Hindawi
Security and Communication Networks
Volume 2021, Article ID 5599996, 14 pages
https://doi.org/10.1155/2021/5599996

Research Article

Data Distribution for Multiple Receivers in a Connected Car Environment Using 5G Communication

Won-Bin Kim,[1] Daehee Seo,[2] Donghyun Kim,[3] and Im-Yeong Lee[1]

[1]*Department of Software Convergence, Soonchunhyang University, Asan-si 31538, Republic of Korea*
[2]*Faculty of Artificial Intelligence and Data Engineering, Sangmyung University, Seoul 03016, Republic of Korea*
[3]*Department of Computer Science, Georgia State University, Atlanta, GA 30303, USA*

Correspondence should be addressed to Im-Yeong Lee; imylee@sch.ac.kr

Received 23 January 2021; Accepted 26 May 2021; Published 12 June 2021

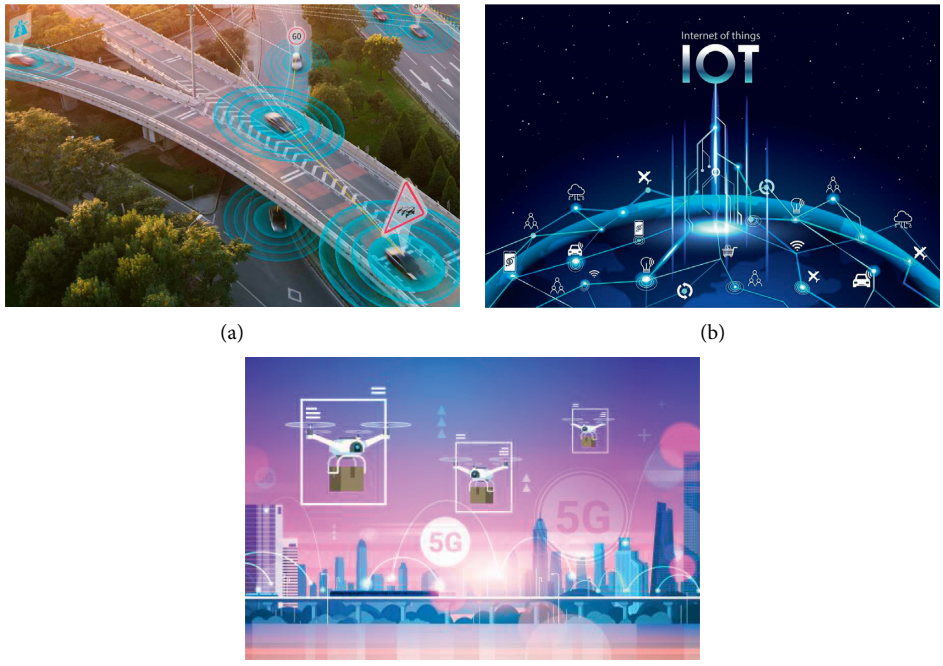
Academic Editor: Jinwei Wang

The development of communication technology has brought changes to various environments. The evolution from 3G to 4G Long-Term Evolution (LTE) was mainly aimed at improving communication speed. However, the evolution from 4G LTE to 5G New Radio (NR) is not aimed at improving speed alone. In addition to the existing communication types, 5G aims to improve communication to support the Internet of Things (IoT), media, and complex content to which things are connected. In such environments, point-to-point communication has a very inefficient structure to allow content providers to transmit data to many content users. In the 5G era, content providers must distribute content to numerous users, and in this process, they need to protect the content. Multireceiver encryption (MRE) is an encryption technology developed for this purpose. MRE allows multiple recipients to decrypt data using their own private key with single encryption of a data provider. With this technology, even if the number of data recipients is 100,000 or 1,000,000, data can be distributed with single encryption. Therefore, while using the existing 1 : 1 encryption method, it is possible to solve the problem of inefficiency in performing encryption for each recipient. However, existing proposed MREs can cause key escrow problems and partial key verification problems. Furthermore, the privacy issues identifying the recipient may arise because anonymity is not available to the recipient. In addition, it is necessary to ensure a fair decryption process for all recipients which a legitimate user cannot decrypt. In this study, we attempted to address these problems, and through our model, it is possible to distribute the data more securely and efficiently in a 5G environment.

1. Introduction

Mobile communication technology has changed significantly in our lifetime. Since the development of the first mobile communication technology, it has undergone various changes, from the previous generations to the current 5th generation communication. As mobile communication technology supports the transmission of digital data beyond simple voice transmission, it is possible to perform tremendous functions using a cellular terminal represented by a smartphone.

The evolution of the Internet has made daily life more convenient and made it possible to communicate through mobile devices anytime, anywhere. Mobile communication technology is at the center of this change and is currently in its fifth generation. 5G NR communication (hereafter referred to as 5G), which was first commercialized in 2018, is designed to support future technologies beyond the limitations of the existing 4G Long-Term Evolution (LTE). Rapidly emerging technologies, such as the Internet of Things (IoT), autonomous vehicles, and Virtual Reality (VR), are extensively large that they are insufficiently covered by conventional 4G LTE in terms of the number of connected devices, amount of transmitted data, and delay speed as shown in Figure 1. According to the Ericsson-LG report, the number of IoT devices is expected to reach 28 billion by 2021. In addition, 4 TB data is transmitted per day for autonomous vehicles, and approximately 1 GB data per minute is required for 8K VR content. Therefore, it is difficult to provide smooth services with 4G LTE, and 5G is



(a) (b)

(c)

Figure 1: Examples of 5G communication.

being developed to provide increasingly diverse services in a stable manner.

5G is developed to communicate quickly and reliably with a large number of devices. Considering IoT and autonomous vehicles (including Vehicle-To-Everything (V2X)), which are representative services to which 5G is applied, a large number of devices can communicate with each other. It can be observed that communication among multiple devices is one of the representative characteristics of 5G. In addition, it is possible to service technologies directly connected to life and security, such as military drones, implantable medical devices, and transportation systems. Therefore, communication security must also be guaranteed. As a result, to provide a 5G service, a technology is required that can safely and efficiently transmit data to multiple recipients (devices).

Data encryption technology prevents the transmission of data to third parties who do not have permission to view it [1–4]. In general, data encryption technology uses public key encryption and symmetric key encryption; therefore, a third party without a decryption key cannot decipher the contents of the data. However, a common encryption method is a 1 : 1 communication between the sender and receiver. Therefore, to provide the same data to multiple recipients (devices) in services such as IoT and autonomous vehicles in a 5G environment through this format, the number of encryptions that must be performed for each recipient is equal to the number of recipients. This leads to an increase in processing speed and latency, along with an increase in the data processing cost. Therefore, to solve this problem, an encryption method is required that allows multiple recipients to decrypt data with only one encryption. Multireceiver Encryption (MRE) is a suitable encryption technology in such environments. MRE allows each recipient to decrypt data using their own private key if the data owner uses the public keys and IDs of multiple recipients to secure data only once. Therefore, the data sender need not encrypt multiple times even if the number of recipients increases, thereby leading to efficient data distribution. Therefore, by using MRE, it is easy to distribute data to multiple users in 5G environments.

However, different 5G based-technologies have different requirements depending on the purpose and application method. For example, a remote drone control system controls multiple drones with a limited amount of power, and there is no need for frequent communication outside of the origin and destination. Therefore, an encryption method with low computation power is suitable. In addition, the encryption applied to a smart metering system transmits only a small amount of data at a low frequency. However, as power is always supplied, there is no need to apply a lightweight encryption method. However, in the case of a connected car, a large amount of data must be transmitted at a high speed, and the data regarding the surrounding environment must be transmitted to all vehicles and transportation systems. Thus, an appropriate encryption method is required. In this study, we considered separate requirements for various applications. As a result, an environment for distributing encrypted data to multiple recipients is set to ensure quick and safe application of a large amount of data in a connected car environment. In addition, we set the requirements, developed a system model in the relevant environment, and proceeded to design and analyze the MRE for a safe and efficient data cannon in a connected car environment using 5G.

2. Related Works

In this section, we discuss the existing literature as it can enhance the understanding of the contents of this study.

2.1. 5G Communication. 5G communication technology has been developed by supplementing the limitations of 4G LTE as a fifth-generation mobile communication technology. 5G communication is designed to support emerging technologies such as IoT, VR, and smart cars (or connected cars). Therefore, it is faster, more stable, and able to communicate with more devices at the same time with lower latency compared with existing mobile communication technologies. When utilizing the characteristics of 5G communication in a drone, diverse tasks such as delivery, monitoring, and rescue support can be carried out by remotely controlling multiple drones as shown in Figure 2. In addition, it is possible to establish a safer and more convenient transportation system by interacting with autonomous/remote driving vehicles and real-time road traffic conditions, and this has been a long-standing goal of humanity. Furthermore, using next-generation content technologies such as VR, it is possible to provide various services through the use of immersive content and combination with mobile devices. 5G communication can provide more complex and high-level services because it can transmit a larger amount of data compared to a reference time while extending from the existing unicast communication environment to multicast and broadcast services.

5G communication can ensure more reliable communication with a larger number of devices at the same time. Therefore, it is possible to control multiple devices at the same time to perform more tasks within a limited time. A typical example is drone control. In the drone industry, 5G plays a key role by controlling multiple drones simultaneously. Services using these industrial drones include drone delivery, which is currently being developed by Amazon. As these services require control of a large number of drones at the same time, a technology is required that can control drones in a stable manner. Another example is intelligent transportation systems. These include not only autonomous vehicles but also V2X technologies such as vehicle-to-vehicle communication and vehicle-to-road side unit (RSU) communication. As such intelligent transportation systems need to process and transmit data generated from numerous sensors and equipment mounted on a vehicle, stable communication is required between numerous vehicles and RSUs. As the technology gradually improves, more machines will interact, and more tasks will be possible. However, as an increasing number of machines are being used in daily life, these machines can be exploited for nefarious purposes to take unfair advantage or threaten life. For example, it is possible to hack drone communications to steal items being delivered or to create a threat to life using drones. In the case of vehicles, there is a greater risk to life. Therefore, for a wider area of 5G usage, there is more emphasis on the safety of communication.

2.2. Certificateless Public Key Cryptography. The public key encryption method basically consists of a public key and a private key pair. Users can use the public key encryption system by revealing the secret private key and the public key corresponding to the private key. The initial public key encryption method was a Public Key Infrastructure (PKI) structure that proved that it was the owner of an individual corresponding to the public key by registering a certificate for a public key with a Certificate Authority (CA). However, in the PKI method, the process of generating, registering, and managing certificates is complicated, and a large cost is incurred. To solve this problem, ID-based Cryptography (IBC) was proposed by Adi Shamir in 1984 as shown in Figure 3 [5]. IBC is a technology that does not use a certificate, which is a disadvantage of the PKI method but uses the unique identity information (domain address, unique number, etc.) of a user as a public key. Therefore, the public key of a user is used as a tool to verify the user's identity. In addition, IBC receives a private key by registering the public key of a user in the Key Generation Center (KGC). However, this causes a key escrow problem in which the KGC knows the private keys of all users. Finally, various studies have been conducted to solve the key escrow problem, and certificateless public key cryptography (CL-PKC) has appeared.

CL-PKC overcame the key escrow problem of IBC with the method proposed by Al-Riyami and Paterson in 2003 [6]. CL-PKC generates a key using unique identity information similar to the existing IBC. However, the KGC does not issue the complete private key of a user but rather a part of the private key of each user. Specifically, a partial private key of each user is issued by using their unique identity information, and the user uses the private key by selecting and adding a secret value to the partial private key. Therefore, the key escrow problem does not occur because the KGC cannot know the complete private key. However, in recent years, additional security problems such as public key substitution attacks and partial private key verification problems have been highlighted, and various studies are being conducted.

2.3. Multireceiver Encryption. MRE is a cryptographic primitive and is a technology that can deliver the same message to multiple recipients with single encryption. MRE has been conducted in various studies based on the form of designating multiple recipients using their public keys by taking advantage of IBC, as shown in Figures 3 and 4 [7–22]. However, in the MRE method, an issue of identifying the recipient has been raised. This has occurred because the information that can specify the recipient can be extracted from the value included in the ciphertext. To solve this problem, Fan et al. [23] proposed a scheme using a Lagrange interpolation polynomial. This scheme used a method of polynomiating the information of the recipient such that their identity could not be directly extracted, and it was argued that the identity of the recipient was not disclosed to anyone. However, several studies, such as Wang et al.'s study, have demonstrated that the recipient can acquire the identity of another recipient [23–25]. Accordingly, Fan et al.

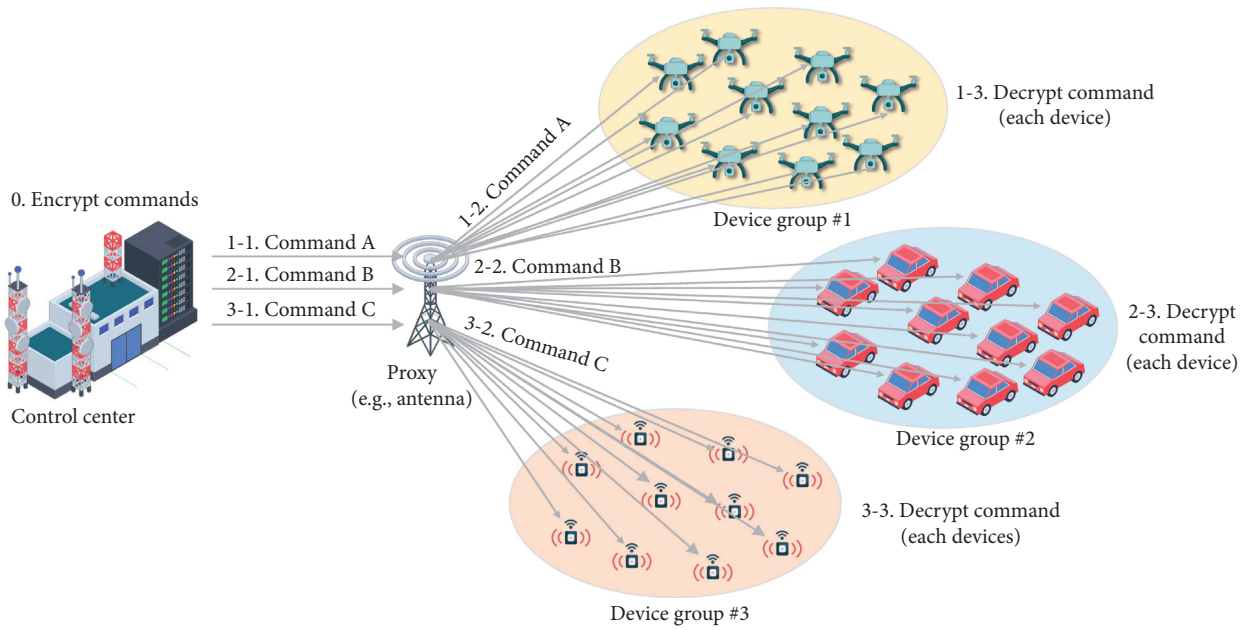


Figure 2: Data distribution in the 5G environment.

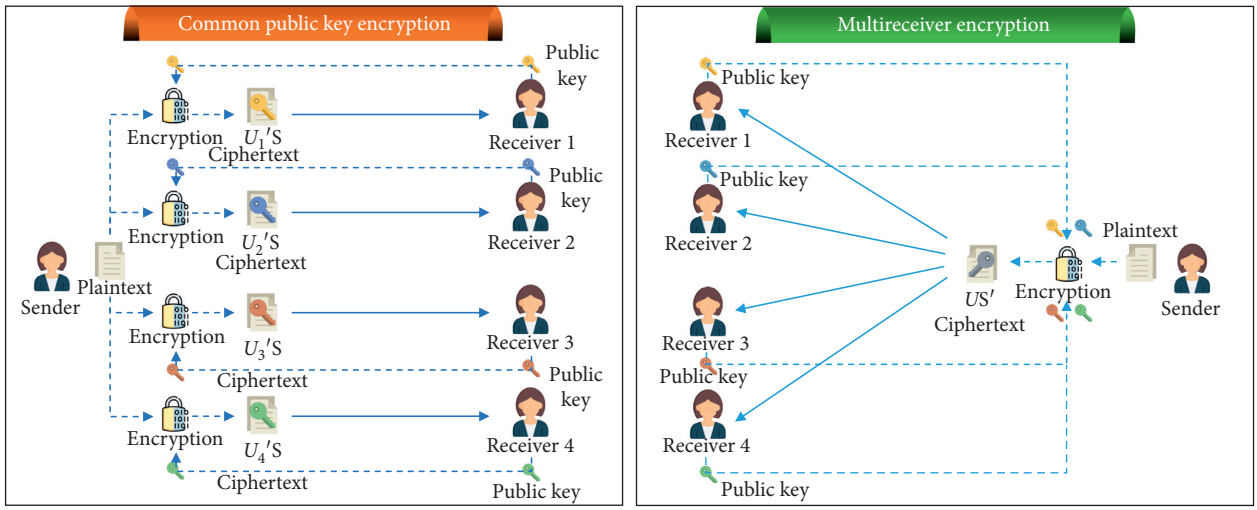


Figure 3: Comparison with common PKE and MRE.

[26] proposed an improved scheme. Later, Zhang and Takagi [27] proposed a scheme that provided anonymity for both the sender and receiver. However, Zhang and Mao [28] revealed that anonymity was not perfect in this scheme as well, and a new ID-based MRE (IBMRE) was proposed.

Since the first MRE was introduced, various MREs using IBC have been studied. However, with the rise of the key escrow problem in IBC, a study was conducted to apply CL-PKC to replace IBC in MRE. Sur et al. [29] improved the implicit certificate-based IBMRE proposed in 2007 and proposed certificateless MRE (CL-MRE) in 2011 [30]. In addition, many researchers have proposed CL-MRE, but confidentiality and anonymity have not been proven in the Oracle model. Subsequently, Hafizul et al. [31] first proposed CL-MRE, which proved confidentiality and anonymity in a random Oracle model. Later, Hung et al. [32] pointed out that the method of Hafizul et al. [31] involved a large amount of computation. Accordingly, they proposed CL-MRE using double-linear pairing with improved association efficiency. However, their method also encountered a problem such that the map-to-point (MTP) hash operation, which required considerable operation time, increased linearly with the number of users. He et al. [33] proposed a CL-MRE scheme that did not use double-linear pairing and MTP operation to solve the problem of Hung et al. Gao et al. [34] proposed a method that does not use bilinear pairing, which takes a lot of computation time. However, because it is not possible to verify whether the sender is a registered user in KGC, an attack by an outsider is possible. Deng [35] and Zhu [36] also proposed a method to solve the key escrow problem, but many operations occur using bilinear pairing, and Zhu et al. cannot provide receiver anonymity. Win et al.

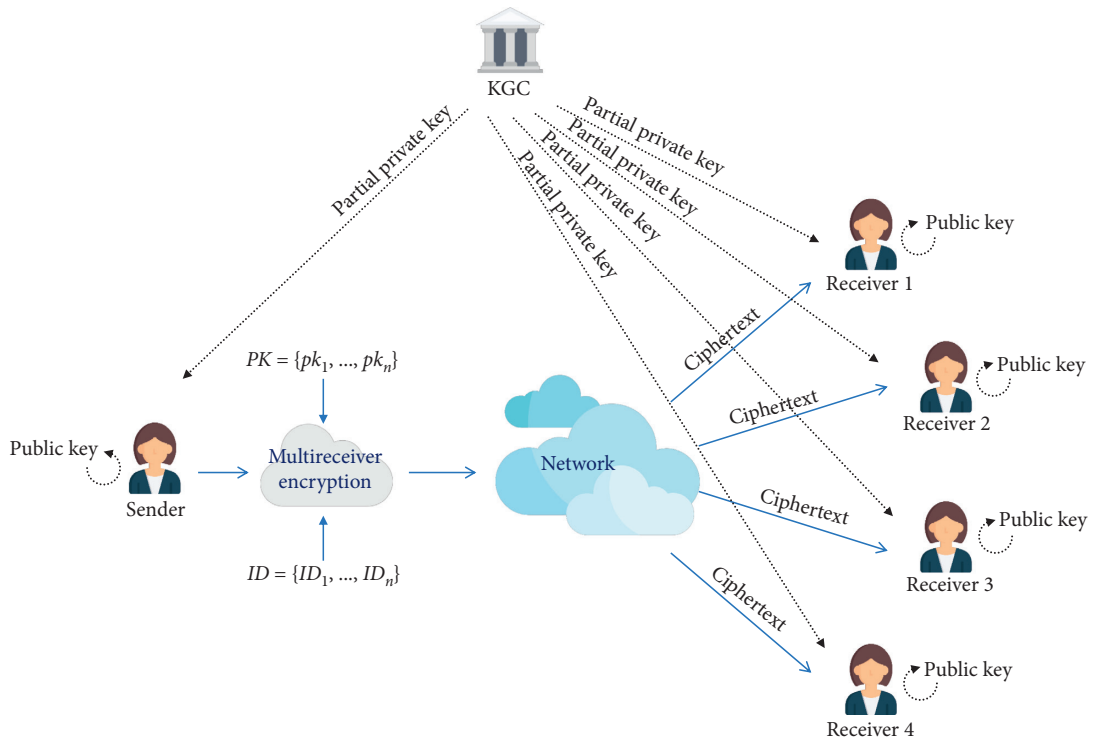


Figure 4: Basic form of MRE.

[37] proposed a method that does not use double-linear pairing but does not provide receiver anonymity and decryption fairness. Wang et al. [38] used bilinear pairing and did not provide partial key verification.

3. Preliminaries

In this section, the system model that is the background of this study is set up. Therefore, the role of the object participating in this model is defined and security requirements are set.

3.1. System Model. Participating objects in this study can be classified into three categories, and the overall form is shown in Figure 5. Among them, the sender and receiver are objects included in the user and may be senders with fixed roles depending on the system environment, and any of the users may be senders. A detailed description of this is as follows:

(i) KGC: in this proposed model environment, KGC can be an organization that manages all transportation systems. For example, it may be the National Highway Traffic Safety Administration (NHTSA) of the United States, and a third party authorized to do so may play a role. Since KGC manages all users within the system, KGC creates common public parameters for the system and makes it possible to use the system by generating partial private keys at the user's request. As the KGC is a semitrusted participant and has the property of honest-but-curious, it responds honestly to user requests. However, there is a possibility of privacy leakage.

(ii) Users (sender and receivers): in this proposed environment, the user basically includes both the sender and the receiver. However, a designated sender may exist separately depending on the application environment as shown in Figure 6. First, if the role of the sender is not fixed, the sender may be all vehicles and transportation equipment (RSU, etc.) in a connected car environment. On the other hand, in the case of an environment in which the role of the sender is fixed, the sender plays the role of the sender by the entity that generally manages the transport system, not the end user, such as a traffic control center or RSU.

All users must obtain a partial private key from the KGC to use the system provided by the KGC. Users who have issued a partial private key can create and disclose their public key. In addition, any user can act as a sender or receiver. The user assuming the sender role must know the public key of the user who becomes the receiver to generate a ciphertext for that user.

(iii) Sender (traffic control devices or vehicles): a sender refers to a user who sends data among users. One sender can designate multiple receivers, and the public keys of all receivers are required to generate ciphertext for multiple receivers. CL-MRE can deliver ciphertext to multiple receivers with a single encryption operation such that, for multiple receivers, it can process more efficiently than general public key encryption.

(iv) Receiver (vehicles): a receiver is a user who receives data from a sender. In this environment, the

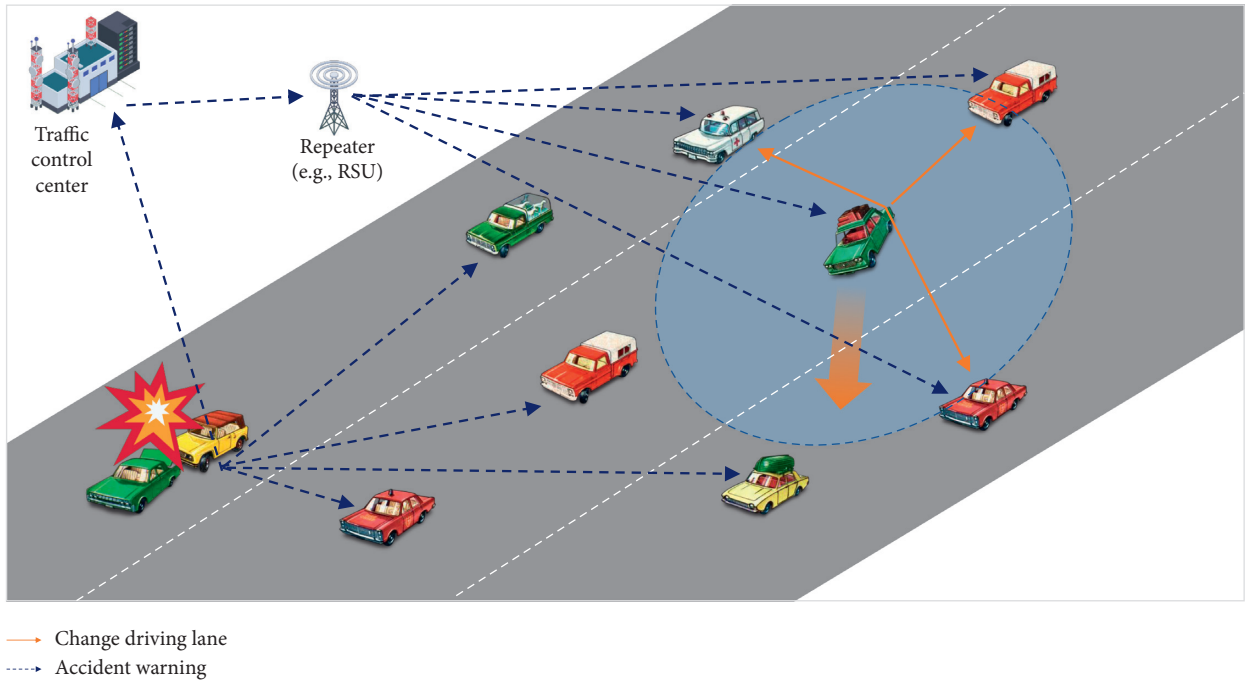


Figure 5: Example of the system model environment.

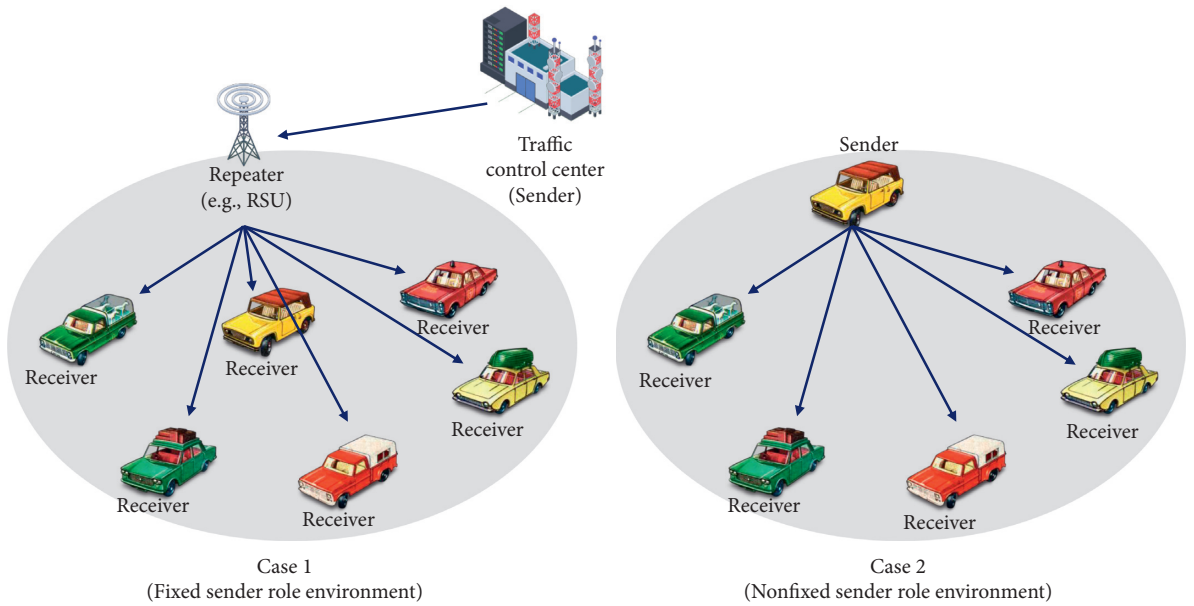


Figure 6: Cases of the sender role.

connected car used by the end user is applicable, and it receives data from a traffic control center or RSU or receives data from another vehicle depending on the application environment. The receiver reveals the public key after completing the key generation process. Thereafter, when the user receives the ciphertext included in the recipient list, the ciphertext can be decrypted with the private key and public key. In this process, the receiver cannot identify other receivers, and other ciphertexts that are not designated as targets cannot be decrypted.

3.2. Formal Definition. This section describes the formal definition of the algorithm used in this study. This section describes the formal definition of the algorithm used in this study. This study is largely divided into four parts (setup phase, key generation phase, data generation phase, and data

receiving phase), and in detail, it consists of a total of seven algorithms, which are as follows:

(i) Setup: this algorithm begins by selecting and entering the security parameter λ. The public parameter params and master secret key are generated by the semitrusted participant KGC, and some of them are distributed by the KGC. Distributed params are used by system participants at all phases.

(ii) Partial-Private-Key-Extract: this algorithm is executed by the KGC according to the input of user i's identity ID_i. The PKG computes the corresponding partial private key s_i using the master private key and delivers it to user i.

(iii) Set-Secret-Value: this algorithm allows users to directly generate their own secret information by using the user's own identity, the ID_i.

(iv) Set-Private-Key: this algorithm is executed by the user i with identity ID_i. It considers $(\mathrm{params}, s_i, t_i)$ as the input and returns the full private key sk_i to user i as the output.

(v) Set-Public-Key: this algorithm is executed by the user i himself/herself to generate his/her public key pk_i according to his/her secret value t_i.

(vi) Multiencryption: this is the Probabilistic Polynomial Time (PPT) algorithm. The sender executes this algorithm to generate a ciphertext for the message m by identities and the public parameters of selected receivers.

(vii) Multidecryption: a selected receiver runs this algorithm to decrypt the received ciphertext using the full private key of the receiver.

3.3. Security Requirements. This section describes the requirements of the system model of this study. There are seven security requirements, and a detailed description of each requirement is as follows:

(i) Confidentiality: the contents of the transmitted data must not be known except by the designated recipient. In addition, the recipients included in the recipient list must be able to know the contents of the data using their own private key.

(ii) Integrity: data transmitted from the sender to the receiver must not be altered due to the intervention of a third party or problems in the communication path during the transmission process. If data changes, legitimate users must know.

(iii) Key escrow problem: in a public key-based encryption environment, the KGC generates individuals who respond to the public key of the user. However, the KGC should not be able to use the private key of the user that it has created and kept to exercise the rights of the user.

(iv) Partial key verifiability: the user must be able to verify whether the partial private key issued from the KGC is the correct partial private key.

(v) Receiver anonymity: the legitimate recipients included in the recipient list must not be able to identify third parties other than themselves through the encrypted message. Therefore, in the process of determining whether the recipient is a recipient, it should not be possible to distinguish or specify data including the identity information of other recipients.

(vi) Decryption fairness: a legitimate user included in the recipient list must not be interrupted by other recipients or third parties in the decryption process. Therefore, it is necessary to prevent the data being transmitted from being modulated or partially missing, making decoding impossible in a proper way.

(vi) Participant verifiability: in general MRE, the sender's key is not entered during the encryption process. Therefore, the sender cannot be identified, and a user outside the system can transmit malicious data to a user inside the system. This has both advantages and disadvantages from many perspectives. However, in an environment such as this study, it is safe to ensure that data can only be distributed among users inside the system. So you can add a signature or use a method like signcryption. However, these methods require a lot of operations, and the sender has the burden of performing a signature with his or her own key.

4. Secure Multireceiver Data Distribution for the Connected Car System

In this chapter, based on the system model presented in Section 3, we design a safe data transmission method for a connected car environment using 5G. To this end, a system model is designed, security requirements are set, and a method suitable for the system model is proposed.

4.1. System Parameters. The following are the system parameters used in this proposed scheme:

(i) *: participants (KGC, sender, and receiver)

(ii) E: elliptic curve

(iii) p, q: λ-bit prime integer

(iv) l_1, l_2: λ-bit integer

(v) G: additive group on elliptic curve E

(vi) G_q: subgroup of G with prime order q

(vii) d: randomly selected master key, $d \in Z_q^*$

(viii) params: KGC's system public parameters

(ix) sk_i: participant i's private key

(x) pk_i: participant i's public key

(xi) m: plaintext

(xii) CT: ciphertext

(xiii) H_1: one-way hash function, $\{0,1\}^* \longrightarrow Z_q^*$

(xiv) H_2: one-way hash function, $\{0,1\}^* \longrightarrow Z_q^*$

(xv) H_3: one-way hash function, $\{0,1\}^* \longrightarrow Z_q^*$

(xvi) H_4: one-way hash function, $\{0,1\}^* \longrightarrow \{0,1\}^{l_1+l_2}$

4.2. Proposed Scheme for the 5G Connected Car System Environment. In this section, the CL-MRE proposed in Section 3 is applied to the 5G connected car system environment and specified. The overall flow of this is shown in Figure 7.

4.2.1. Setup Phase. In this step, KGC creates a secret light disclosure parameter for the proposed CL-MRE data distribution.

(i) Setup: with the given security parameter λ, this algorithm is executed by KGC to generate the system's parameters. The following steps will be implemented KGC in this algorithm:

(1) Choose two λ-bit prime integers p, q, two λ-bit integers l_1, l_2, and an elliptic curve E defined on F_p. Let G be the additive group on elliptic curve E and G_q be the subgroup of G with prime order q.

(2) Select randomly a generator $P \in G_q$.

(3) Randomly choose $d \in Z_q^*$ as the master key and $P_{\text{pub}} = d \cdot P$.

(4) Select four secure one-way hash functions are follows: H_i: $\{0,1\}^* \longrightarrow Z_q^*$ $(i = 1, 2, 3)$, H_4: $\{0,1\}^* \longrightarrow \{0,1\}^{l_1+l_2}$.

(5) Publish system's public parameters params = $\{p, q, l_1, l_2, E, G, G_q, P, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$ and message space $M = \{0,1\}^{l_1}$.

4.2.2. Key Generation Phase. In this phase, the process of generating private and public keys for each receiver device are included as shown in Figure 8.

(i) Set-Secret-Value: a user i with ID_i randomly selects $t_i \in Z_q^*$ as his or her secret value and computes $T_i = t_i \cdot P$ as the corresponding public key, and user i sends (T_i, ID_i) to KGC.

(ii) Partial-Private-Key-Extract: according to the identity ID_i of receiver i, the KGC performs the following steps:

(1) Randomly select $r_i \in Z_q^*$ and compute $R_i = r_i \cdot P$

(2) Calculate $k_i = r_i + \text{d}H_1(R_i + T_i, \text{ID}_i) + H_1(\text{d}T_i + \text{ID}_i) (\text{mod}P)$

(3) Calculate $j_i = d + r_i H_1(R_i + T_i, \text{ID}_i) + H_1(\text{d}T_i + \text{ID}_i) (\text{mod}P)$

(4) After that, R_i, j_i, and k_i are delivered to receiver i through the public channel

(iii) Set-Private-Key: after receiving R_i, j_i, and s_i from KGC, the user i verifies these. If verification passes, user i computes private key $\text{sk}_i = (s_i, t_i)$ as in the following steps:

(1) Verify whether the equation: $k_i \cdot P = R_i + H_1(R_i + T_i, \text{ID}_i) P_{\text{Pub}} + H_1(t_i P_{\text{Pub}}, \text{ID}_i) P$. $j_i \cdot P = P_{\text{Pub}} + R_i + H_1(R_i + T_i, \text{ID}_i) + H_1(t_i P_{\text{Pub}}, \text{ID}_i) P$

(2) If yes, compute $s_i = k_i - H_1(t_i P_{\text{Pub}}, \text{ID}_i)$ and $h_i = j_i - H_1(t_i P_{\text{Pub}}, \text{ID}_i)$

(3) After that, user i keeps secret $\text{sk}_i = (s_i, t_i, h_i)$ as his or her full private

(iv) Set-Public-Key: user i keeps $\text{pk}_i = (R_i, T_i)$ as the full public key.

4.2.3. Data Generation Phase. In this phase, the sender of the data specifies the recipient of the data and generates a ciphertext using the recipient's public key as shown in Figure 9.

(i) Multiencryption: this algorithm is executed by sender to generate a ciphertext for given message m and list of selected receivers i with identity ID_i $(1 \le i \le n)$, respectively. The following steps will be performed in this algorithm:

(1) Compute $w = H_1(R_{\text{sender}} + T_{\text{sender}}, \text{ID}_{\text{sender}})$ and given message $m \in M$. Calculate $z = H_2(m, w)$ and $Z = zP$.

(2) Compute $U_i = z \cdot (R_i + H_1(R_i + T_i, \text{ID}_i) P_{\text{pub}} + T_i)$ and $\mu_i = H_3(U_i, w, \text{ID}_i)$, where $i = 1, 2, \ldots, n$.

(3) Randomly select $\theta \in Z_q^*$ and compute a polynomial $f(x)$ with degree n as follows.

(4) Then, compute a polynomial $f(x)$ with degree n as follows: $f(x) = \prod_{i=0}^{n} (x - \mu_i) + \theta (\text{mod}q) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_i \in Z_p^*$ $(i = 0, 1, \ldots, n-1)$ (2).

(5) Compute $C = H_4(Z, \theta) \oplus (m \| w)$.

(6) Compute $V = s_{\text{sender}} + h_{\text{sender}}$.

(7) Generate ciphertext $\text{CT} = (Z, C, w, V, R_{\text{sender}}, \{a_i\})$, $i \in \{1, 2, \ldots, n-1\}$.

4.2.4. Data Receiving Phase. In this phase, the device uses its own private key to decrypt the received ciphertext to get the plaintext as shown in Figure 10.

(i) Multidecryption: this algorithm is executed by selected receiver R_i to extract plaintext from the received ciphertext $\text{CT} = (Z, C, w, V, R_{\text{sender}}, \{a_i\})$, $i \in \{1, 2, \ldots, n-1\}$. Receiver i performs the following steps:

(1) Compute $U_i = (s_i + t_i) \cdot Z$ and $\mu_i = H_3(U_i, \text{ID}_i, w)$, $i \in \{1, 2, \ldots, n\}$.

(2) Calculate $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $\theta = f(\mu_i)$.

(3) Verify whether the equation: $V \cdot P = (R_{\text{sender}} + P_{\text{Pub}})(1 + w)$.

(4) If yes, compute $m \| w = H_4(Z, \theta) \oplus C$.

(5) Verify if $Z = zP = H_2(m, w)P$ holds. If not, return $\perp$; otherwise, receiver i outputs the plaintext m.

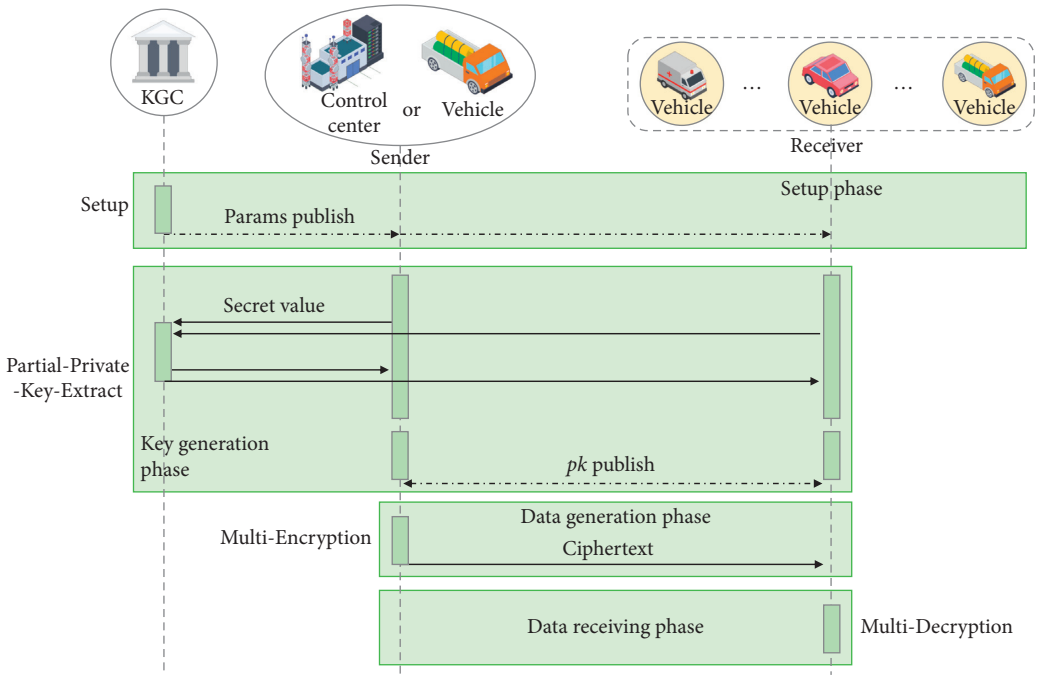


Figure 7: Flow of the proposed scheme for the connected car system on the 5G communication environment.

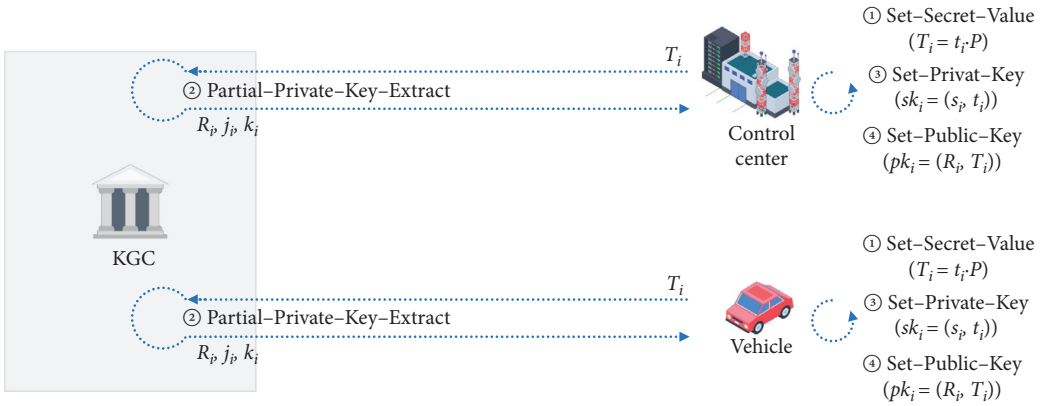


Figure 8: Flow of the key generation phase.

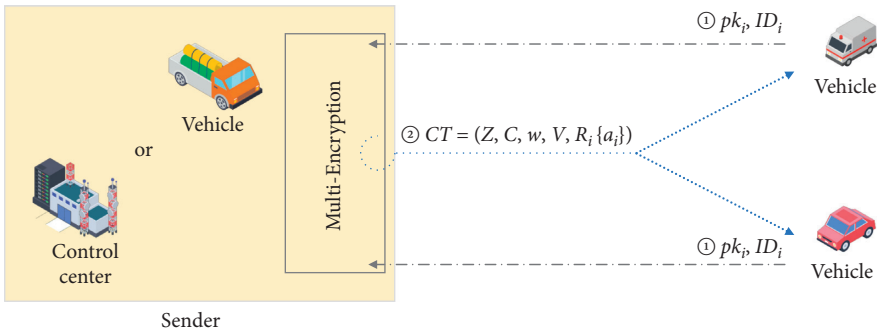


Figure 9: Flow of the data generation phase.

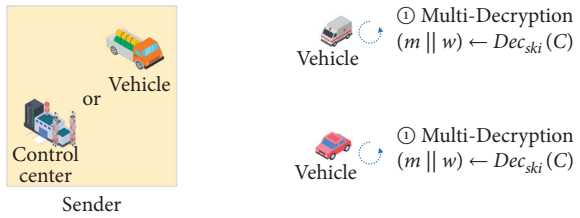


Figure 10: Flow of the data receiving phase.

5. Analysis of the Proposed CL-MRE Scheme

In this section, we analyze the proposed scheme based on the security requirements set in Section 3. The security requirements consist of confidentiality, integrity, the key escrow issue, partial key verification possibility, recipient anonymity, decryption fairness, and efficiency. The analysis results are shown in Table 1.

5.1. Correctness. In this section, we will prove the correctness of the scheme proposed in Section 4.

Theorem 1. *The receiver can perform decryption using the ciphertext C received from the sender and his/her private key and obtain the plaintext m.*

Proof. Assuming that one of the receivers is Receiver 1, Receiver 1 can perform the following process using CT = $(Z, C, w, V, R_{\text{sender}}, \{a_i\})$, $i \in \{1, 2, \ldots, n-1\}$ received from the sender and its own private key $\text{sk}_1 = (s_1, t_1)$. Receiver 1 constructs the following equation using $\{a_i\}$, $i \in \{1, 2, \ldots, n-1\}$ of CT:

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ &= \prod_{i=0}^{n} (x - \mu_i) + \theta (\text{mod} q). \end{aligned} \tag{1}$$

Receiver 1 creates U_1 and μ_1 as follows using his private key $\text{sk}_1 = (s_1, t_1)$:

$$\begin{aligned} U_1 &\longleftarrow (s_1 + t_1) \cdot Z, \\ \mu_1 &\longleftarrow H_3(U_1, \text{ID}_1, w). \end{aligned} \tag{2}$$

Receiver 1 obtains θ using the generated equation and μ_1 as follows:

$$\begin{aligned} \theta \longleftarrow f(\mu_1) &= \prod_{i=0}^{n} (\mu_1 - \mu_i) + \theta (\text{mod} q) \\ &= (\mu_1 - \mu_1) \cdot (\mu_1 - \mu_2) \cdots (\mu_1 - \mu_n) + \theta (\text{mod} q) \\ &= 0 \cdot (\mu_1 - \mu_2) \cdots (\mu_1 - \mu_n) + \theta (\text{mod} q). \end{aligned} \tag{3}$$

Receiver 1 can obtain m as follows using Z, C, and the acquired θ:

$$m \| w \longleftarrow H_4(Z, \theta) \oplus C. \tag{4}$$

□

Theorem 2. *The receiver can confirm that the sender is a registered user in KGC.*

Proof. Assuming that one of the receivers is Receiver 1, Receiver 1 can perform the following process using CT = $(Z, C, w, V, R_{\text{sender}}, \{a_i\})$, $i \in \{1, 2, \ldots, n-1\}$ received from the sender.

Receiver 1 performs the following operation using V, R, and w included in CT and public parameters P and P_pub of KGC to check if the values match:

$$\begin{aligned} V \cdot P &= (R_{\text{sender}} + P_{\text{Pub}})(1 + w) \\ &= (r_{\text{sender}} \cdot P + d \cdot P)(1 + w) \\ &= (r_{\text{sender}} + d) \cdot P \cdot (1 + w) \\ &= (r_{\text{sender}} + d + r_{\text{sender}} w + \text{d}w) \cdot P \\ &= (r_{\text{sender}} + \text{d}w + d + r_{\text{sender}} w) \cdot P \\ &= (r_{\text{sender}} + \text{d}H_1(R_{\text{sender}} + T_{\text{sender}}, \text{ID}_{\text{sender}}) + d + r_i H_1(R_{\text{sender}} + T_{\text{sender}}, \text{ID}_{\text{sender}})) \cdot P \\ &= (r_{\text{sender}} + \text{d}H_1(R_{\text{sender}} + T_{\text{sender}}, \text{ID}_{\text{sender}}) + H_1(\text{d}T_{\text{sender}} + \text{ID}_{\text{sender}}) \\ &\quad - H_1(\text{d}T_{\text{sender}} + \text{ID}_{\text{sender}}) + d + r_i H_1(R_{\text{sender}} + T_{\text{sender}}, \text{ID}_{\text{sender}}) + H_1(\text{d}T_{\text{sender}} + \text{ID}_{\text{sender}}) - H_1(\text{d}T_{\text{sender}} + \text{ID}_{\text{sender}})) \cdot P \\ &= (k_{\text{sender}} - H_1(\text{d}T_{\text{sender}} + \text{ID}_{\text{sender}}) + j_{\text{sender}} - H_1(\text{d}T_{\text{sender}} + \text{ID}_{\text{sender}})) \cdot P \\ &= (S_{\text{sender}} + h_{\text{sender}}) \cdot P \\ &= (V) \cdot P. \end{aligned} \tag{5}$$

□

Table 1: Comparison of security requirements.

	Without bilinear pairing (yes/no)	Secure for the key escrow problem (secure/insecure)	Partial key verifiability (offer/not offer)	Receiver anonymity (offer/not offer)	Decryption fairness (offer/not offer)	Message integrity (offer/not offer)	Participant verifiability (offer/not offer)
Sur et al. [30]	X	√	X	X	X	√	X
Hung et al. [32]	X	√	X	√	X	√	X
Gao et al. [34]	√	√	√	√	√	√	X
Deng [35]	X	√	√	√	√	√	X
Zhu [36]	X	√	X	X	X	√	X
Win et al. [37]	√	√	√	X	X	√	X
Wang et al. [38]	X	√	X	√	√	√	X
Proposed scheme	√	√	√	√	√	√	√

√: yes/offer/secure. X: no/not offer/insecure.

5.2. Analysis of Security Requirements. In this section, we analyze the proposed scheme based on the security requirements set in Section 3. The security requirements consist of confidentiality, integrity, the key escrow issue, partial key verification possibility, recipient anonymity, decryption fairness, and efficiency. The analysis results are shown in Table 1.

Confidentiality: in this proposed scheme, an ECC-based encryption operation is performed to provide confidentiality of the data. In this process, the message itself is not encrypted with the public key of each recipient, but a session key is created to encrypt the message. Therefore, to decrypt a message, a session key must be obtained, and to obtain a session key, only a legitimate recipient must carry out computation. For this, the proposed scheme has a recipient verification procedure based on the Lagrange interpolation polynomial, which is as follows:

$$\begin{aligned} f(x) &= \prod_{i=0}^{n} (x - \mu_i) + \theta (\mathrm{mod} q) \\ &= x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0. \end{aligned} \tag{6}$$

Here, μ_i is $\mu_i = H_3(U_i, \mathrm{ID}_i, w)$, and U_i is $U_i = s \cdot (R_{\mathrm{ID}_i} + k_{\mathrm{ID}_i} P_{\mathrm{pub}} + \mathrm{PK}_{\mathrm{ID}_i})$. Therefore, each recipient must have their own private key to generate μ_i, and the user who generates μ_i can obtain the session key e through the following process:

$$\theta = f(\mu_i) = \prod_{i=0}^{n} (\mu_i - \mu_i) + \theta (\mathrm{mod} q). \tag{7}$$

Integrity: the receiver having decrypted the data can verify the integrity of the data using the values included in the ciphertext and the parameters of the public KGC as follows:

Verify: $Z = zP = H_2(m, w)P$, where $H_4(Z, \theta) \oplus C$.

Key escrow problem: this proposed scheme uses the form of CL-PKC to solve the IBC key escrow problem. Therefore, the KGC can solve the key escrow problem because it can only know the partial private key, not the full private key.

Partial key verifiability: this proposed scheme is designed to satisfy several security requirements. In this process, there is some increase in the amount of computation, but it can be observed from Figure 11 that the difference is not significant compared to other methods. Table 2 shows the detailed calculations generated in each step of this proposed scheme.

Receiver anonymity: in this proposed scheme, a Lagrange interpolation polynomial is applied to provide anonymity of the recipient. In this method, the information of the user included in the polynomial cannot be obtained because the process of confirming the recipient is confirmed by a polynomial. The formula of this polynomial is as follows:

$$\begin{aligned} f(x) &= \prod_{i=0}^{n} (x - \mu_i) + \theta (\mathrm{mod} q) \\ &= (x - \mu_1) \cdot (x - \mu_2) \cdot \cdots \cdot (x - \mu_n) + \theta (\mathrm{mod} q) \\ &= x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0. \end{aligned} \tag{8}$$

Decryption fairness: the decryption process of the recipient data included in the recipient list should not be unfavorable or impossible to decrypt because of the intervention of a third party or KGC.

Participant verifiability: in this study, the participant verification function was designed to solve the problem of not being able to distinguish whether the data sender is an internal user of the system. This is a function that allows the sender of data to simply check whether the sender of the data is an internal user of the system, rather than allowing the sender to identify himself by using his key in the encryption step. For this purpose, only KGC knows, and verification is performed using d, which is a value issued to users inside the system by KGC. The data receiver uses that users do not know d but can obtain public parameter P_{Pub} and several parameters by calculating public parameter P on the calculated value of d. To this end, KGC calculates two values k_i and j_i and provides them to the user (sender).

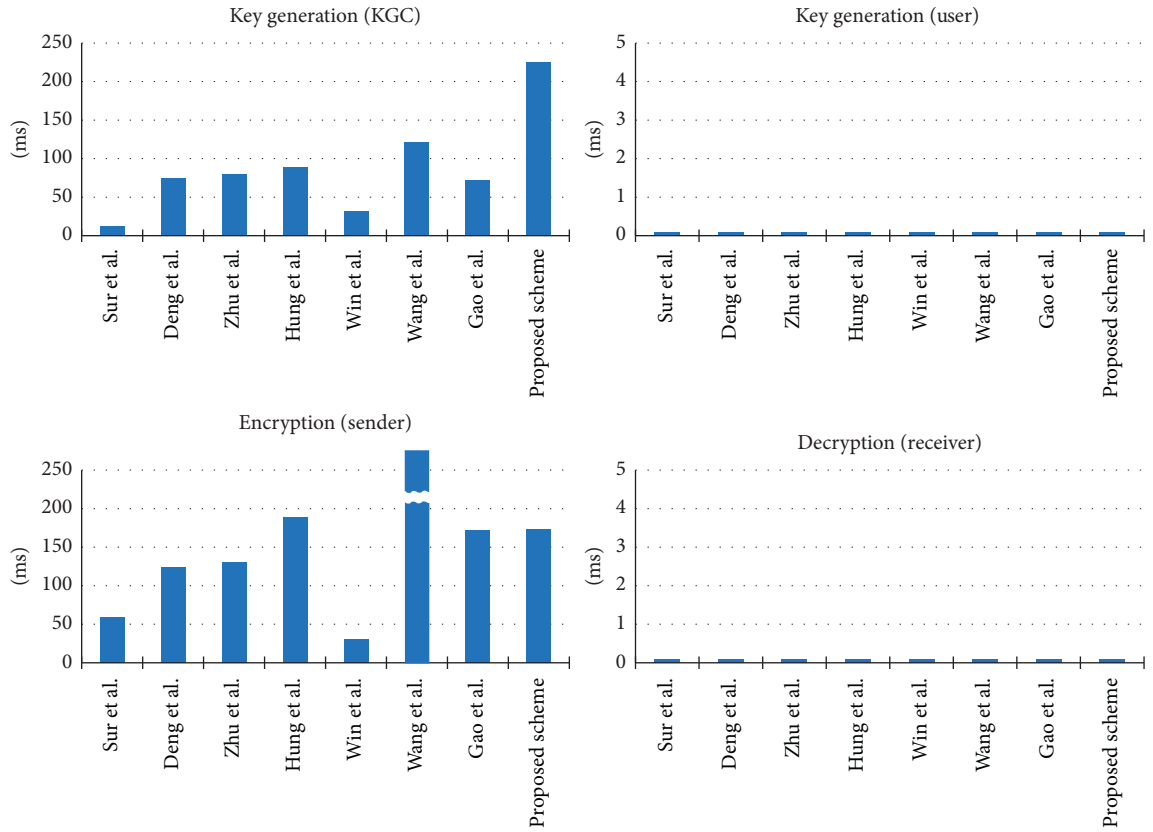


Figure 11: Comparison of computation time (number of users: 100).

Table 2: Comparison of computation complexity.

	Private key gen (KGC)	Private key gen (User)	Public key gen (user)	Encryption (sender)	Decryption (receiver)
Sur et al. [30]	nT_e	—	$2T_e$	$(2n+1)T_e + nT_m$	$1T_p + 1T_e$
Hung et al. [32]	$nT_h + nT_m$	—	$1T_m$	$nT_h + nT_p + nT_e + (n+1)T_m$	$1T_p + 1T_m$
Gao et al. [34]	$2nT_m$	$3T_m$	—	$(4n+1)T_m$	$2T_m$
Deng [35]	$2nT_m$	—	$1T_m$	$1T_p + (3n+3)T_m$	$1T_p + 1T_m$
Zhu [36]	$nT_h + nT_m$	—	$1T_m$	$nT_h + 1T_p + (2n+2)T_m$	$2T_p + 2T_m$
Win et al. [37]	nT_m	$2T_m$	$1T_m$	$(n+3)T_m + 1\text{SE}$	$4T_m + 1\text{SD}$
Wang et al. [38]	$nT_h + 2nT_m$	—	—	$nT_h + 1T_p + 1T_e + (n^2+n+1)T_m$	$3T_p + 2T_m$
Proposed scheme	$5nT_m$	$2T_m$	—	$(4n+1)T_m$	$4T_m$

T_m: time for a modular multiplication operation; T_b: time for a bilinear pairing operation; T_e: time for a modular exponentiation operation; T_h: time for a map-to-point (MTP) hash function operation; SE: symmetric encryption; SD: symmetric decryption; n: number of users.

$$k_i = r_i + \mathrm{d}H_1(R_i + T_i, \mathrm{ID}_i) + H_1(\mathrm{d}T_i + \mathrm{ID}_i) (\mathrm{mod}P),$$
$$j_i = d + r_i H_1(R_i + T_i, \mathrm{ID}_i) + H_1(\mathrm{d}T_i + \mathrm{ID}_i) (\mathrm{mod}P). \quad (9)$$

The user (sender) verifies the received value and obtains j_i and k_i, respectively, and s_i and h_i through the following operation:

$$s_i = k_i - H_1(t_i P_{\mathrm{Pub}}, \mathrm{ID}_i) = r_i + \mathrm{d}H_1(R_i + T_i, \mathrm{ID}_i),$$
$$h_i = j_i - H_1(t_i P_{\mathrm{Pub}}, \mathrm{ID}_i) = d + r_i H_1(R_i + T_i, \mathrm{ID}_i). \quad (10)$$

The user (sender) who obtains s_i and h_i performs encryption for data distribution, and creates V using s_i and h_i in the encryption step.

$$\begin{aligned} V &= r_i + \mathrm{d}H_1(R_i + T_i, \mathrm{ID}_i) + d + r_i H_1(R_i + T_i, \mathrm{ID}_i) \\ &= r_i + d + r_i H_1(R_i + T_i, \mathrm{ID}_i) + \mathrm{d}H_1(R_i + T_i, \mathrm{ID}_i) \\ &= (r_i + d)(1) + (r_i + d)(H_1(R_i + T_i, \mathrm{ID}_i)) \\ &= (r_i + d)(1 + H_1(R_i + T_i, \mathrm{ID}_i)). \end{aligned} \quad (11)$$

Thereafter, the receiver who receives the ciphertext $\mathrm{CT} = (Z, C, w, V, R_i\{a_i\})$, $i \in \{1, 2, \ldots, n-1\}$ including V may

perform the following operation using the parameters included in CT:

$$\begin{aligned} V \cdot P &= \left(R_i + P_{\text{Pub}}\right)(1 + w) \\ &= \left(r_i P + \mathrm{d}P\right)(1 + w) = \left(r_i + d\right)(1 + w)P \\ &= \left(r_i + d\right)\left(1 + H_1\left(R_i + T_i, \mathrm{ID}_i\right)\right)P \\ &= V \cdot P, \quad \text{where } w = H_1\left(R_i + T_i, \mathrm{ID}_i\right). \end{aligned} \tag{12}$$

Through this process, the receiver can verify that the sender has received the KGC's master secret key d from the KGC without verifying the sender's identity.

Efficiency: this proposed scheme was designed with the highest priority to achieve security requirements for a safe 5G communication environment. Although this proposed scheme satisfies all security requirements, computational efficiency decreased in some stages. This test was performed assuming that there were 100 users. First, the amount of computation significantly increased in the key generation step, and the computation time increased about twice as much as that of Gao et al., the basis of this study. However, in terms of users, the amount of computation and computation time were similar to those of the previous one. In the end, from the user's perspective, the security level has been further improved without significantly increasing computing costs as shown in Table 2. Therefore, the proposed form shows sufficiently meaningful results for the purpose of improving security without significantly increasing the amount of computation.

6. Conclusions

This study focuses on technology for the safe and efficient distribution of data in 5G. To this end, we have performed a comparison with the recent literature and showed that our proposed scheme is better in some areas. Existing methods pose a threat in terms of security, and in some methods, it has been observed that the amount of computation increases rapidly as the number of users increases. In addition, there are issues such as the key escrow issue, partial key verification, recipient anonymity, and decryption fairness not being provided. Such problems may cause the data to be forged or damaged by an external third party or a disadvantage in decrypting and obtaining the data by the data receiver inside the system. Therefore, to solve this problem, we used a Lagrange polynomial-based recipient identification process and achieved recipient anonymity at the same time. In addition, by solving the problem of decryption fairness that may appear in this process, we have solved the problem of disadvantage to a legitimate data receiver to acquire data by a third party. In addition, this proposed scheme is designed to determine, through participant verification, whether the user who transmits data belongs to the system. This is intended to perform quick verification while tackling external attacks that may appear in the connected car environment using 5G on which this study is focused. Through this, data can be transmitted more safely and efficiently in a connected car environment, which is an environment in which a large amount of data is simultaneously distributed in a fast-moving vehicle. Finally, our model can provide a basis for more efficient use of the 5G environment.

Data Availability

The calculation efficiency of this study was measured using Python version 3.9.1 and ECC open source, and the elliptic curve standard used for the calculation time measurement was tested based on secp256k1. The computing device used in this test was conducted using an 8-core 2.5 GHz processor and 8 GB memory.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-019R1A2C1085718) and the Soonchunhyang University Research Fund and the BK21 FOUR (Fostering Outstanding Universities for Research) (no. 5199990914048).

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[3] Dierks, T.; Rescorla, E.. The transport layer security (TLS) protocol version 1.2. 2008.

[4] E. P. Stepanova, I. A. Kalmykov, and E. Viktorovna, "Announcing the advanced encryption standard (AES)," *Journal of Digital Information Management*, vol. 14, p. 2, 2001.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, pp. 47–53, Springer, Berlin, Germany, 1984.

[6] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology—ASIACRYPT 2003*, pp. 452–473, Springer, Berlin, Germany, 2003.

[7] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," in *Public Key Cryptography-PKC 2005*, pp. 380–397, Springer, Berlin, Germany, 2005b.

[8] S. Chatterjee and P. Sarkar, "Multi-receiver identity-based key encapsulation with shortened ciphertext," in *Progress in Cryptology—INDOCRYPT 2006*, pp. 394–408, Springer, Berlin, Germany, 2006.

[9] F. C. Zhou, M. Q. Lin, Y. Zhou, and Y. X. Li, "Efficient anonymous broadcast encryption with adaptive security," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 9, no. 11, pp. 4680–4700, 2015.

[10] L. Zhang, Y. Hu, and Q. Wu, "Identity-based threshold broadcast encryption in the standard model," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 4, no. 3, pp. 400–410, 2010.

[11] P. Vijayakumar, S. Bose, A. Kannan, and L. Jegatha Deborah, "Computation and communication efficient key distribution protocol for secure multicast communication," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 4, pp. 878–894, 2013.

[12] I. Kim and S. Hwang, "An optimal identity-based broadcast encryption scheme for wireless sensor networks," *IEICE Transactions on Communications*, vol. E96.B, no. 3, pp. 891–895, 2013.

[13] J. Jongkil Kim, W. Susilo, M. Man Ho Au, and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 679–693, 2015.

[14] J. Li, Q. Yu, and Y. Zhang, "Identity-based broadcast encryption with continuous leakage resilience," *Information Sciences*, vol. 429, pp. 177–193, 2018.

[15] J. Lai, Y. Mu, F. Guo, P. Jiang, and S. Ma, "Identity-based broadcast encryption for inner products," *The Computer Journal*, vol. 61, no. 8, pp. 1240–1251, 2018.

[16] Y. Ming and Y. Wang, "Identity based broadcast encryption with group of prime order," *The International Arab Journal of Information Technology*, vol. 13, no. 5, pp. 531–541, 2016.

[17] J. H. Park and D. H. Lee, "Security analysis of a multi-receiver identity-based key encapsulation mechanism," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E92-A, no. 1, pp. 329–331, 2009.

[18] H. Wang, P. Zeng, and K.-K. R. Choo, "MDMR-IBE: efficient multiple domain multi-receiver identity-based encryption," *Security and Communication Networks*, vol. 7, no. 11, pp. 1641–1651, 2014.

[19] K. Xu, Y. Liao, L. Qiao, Z. Liu, and X. Yang, "An identity-based (IDB) broadcast encryption scheme with personalized messages (BEPM)," *PLoS One*, vol. 10, no. 12, Article ID e0143975, 2015.

[20] X. Zhao and F. Zhang, "Fully CCA2 secure identity-based broadcast encryption with black-box accountable authority," *Journal of Systems and Software*, vol. 85, no. 3, pp. 708–716, 2012.

[21] L. Zhang, Q. Wu, and Y. Hu, "New constructions of identity-based broadcast encryption without random oracles," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 2, pp. 428–439, 2011.

[22] L. Zhang, Y. Hub, and Q. Wu, "Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups," *Mathematical and Computer Modelling Dynmaics*, vol. 55, no. 1–2, pp. 12–18, 2012.

[23] C. Chun-I Fan, L. Ling-Ying Huang, and P. Pei-Hsiu Ho, "Anonymous multireceiver identity-based encryption," *IEEE Transactions on Computers*, vol. 59, no. 9, pp. 1239–1249, 2010.

[24] H. Wang, Y. Zhang, H. Xiong, and B. Qin, "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme," *IET Information Security*, vol. 6, no. 1, pp. 20–27, 2012.

[25] H.-Y. Chien, "Improved anonymous multi-receiver identity-based encryption," *The Computer Journal*, vol. 55, no. 4, pp. 439–446, 2012.

[26] C. Fan, P. Tsai, J. Huang, and W. Chen, "Anonymous multi-receiver certificate-based encryption," in *Proceedings of the 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 19–26, Beijing, China, October 2013.

[27] M. Zhang and T. Takagi, "Efficient constructions of anonymous multireceiver encryption protocol and their deployment in group E-mail systems with privacy preservation," *IEEE Systems Journal*, vol. 7, no. 3, pp. 410–419, 2013.

[28] J. Zhang and J. Mao, "An improved anonymous multi-receiver identity-based encryption scheme," *International Journal of Communication Systems*, vol. 28, no. 4, pp. 645–658, 2015.

[29] C. Sur, C. D. Jung, and K. H. Rhee, "Multi-receiver certificate-based encryption and application to public key broadcast encryption," in *Proceedings of the 2007 ECSIS Symposium on Bio-inspired, Learning, and Intelligent Systems for Security (BLISS 2007)*, pp. 35–40, Edinburgh, UK, August 2007.

[30] C. Sur, Y.-H. Park, and K.-H. Rhee, "A multi-receiver certificateless encryption scheme and its application," *Journal of Korea Multimedia Society*, vol. 14, no. 6, pp. 775–784, 2011.

[31] S. K. Hafizul, K. Muhammad, and M. Ali, "Anonymous and provably secure certificateless multi-receiver encryption without bilinear pairing," *Security and Communication Networ*, vol. 8, no. 13, pp. 2214–2231, 2015.

[32] Y.-H. Hung, S.-S. Huang, Y.-M. Tseng, and T.-T. Tsai, "Efficient anonymous multireceiver certificateless encryption," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2602–2613, 2017.

[33] D. He, H. Wang, L. Wang, J. Shen, and X. Yang, "Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices," *Soft Computing*, vol. 21, no. 22, pp. 6801–6810, 2017b.

[34] R. Gao, J. Zeng, and L. Deng, "Efficient certificateless anonymous multi-receiver encryption scheme without bilinear parings," *Mathematical Problems in Engineering*, vol. 2018, Article ID 1486437, 13 pages, 2018.

[35] L. Deng, "Anonymous certificateless multi-receiver encryption scheme for smart community management systems," *Soft Computing*, vol. 24, no. 1, pp. 281–292, 2020.

[36] J. Zhu, "A new efficient certificateless multi-receiver public key encryption scheme," *International Journal of Computer Science Issues*, vol. 13, no. 6, pp. 1–7, 2016.

[37] E. K. Win, T. Yoshihisa, Y. Ishi, T. Kawakami, Y. Teranishi, and S. Shimojo, "A lightweight multi-receiver encryption scheme with mutual authentication," in *Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, pp. 491–497, IEEE, Turin, Italy, July 2017.

[38] Q. Wang, F. Li, and H. Wang, "An anonymous multi-receiver with online/offline identity-based encryption," *Wireless Communications and Mobile Computing (WCMC)*, vol. 2018, Article ID 5702068, 10 pages, 2018.