{1, \ldots, n_1\} \to \mathcal{U}$. A monotone boolean formula F can be converted into an MSP $(\mathbf{M}, \pi)$ [45]. Every element in the matrix $\mathbf{M}$ is either 0, 1, or -1. Each row of matrix $\mathbf{M}$ represents an input in F, and the number of columns is equal to the number of AND gates in F.

Suppose S is a set of attributes, and $I = \{i \mid i \in \{1, \ldots, n_1\}, \pi(i) \in S\}$ is the set of rows in $\mathbf{M}$ that belong to S. We define the acceptance of S by $(\mathbf{M}, \pi)$ as the existence of a linear combination of rows in I that yields the vector $(1, 0, \ldots, 0)$ such that $\sum_{i \in I} \gamma_i (\mathbf{M})_i = (1, 0, \ldots, 0)$, where $(\mathbf{M})_i$ denotes the ith row of $\mathbf{M}$.

III. System Model and Threat Model

A. System Model

We consider a scenario for downlink group communication through LEO satellites (Fig. 2, right). The system comprises three key components: the server, N ground users, and the LEO satellite. The server utilizes a terrestrial ground station to access the on-orbit satellite, which transmits encrypted data to different groups of users. The server determines the access policy for users based on their corresponding privileges, and all users possess secret keys generated by the server. In our system, we assume that the LEO satellite can obtain the location information of all users and is aware of their access privileges as provided by the server. The satellite is equipped with advanced phased array technology at a height h, enabling it to generate beams with flexible directionality. The coordinates of the center of a beam are represented by $\mathbf{w}_m$, while the beam's coverage radius is denoted by r_m. The adjustable beamwidth, θ_m, expressed in degrees, is adaptive to provide optimal signal strength for a legitimate group of users (Fig. 2, left). The server employs group communication to send encrypted data to users, ensuring that only legitimate recipients within the beam can decrypt it. The system is capable of managing the mobility of user devices and handling beam handovers when devices are covered by multiple beams, ensuring a smooth transition of the wireless signal from one beam to another. LEO satellites, equipped with phased array antennas, maintain continuous communication sessions with user devices, even during ground station handovers between satellites.
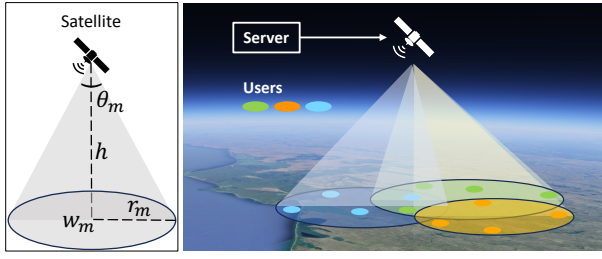
Fig. 2. StarCast system model

B. Threat Model

We assume that the satellite communication service is controlled and provided by an honest-but-curious third party, such as Starlink. Consequently, a security mechanism is required to preserve data confidentiality and achieve access control. We assume that an attacker can intercept wireless signals transmitted between the satellite and user devices, potentially gaining access to ciphertext. Our primary concern is the encryption of the plaintext data and ensuring access control, so only the legitimate group of users can decrypt the ciphertext and access the original information. Other types of attacks, such as jamming or physical destruction of user devices, are beyond the scope of this research and require separate studies to address.

IV. DESIGN OF STARCAST

A. Scheme Overview

The key idea of StarCast is to secure the group communication scheme for LEO satellite networks while preserving the inherent spectrum efficiency of group communication. At the physical layer, StarCast broadcasts encrypted data to all users covered by the same beam simultaneously. At the presentation layer, the cryptographic design ensures data confidentiality and guarantees that only legitimate users can decrypt the information. To achieve this, the server in StarCast sends the ciphertext c for group communication, attaching it with an access policy $\mathcal{A}$. On the user side, a secret key sk associated with a set of attributes can decrypt the ciphertext only if the set of attributes S satisfies the access policy $\mathcal{A}$. Our formal definitions of the cryptographic design follow [20], [21], whose security properties and proofs are well established.

The high-level concept of the StarCast cryptographic scheme with MSPs is described as follows. Each secret key is associated with the user's attribute set, S. For each attribute $x \in S$, there is a corresponding component sk_y in the key. These components are composed of elements from group $\mathbb{G}_2$. To prevent users from colluding multiple keys to decrypt a ciphertext that none of them could individually decrypt, the policies of these components and their interconnections must be tied properly. Meanwhile, each ciphertext contains components from a group $\mathbb{G}_1$. For a given access policy represented by an MSP, each row of the MSP matrix corresponds to a component c_i, where i is the i-th row of the matrix $\mathbf{M}$. This part can mask the i-th row's share by some specific

numbers, which have to correspond to $sk_{\pi(i)}$, by the form of the component of the key. Thus, it allows a user with attribute $\pi(i)$ to reveal the i-th share during **Dec()**. This ensures that only users with a specific set of policy-compliant attributes can decrypt the information while also preventing any type of collusion attack. The public parameters, established during **Setup()**, provide the necessary values for both the ciphertext and key components. It is crucial to assign distinct group elements to each attribute to prevent any single key component from revealing multiple shares in a ciphertext.

B. Workflow

We illustrate the workflow of StarCast in Fig. 3. For initialization, the server first sets up essential security parameters and generates a public key and a master key at step ①. Then, it generates and distributes the corresponding secret keys for each user based on their attributes at step ②. During group communication, the server encrypts data at step ③ according to the access policy, which is formulated by the data management rules and users' privilege. At step ④, the server uploads ciphertexts to the LEO satellites, which serve as critical infrastructure for utilizing group communication to deliver these messages to users. The LEO satellites, equipped with advanced phased array technology, can generate the beam with flexible directionality and adjustable beamwidth, leveraging vendor-provided algorithms to ensure optimal signal strength for the legitimate user group. Finally, at step ⑤, the users decrypt the ciphertext data if and only if their attributes satisfy the corresponding access policies.

For example, we consider the server to define the access policy for users as follows: Only the team leaders or Team Blue's members participating in task Alpha can decrypt the message, i.e., $\mathcal{A} = ($"Alpha"AND("Leader"OR("Blue"AND"Member"))). As a result, the user with an attribute set $S_1 = \{$Alpha, Blue, Leader, . . .$\}$ can decrypt the message, but another user with an attribute set $S_4 = \{$Beta, Blue, Member, . . .$\}$ cannot.

C. Protocol Details

Setup(1^λ): On inputting a security parameter λ, the server generates $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g, h)$. $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are three groups with prime order p, while g and h are two generators for $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Server picks $\alpha_1, \beta_1, \alpha_2, \beta_2 \leftarrow_R \mathbb{Z}_p^*$ and $\delta_1, \delta_2, \delta_3 \leftarrow_R \mathbb{Z}_p$, computes the public key pk and the master key mk:

$$pk : (h, T_1 := e(g,h)^{\delta_1\alpha_1+\delta_3}, \tag{1}$$
$$H_1 := h^{\alpha_1}, T_2 := e(g,h)^{\delta_2\alpha_2+\delta_3}, H_2 := h^{\alpha_2})$$
$$mk : (\alpha_1, \beta_1, \alpha_2, \beta_2, g, h, g^{\delta_1}, g^{\delta_2}, g^{\delta_3}) \tag{2}$$

KeyGen(mk, S): The server processes the attribute sets for each user and generates their respective secret keys. It picks $\rho_1, \rho_2 \leftarrow_R \mathbb{Z}_p$ and uses h, β_1, β_2 from mk to compute:

$$sk_0 := (h^{\beta_1\rho_1}, h^{\beta_2\rho_2}, h^{\rho_1+\rho_2}) \tag{3}$$

Arbitrary binary strings can be mapped to elements of the group $\mathbb{G}_1$ using a hash function $\mathcal{H}$. $\mathcal{H}$ receives two kinds
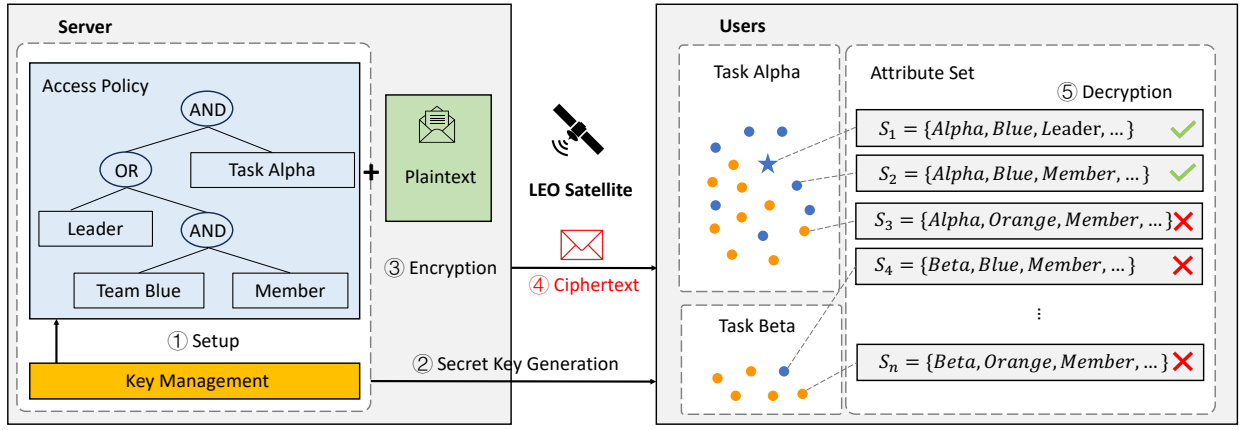
Fig. 3. **System Design:** In our system, the server defines an access policy, and only those users whose attributes meet it can decrypt the data. An LEO satellite utilizes group communication to send the ciphertext to the users of the legitimate group simultaneously.

of input: strings and numbers. It takes the form of (ξ, ℓ, t) or (ρ, ℓ, t), where ξ is an arbitrary string, ρ is a positive integer, $\ell \in \{1, 2, 3\}$ and $t \in \{1, 2\}$. These two inputs are denoted, for simplicity, as $\xi\ell t$ and $0\rho\ell t$, respectively. For easy differentiation between them, append 0 at the beginning of the second element. For all $x \in S$ and $t = 1, 2$, where $\sigma_x \leftarrow_R \mathbb{Z}_p$, compute:

$$sk_{x,t} := \mathcal{H}(x1t)^{\frac{\beta_1\rho_1}{a_t}} \cdot \mathcal{H}(x2t)^{\frac{\beta_2\rho_2}{a_t}} \cdot \mathcal{H}(x3t)^{\frac{\rho_1+\rho_2}{a_t}} \cdot g^{\frac{\sigma_x}{a_t}}. \quad (4)$$

Set $sk_x := (sk_{x,1}, sk_{x,2}, g^{-\sigma_x})$, again for $t = 1, 2$, where $\sigma' \leftarrow_R \mathbb{Z}_p$, compute:

$$sk'_t := g^{d_t} \cdot \mathcal{H}(011t)^{\frac{\beta_1\rho_1}{a_t}} \cdot \mathcal{H}(012t)^{\frac{\beta_2\rho_2}{a_t}} \cdot \mathcal{H}(013t)^{\frac{\rho_1+\rho_2}{a_t}} \cdot g^{\frac{\sigma'}{a_t}}. \quad (5)$$

Set $sk' = (sk'_1, sk'_2, g^{\delta_3}, g^{-\sigma'})$, server generates the secret key for a user as $(sk_0, \{sk_x\}_{x \in S}, sk')$.

Enc$(pk, (\mathbf{M}, \pi), m)$: server picks $s_1, s_2 \leftarrow_R \mathbb{Z}_p$ and generates:

$$c_0 := (H_1^{s_1}, H_2^{s_2}, h^{s_1+s_2}) \quad (6)$$

When the secret message m is split into shares using the MSP matrix $\mathbf{M}$, assuming $\mathbf{M}$ has n_1 rows and n_2 columns, such that $(\mathbf{M})_{i,j}$ denotes the (i, j)-th element of $\mathbf{M}$. Then, for $i = 1, \ldots, n_1$ and $\ell = 1, 2, 3$, calculate:

$$c_{i,\ell} := \mathcal{H}(\pi(i)\ell 1)^{s_1} \mathcal{H}(\pi(i)\ell 2)^{s_2} \cdot$$
$$\prod_{j=1}^{n_2} [\mathcal{H}(0j\ell 1)^{s_1} \cdot \mathcal{H}(0j\ell 2)^{s_2}]^{(\mathbf{M})_{i,j}}, \quad (7)$$

and set $c_i := (c_{i,1}, c_{i,2}, c_{i,3})$, $c' := T_1^{s_1} \cdot T_2^{s_2} \cdot m$. The ciphertext is $(c_0, c_1, \ldots, c_{n_1}, c')$.

Dec(pk, c, sk): if the set of attributes S in sk satisfies the MSP $(\mathbf{M}, \pi)$ in c, then there exist constants (i.e., coefficients) $\{\gamma_i\}_{i \in I}$ that satisfy equation $\sum_{i \in I} \gamma_i(\mathbf{M})_i = (1, 0, \ldots, 0)$. A user can decrypt the message m by computing z_1/z_2 ($sk_{0,1}$,

$sk_{0,2}$, $sk_{0,3}$ denote the first, second, and third elements of sk_0, which is same for c_0):

$$z_1 := c' \cdot e\left(\prod_{i \in I} c_{i,1}^{\gamma_i}, sk_{0,1}\right) \cdot e\left(\prod_{i \in I} c_{i,2}^{\gamma_i}, sk_{0,2}\right)$$
$$\cdot e\left(\prod_{i \in I} c_{i,3}^{\gamma_i}, sk_{0,3}\right), \quad (8)$$

$$z_2 := e\left(sk'_1, \prod_{i \in I} sk_{\pi(i),1}^{\gamma_i}, c_{0,1}\right) \cdot e\left(sk'_2, \prod_{i \in I} sk_{\pi(i),2}^{\gamma_i}, c_{0,2}\right)$$
$$\cdot e\left(sk'_3, \prod_{i \in I} sk_{\pi(i),3}^{\gamma_i}, c_{0,3}\right). \quad (9)$$

The plaintext m sent to the encryption process is an element of the target group. It is possible that, in reality, the data is too large to fit into a single $\mathbb{G}_T$ element, and it would be quite costly to disassemble the message and encrypt it using attribute-based encryption. To efficiently process large messages, one effective solution is to utilize the hash result of $T_1^{s_1} T_2^{s_2}$ as a symmetric session key. This key can then be utilized to efficiently encrypt the message using an ordinary symmetric encryption scheme, e.g., AES. Therefore, the computational cost of encrypting data of any size using this CP-ABE approach can be reduced to the expense of one single ABE encryption process.

D. Scheme Discussion

StarCast can support *backward secrecy* and *revocability*, ensuring that any new user cannot decrypt the ciphertext before joining the group. To accomplish this, the master key mk is updated before each new user joins. Additionally, the secret keys sk for all current legitimate users are regenerated. Member revocation is realized in a similar manner by updating the mk for all users, excluding those that need to be revoked.

Handling Dynamically Changing User Groups. StarCast is well-suited for the dynamic nature of LEO satellite communication, where the intended recipients (i.e., policies) of
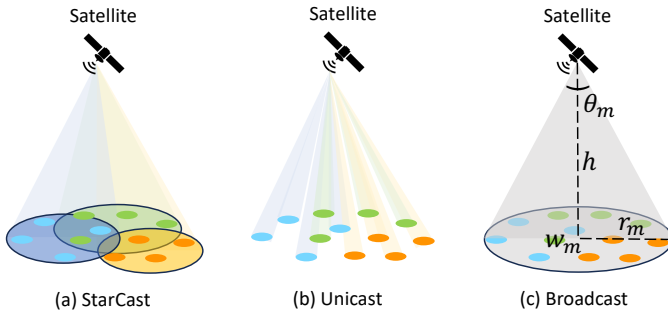
(a) StarCast   (b) Unicast   (c) Broadcast

Fig. 4. Comparison of StarCast, Unicast, and Broadcast Schemes for Secure Communication in LEO Satellite Networks

Fig. 5. StarCast Communication Test-Bed

different messages may change dynamically. The user's sk is valid for decrypting any ciphertext as long as the user's attributes satisfy the policy of that specific ciphertext. users do not need separate keys for each ciphertext; instead, they use the same attribute-based key across different policies, decrypting only those ciphertexts for which their attributes satisfy the policy. As long as a user's attributes have not changed, there is no need to update its sk, their secret key remains the same, regardless of how many different policies are used to encrypt different messages (for example, the access policy for a new encrypted data may become more restrictive or inclusive). The ability to decrypt one ciphertext does not affect the ability to decrypt another. Each ciphertext is evaluated independently based on its policy and the recipient's attributes.

V. EVALUATION

To evaluate the spectrum efficiency of our design, we compare the total data rate for legitimate users (those who meet the decryption policy for a specific ciphertext) across different secure LEO satellite communication methods. We prototype and evaluate the latency of StarCast using the Starlink LEO satellite network, and analyze the computational cost of the cryptographic scheme. Additionally, we compare the cost across conventional unicast encryption, broadcast encryption, and StarCast for secure LEO satellite group communications.

A. Total Data Rate from Legitimate Users

We consider the secure satellite communication schemes illustrated in Fig. 4 and follow our system model assumption. These users are grouped according to various information access privileges (as indicated by different colors). In a unicast framework (Fig. 4(b)), the satellite directs a narrow, focused beam to a single user. The broadcast framework (Fig. 4(c)) involves the satellite generating a wide beam that covers the entire geographical area. StarCast strikes a balance between the two (Fig. 4(a)), where the satellite generates beams of intermediate width, targeting specific groups of users with shared content.

To analyze the sum of legitimate users' data rates, we follow the performance evaluation model from [9]. We assume that the same group of users utilizes the line-of-sight path to

the satellite and requests the same content. Although satellite communication can support multiple beams simultaneously, we simplify the analysis by assuming that only one beam is used for transmission at any given time. The satellite provides communication services to a total of N users. They are grouped into M groups, and each group is served sequentially using time division. Let $\mathcal{G}_m$ represent the set of users in group m, where $m \in 1, 2, \ldots, M$, and the number of users in each group is given by $|\mathcal{G}_m|$, such that $\sum_{m=1}^{M} |\mathcal{G}_m| = N$. The number of groups M is determined by the information access privileges based on the attribute sets of the users. A beam sample is shown in Fig. 4(c), where $\mathbf{w}_m$ represents the coordinates of the center of the beam serving group m. The adjustable coverage radius of the beam for group m, denoted by r_m. Here, h represents the height of the satellite, and θ_m is the beam angle, expressed in degrees, which measures the direction in which the gain falls to half of its maximum. The beam coverage radius r_m is related to the beam angle θ_m by $r_m = h \tan\left(\frac{\theta_m}{2}\right)$.

The data rate C_i for user i is determined by the signal-to-noise ratio (SNR). The received power P_r^i can be calculated using the Friis transmission equation:

$$P_i^r = \frac{1}{2}\alpha G_i^t G^r P^t \left(\frac{\lambda}{4\pi h}\right)^2, \qquad (10)$$

where α is the power attenuation factor, G_i^t and G^r are the gains of the transmitter and receiver antennas, respectively, P^t is the transmitted power of the satellite, and λ is the wavelength. The transmitter antenna gain G_t^i is a function of the beamwidth θ_i and can be approximated as $G_i^t = \eta \left(\frac{70\pi}{\theta_i}\right)^2$, where η is the antenna efficiency, and θ_i is the beam angle. Suppose group $\mathcal{G}_m$ is the legitimate group, the sum of users' data rate can be expressed as:

$$C_m = \sum_{i=1}^{|\mathcal{G}_m|} B \log_2(1 + \frac{P_i^r}{N_0 B}), \qquad (11)$$

where B is the channel bandwidth, and N_0 is the noise power spectral density.

In comparing the sum of legitimate users' data rates of secure unicast, broadcast, and StarCast satellite transmission frameworks, we simulate the scheme with users distributed by
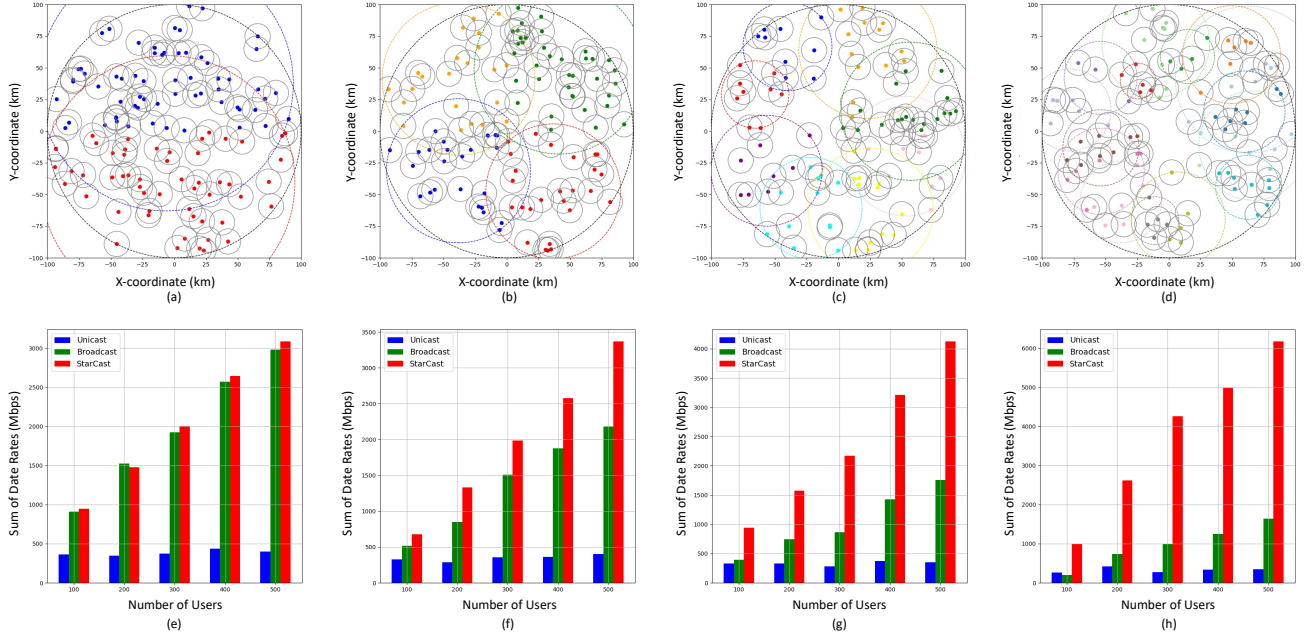
Fig. 6. User Grouping and Beam Coverage in a Satellite-Serviced Area: Visualizations with (a) 2 Groups of Users, (b) 4 Groups of Users, (c) 8 Groups of Users, and (d) 16 Groups of Users; Performance Comparison of Sum of Data Rates for Legitimate Users Across the Three Communication Methods for (e) 2 Groups of Users, (f) 4 Groups of Users, (g) 8 Groups of Users, and (h) 16 Groups of Users.
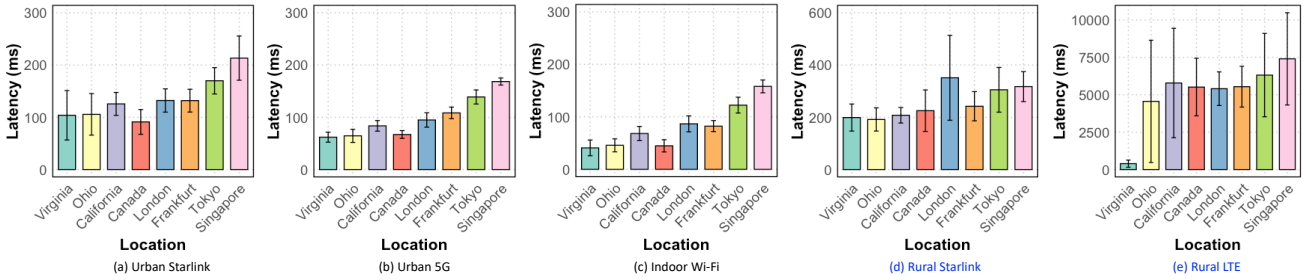

Fig. 7. Average ciphertext communication latency from eight AWS servers to the end device, with standard deviation samples indicated.

groups in the coverage of the satellite, and the channel between satellite and user is modeled as the Rician channel. The system parameters for a typical LEO satellite are summarized in Tab. II.

TABLE II
LEO SATELLITE SIMULATION PARAMETERS

Parameters	Values
The height of satellite h	550 km
The maximum beam coverage radius	100 km
Frequency Band	Ku (12 GHz)
Bandwidth B	1 GHz
Satellite power P^t	13 dBW
User terminal antenna gain G^r	30 dBi
The efficiency of the antenna η	0.7
Phased array antenna diameter D	0.5 m
Power attenuation α	1
AWGN power spectral density N_0	-174 dBm/Hz

Fig. 6 (a)-(d) illustrate the beam coverage and user grouping

scenarios for 2, 4, 8, and 16 groups of users, respectively, in a satellite-serviced area. Users are represented as colored dots corresponding to their groups, while the large black circle represents the broadcast beam coverage, the medium-sized circles denote the StarCast group communication beam coverage for each group, and the small gray circle indicates the unicast beam coverage area. As the number of user groups increases, the StarCast beam coverage becomes finer, improving beam directionality and targeting precision for legitimate groups.

In Fig. 6(e)-(h), the simulated results compare the total data rates for legitimate users across unicast, broadcast, and StarCast frameworks for 2, 4, 8, and 16 groups of users, respectively. Each individual figure depicts the total data rates for legitimate users across different communication frameworks as the number of users increases. The unicast approach, while capable of providing the highest individual data rates due to its narrow and highly focused beams (resulting in a high antenna gain G_t^i), often yields the lowest sum of data rates
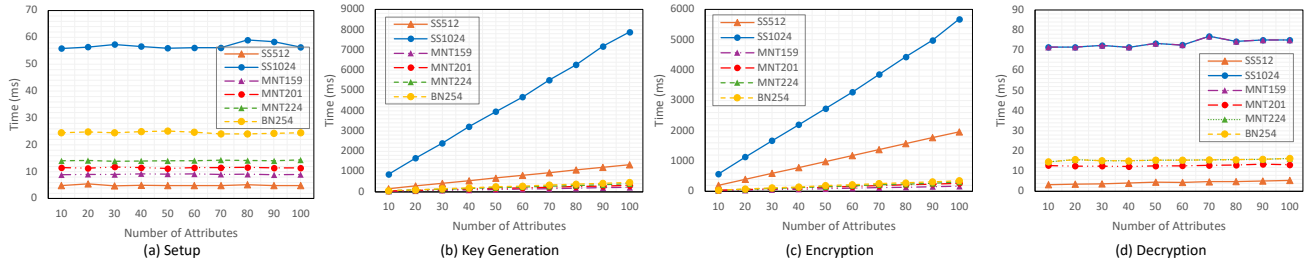
Fig. 8. Computation times for StarCast by (a) setup, (b) key generation, (c) encryption, and (d) decryption processes as the number of attributes increases.

for a group of legitimate users C_m. This inefficiency arises from the sequential time-sharing required to serve each user, leading to redundant transmissions of the encrypted content. Conversely, the broadcast framework delivers content to all users simultaneously by utilizing a wide beam with a large beamwidth θ_m. However, this method results in a lower C_m due to the reduced antenna gain G_t^m, as it must cover a broader area, which includes unintended users.

StarCast demonstrates its scalability and efficiency by adjusting the beamwidth θ_m to optimally target specific user groups. This method enables simultaneous delivery of encrypted data to all legitimate users within each group. As the number of groups increases, StarCast beams become finer, effectively enhancing signal strength and reducing interference. Consequently, the StarCast framework achieves the highest C_m among the three communication methods as the number of user groups increases. It also demonstrates the efficiency with the number of groups of users increasing. As shown in Fig. 6(e)-(h), the StarCast framework becomes increasingly efficient as the number of groups grows. While providing modest gains for 2 groups (Fig. 6(e)), it achieves significant performance improvements for 4, 8, and 16 groups (Fig. 6(f)-(h)), consistently outperforming unicast and broadcast in total data rates. This demonstrates the scalability and efficiency of StarCast in handling higher user densities within the group.

B. Prototyping and Evaluation of StarCast Latency Using Starlink LEO Satellite Communication

Currently, Starlink satellites with DTC capability only support emergency text services and are expected to support voice and IoT connections after 2025 [46]. Therefore, we developed a prototype of StarCast using the Starlink Gen 3 Standard Kit and its LEO satellite network as an example to test the latency of StarCast (see Fig. 5). We utilized a MacBook Pro (Apple M1 Pro Processor, 16 GB Memory) as an end device, connecting it to the Starlink antenna via a built-in WiFi signal. Additionally, we tested eight Amazon Web Services (AWS) virtual machines (free-tier EC2 instances with Ubuntu 22.04 Linux OS) as servers, located in Virginia, Ohio, California, Canada, London, Frankfurt, Tokyo, and Singapore, to evaluate the end-to-end latency of ciphertext communication. These servers transmitted ciphertext to our end device, which received the LEO communication link through the Starlink standard kit. To examine the impact of different environments

on the communication link, we deployed our Starlink antenna in both urban and rural areas. For comparison, we evaluated the performance of Starlink communication against other methods, including T-Mobile's 5G and LTE network services, as well as indoor WiFi, using the same AWS servers.

To establish a UDP broadcast session from an AWS server to a local device, we begin by creating a UDP socket on the AWS server using the `socket.socket(socket.AF_INET, socket.SOCK_DGRAM)` command. We enable the socket's broadcast capability by setting the `SO_BROADCAST` option with `setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)`. After configuring the socket, we send the encrypted data to the broadcast address via the `sendto` method. On the local device side, we similarly set up a UDP socket with the `SO_REUSEADDR` option enabled. This socket is then bound to listen on the same port as the server, and we use the `recvfrom` method to receive and process the broadcasted ciphertext. Although we implement the UDP broadcast on the Starlink network, the inherent limitation that Starlink does not physically support group communication in its current configuration means that our experimental results are based on an end-to-end session with a smaller beamwidth compared to a true group communication scenario. Therefore, our results are more representative of a situation where the legitimate group is geographically concentrated in a compact area.

Latency Evaluation. We first evaluate the communication latency from eight AWS servers to our end device located in an urban area, as shown in Fig. 7(a)-(c). The latency increases as the distance from the server location to the client increases, ranging from Virginia to Singapore. Fig. 7(a) presents the test results when the end device is connected to the Starlink antenna via a wireless signal. We observed that Starlink's latency is, on average, slightly higher than that of the 5G network and indoor WiFi, as depicted in Fig. 7(b)-(c). However, the variation in Starlink's latency is significantly greater than that of the 5G network and indoor WiFi. We repeated the same experimental setup in a rural environment, where Starlink communications achieved latency below 400 ms, as shown in Fig. 7(d). Notably, a latency spike occurs during communication from London, corresponding to a period when a connected satellite was moving away from

the local antenna, according to the Starlink Coverage Map. In this rural location, 5G networks were unavailable, and the only terrestrial wireless network service was a weak T-Mobile LTE signal. Fig. 7(e) shows that this unstable LTE signal exhibits significantly higher average latency and greater variation compared to other methods. In contrast, Starlink consistently provides reliable network service, even in rural areas.

C. Computation Evaluation

We implemented the StarCast schemes using Python 3.6 and the Charm 0.50 framework [47]. To assess the computation cost of StarCast, we conducted tests over elliptic curves of types SS512, SS1024, MNT159, MNT201, MNT224, and BN254, with the number of attributes ranging from 10 to 100. The experimental results are depicted in Fig. 8. Fig. 8(a) illustrates the time required for the setup algorithms of the CP-ABE schemes we implemented, with setup times consistently below 100 ms regardless of the number of attributes. Fig. 8(b) and (c) show that the key generation and encryption times scale linearly with the number of attributes, corroborating our cryptographic design. The decryption time, in Fig. 8(d) remains under 80 ms. This is because only a constant number of pairing operations are required.

D. Comparison of Encryption Efficiency Across Unicast, Broadcast, and StarCast Frameworks

Total Number of Ciphertexts. In a unicast framework, where a satellite directs a narrow beam to individual users, delivering a message to a group $\mathcal{G}_m$ requires $|\mathcal{G}_m|$ encrypted messages, as each user receives a unique ciphertext with E2EE encryption [13], [14]. In contrast, broadcast encryption requires only one ciphertext for all recipients, regardless of group size [15], [16]. Similarly, StarCast transmits a single encrypted message, but only users meeting the access policy can decrypt it.

Total Size of Ciphertexts. In unicast, each user receives a unique ciphertext, making the total size N times that of a single ciphertext with asymmetric encryption, where N is the number of users. For example, with RSA-256, the total size is $N \times 2048$ bits. Broadcast encryption [15] scales linearly with group size, as the group key is encrypted with each member's public key, resulting in a size of $N \times 2048$ bits plus overhead.

The StarCast framework, leveraging attribute-based encryption, keeps ciphertext size dependent only on the number of attributes. As discussed in Sec. IV-B, an access policy requires only a small set of attributes (e.g., three in our case). StarCast's ciphertext comprises three elements from group $\mathbb{G}$ per attribute and three from group $\mathbb{H}$, ensuring efficient scaling. For an elliptic curve MNT224, each $\mathbb{G}$ element is 224 bits, while each $\mathbb{H}$ element is 672 bits. Comparatively, CGW [19] requires two $\mathbb{G}$ and two $\mathbb{H}$ elements per attribute, leading to slightly larger ciphertexts, as $\mathbb{H}$ elements are three times the size of $\mathbb{G}$. Waters [18] and BSW [17] further increase ciphertext size, requiring an attribute-dependent number of elements in $\mathbb{G}$ and an additional element in $\mathbb{H}$.

Total Number of Encryption Keys. In unicast, N public keys are required, one per user. Similarly, broadcast encryption necessitates N keys, as the group key is encrypted with each user's public key. In contrast, StarCast requires only one public key for encryption, embedding the access policy in the ciphertext to determine eligible decryption users.

VI. Conclusion

In this paper, we introduce StarCast, a secure and efficient group encryption scheme designed to address the critical challenges of scalability, security, and spectrum efficiency in LEO satellite networks. By leveraging CP-ABE, StarCast enables fine-grained access control, simplifies key management, and supports simultaneous data transmission to multiple users within a beam. This approach provides better utilization of limited satellite spectrum resources while maintaining robust security features such as backward secrecy, revocability, and resistance to collusion attacks. Through our implementation and comparative evaluations against unicast and broadcast frameworks, we demonstrated StarCast's capability to significantly enhance the performance and efficiency of secure satellite communication systems. StarCast provides a scalable and reliable solution for supporting the growing connectivity demands in remote and underserved regions, laying the foundation for advanced applications in IoT, disaster recovery, and military communications.

VII. Acknowledgment

References

[1] J. Krause, "Non-terrestrial networks." https://www.3gpp.org/technologies/ntn-overview. Online; accessed December-2024.

[2] N. Heydarishahreza, T. Han, and N. Ansari, "Spectrum sharing and interference management for 6g leo satellite-terrestrial network integration," *IEEE Communications Surveys & Tutorials*, 2024.

[3] H. B. Pasandi, J. A. Fraire, S. Ratnasamy, and H. Rivano, "A survey on direct-to-device satellite communications: Advances, challenges, and prospects," in *LEO-NET'24: Proceedings of the 2nd International Workshop on LEO Networking and Communication*, pp. 7–12, ACM, 2024.

[4] Z. Xiao, J. Yang, T. Mao, C. Xu, R. Zhang, Z. Han, and X.-G. Xia, "Leo satellite access network (leo-san) towards 6g: Challenges and approaches," *IEEE Wireless Communications*, 2022.

[5] G. Curzi, D. Modenini, and P. Tortora, "Large constellations of small satellites: A survey of near future challenges and missions," *Aerospace*, vol. 7, no. 9, p. 133, 2020.

[6] H. Xie, Y. Zhan, G. Zeng, and X. Pan, "Leo mega-constellations for 6g global coverage: Challenges and opportunities," *IEEE Access*, vol. 9, pp. 164223–164244, 2021.

[7] Starlink, "Satellite technology." https://www.starlink.com/technology. Online; accessed December-2024.

[8] "DVB-S2X (Second Generation Satellite Extensions); DVB BlueBook A083-2r4 (Draft EN 302 307-2 V1.4.1)," tech. rep., DVB Project Office, 17a Ancienne Route CH-1218 Grand Saconnex, Geneva, 2024.

[9] B. Liu, C. Jiang, L. Kuang, and J. Lu, "Joint user grouping and beamwidth optimization for satellite multicast with phased array antennas," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2020.

[10] L. Yin and B. Clerckx, "Rate-splitting multiple access for multigroup multicast and multibeam satellite systems," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 976–990, 2020.

[11] Y. Yan, K. An, B. Zhang, W.-P. Zhu, G. Ding, and D. Guo, "Outage-constrained robust multigroup multicast beamforming for satellite-based internet of things coexisting with terrestrial networks," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8159–8172, 2020.

[12] X. Zhu, C. Jiang, L. Yin, L. Kuang, N. Ge, and J. Lu, "Cooperative multigroup multicast transmission in integrated terrestrial-satellite networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 5, pp. 981–992, 2018.

[13] N. Weiler, "Secure anonymous group infrastructure for common and future internet applications," in *Seventeenth Annual Computer Security Applications Conference*, pp. 401–410, IEEE, 2001.

[14] C. Grosch, "Framework for anonymity in ip-multicast environments," in *Globecom'00-IEEE. Global Telecommunications Conference. Conference Record (Cat. No. 00CH37137)*, vol. 1, pp. 365–369, IEEE, 2000.

[15] A. Barth, D. Boneh, and B. Waters, "Privacy in encrypted content distribution using private broadcast encryption," in *International conference on financial cryptography and data security*, pp. 52–64, Springer, 2006.

[16] A. Fiat and M. Naor, "Broadcast encryption," in *Advances in Cryptology—CRYPTO'93: 13th Annual International Cryptology Conference Santa Barbara, California, USA August 22–26, 1993 Proceedings 13*, pp. 480–491, Springer, 1994.

[17] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, pp. 321–334, IEEE, 2007.

[18] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International workshop on public key cryptography*, pp. 53–70, Springer, 2011.

[19] J. Chen, R. Gay, and H. Wee, "Improved dual system abe in prime-order groups via predicate encodings," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 595–624, Springer, 2015.

[20] S. Agrawal and M. Chase, "Fame: Fast attribute-based message encryption," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 665–682, 2017.

[21] D. Riepel and H. Wee, "Fabeo: Fast attribute-based encryption with optimal security," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2491–2504, 2022.

[22] L. Meng, L. Chen, Y. Tian, and M. Manulis, "Fabesa: Fast (and anonymous) attribute-based encryption under standard assumption," *Cryptology ePrint Archive*, 2024.

[23] L. Meng, L. Chen, Y. Tian, M. Manulis, and S. Liu, "Fease: Fast and expressive asymmetric searchable encryption.," *IACR Cryptol. ePrint Arch.*, vol. 2024, p. 54, 2024.

[24] J.-C. Liou and N. L. Johnson, "Instability of the present leo satellite populations," *Advances in Space Research*, vol. 41, no. 7, pp. 1046–1053, 2008.

[25] ITU, "Population of global offline continues steady decline to 2.6 billion people in 2023." https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx. Online; accessed December-2024.

[26] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, *et al.*, "Satellite communications in the new space era: A survey and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, 2020.

[27] Y. Zou, Y. Long, S. Gong, D. T. Hoang, W. Liu, W. Cheng, and D. Niyato, "Robust beamforming optimization for self-sustainable intelligent reflecting surface assisted wireless networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 2, pp. 856–870, 2021.

[28] T. Van Chien, E. Lagunas, T. H. Ta, S. Chatzinotas, and B. Ottersten, "User scheduling and power allocation for precoded multi-beam high throughput satellite systems with individual quality of service constraints," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 1, pp. 907–923, 2022.

[29] W. Wang, L. Gao, R. Ding, J. Lei, L. You, C. A. Chan, and X. Gao, "Resource efficiency optimization for robust beamforming in multi-beam satellite communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 6958–6968, 2021.

[30] C. Du, H. Yu, Y. Xiao, Y. T. Hou, A. D. Keromytis, and W. Lou, "{UCBlocker}: Unwanted call blocking using anonymous authentica-tion," in *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 445–462, 2023.

[31] H. Yu, C. Du, Y. Xiao, A. Keromytis, C. Wang, R. Gazda, Y. T. Hou, and W. Lou, "Aaka: An anti-tracking cellular authentication scheme leveraging anonymous credentials," in *Network and Distributed System Security Symposium (NDSS)*, 2023.

[32] C. Du, H. Yu, Y. Xiao, W. Lou, C. Wang, R. Gazda, and Y. T. Hou, "Mobile tracking in 5g and beyond networks: Problems, challenges, and new directions," in *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pp. 426–434, IEEE, 2022.

[33] S. Li, S. Shi, Y. Xiao, C. Zhang, Y. T. Hou, and W. Lou, "Bijack: Breaking bitcoin network with tcp vulnerabilities," in *European Symposium on Research in Computer Security*, pp. 306–326, Springer, 2023.

[34] C. Zhang, N. Wang, S. Shi, C. Du, W. Lou, and Y. T. Hou, "Mindfl: Mitigating the impact of imbalanced and noisy-labeled data in federated learning with quality and fairness-aware client selection," in *MILCOM 2023-2023 IEEE Military Communications Conference (MILCOM)*, pp. 331–338, IEEE, 2023.

[35] C. Zhang, S. Shi, N. Wang, X. Xu, S. Li, L. Zheng, R. Marchany, M. Gardner, Y. T. Hou, and W. Lou, "Hermes: Boosting the performance of machine-learning-based intrusion detection system through geometric feature learning," in *Proceedings of the Twenty-fifth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, pp. 251–260, 2024.

[36] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, p. 109246, 2022.

[37] Y. Liu, L. Ni, and M. Peng, "A secure and efficient authentication protocol for satellite-terrestrial networks," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5810–5822, 2022.

[38] A. Godhwani, M. Murfield, T. Delaney, K.-S. Fong, P. Browne, and S. Hryckiewicz, "The use of pki in next generation uhf satcom," in *2011-MILCOM 2011 Military Communications Conference*, pp. 1733–1738, IEEE, 2011.

[39] H. Yu, C. Zhang, and H. Jiang, "A fpga-based heterogeneous implementation of ntruencrypt," in *Advances in Parallel & Distributed Processing, and Applications: Proceedings from PDPTA'20, CSC'20, MSV'20, and GCC'20*, pp. 461–475, Springer, 2021.

[40] C. Zhang, H. Yu, Y. Zhou, and H. Jiang, "High-performance and energy-efficient fpga-gpu-cpu heterogeneous system implementation," in *Advances in Parallel & Distributed Processing, and Applications: Proceedings from PDPTA'20, CSC'20, MSV'20, and GCC'20*, pp. 477–492, Springer, 2021.

[41] K. Fan, C. Zhang, R. Shan, H. Yu, and H. Jiang, "Gpu acceleration of ciphertext-policy attribute-based encryption," in *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, pp. 94–101, IEEE, 2019.

[42] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, pp. 457–473, Springer, 2005.

[43] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*, pp. 62–91, Springer, 2010.

[44] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 463–474, 2013.

[45] A. Lewko and B. Waters, "Unbounded hibe and attribute-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 547–567, Springer, 2011.

[46] Starlink, "Starlink direct to cell." https://www.starlink.com/business/direct-to-cell. Online; accessed December-2024.

[47] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," *Journal of Cryptographic Engineering*, vol. 3, pp. 111–128, 2013.