micromachines

Article

A Conditional Privacy Preserving Generalized Ring Signcryption Scheme for Micro Aerial Vehicles

Insaf Ullah [1], Muhammad Asghar Khan [1], Ako Muhammad Abdullah [2,3], Syed Agha Hassnain Mohsan [4,*], Fazal Noor [5], Fahad Algarni [6] and Nisreen Innab [7]

1 Hamdard Institute of Engineering and Technology, Hamdard University, Islamabad 440000, Pakistan
2 Computer Science Department, College of Basic Education, University of Sulaimani, Sulaimaniyah 00964, Kurdistan Region, Iraq
3 Department of Information Technology, University College of Goizha, Sulaimaniyah 00964, Kurdistan Region, Iraq
4 Ocean College, Zhejiang University, Zheda Road 1, Zhoushan 316021, China
5 Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia
6 College of Computing and Information Technology, The University of Bisha, Bisha 67714, Saudi Arabia
7 Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, P.O. Box 71666, Riyadh 11597, Saudi Arabia
* Correspondence: hassnainagha@zju.edu.cn

Abstract: Micro Aerial Vehicles (MAVs) are a type of UAV that are both small and fully autonomous, making them ideal for both civilian and military applications. Modern MAVs can hover and navigate while carrying several sensors, operate over long distances, and send data to a portable base station. Despite their many benefits, MAVs often encounter obstacles due to limitations in the embedded system (such as memory, processing power, energy, etc.). Due to these obstacles and the use of open wireless communication channels, MAVs are vulnerable to a variety of cyber-physical attacks. Consequently, MAVs cannot execute complex cryptographic algorithms due to their limited computing power. In light of these considerations, this article proposes a conditional privacy-preserving generalized ring signcryption scheme for MAVs using an identity-based cryptosystem. Elliptic Curve Cryptography (ECC), with a key size of 160 bits, is used in the proposed scheme. The proposed scheme's security robustness has been analyzed using the Random Oracle Model (ROM), a formal security evaluation method. The proposed scheme is also compared in terms of computation cost, communication cost and memory overhead against relevant existing schemes. The total computation cost of the proposed scheme is 7.76 ms, which is 8.14%, 5.20%, and 11.40% schemes. The results show that the proposed scheme is both efficient and secure, proving its viability.

Keywords: micro aerial vehicles; security; signcryption; elliptic curve cryptography; ring signcryption

Citation: Ullah, I.; Khan, M.A.; Abdullah, A.M.; Mohsan, S.A.H.; Noor, F.; Algarni, F.; Innab, N. A Conditional Privacy Preserving Generalized Ring Signcryption Scheme for Micro Aerial Vehicles. *Micromachines* **2022**, *13*, 1926. https://doi.org/10.3390/mi13111926

Academic Editor: Arman Roohi

Received: 20 September 2022
Accepted: 28 October 2022
Published: 8 November 2022

1. Introduction

Micro Aerial Vehicles (MAVs) are getting a lot of attention from research organizations and businesses around the world [1]. These flying machines have proven their worth in situations where humans cannot reach or work efficiently, such as last-minute package delivery during rush hours or base searches in inaccessible areas of the battlefield. Compared to conventional methods, MAVs can significantly lower the risk to human life, increase the system's efficiency, and shorten the time of operations. The broad capabilities of MAVs range from surveillance MAVs with fixed wings to advanced MAVs capable of hovering, navigation, carrying several sensors, and carrying out their missions up to several kilometers in range [2]. MAVs can transmit data to a portable base station and can exchange data with one another. A general architecture of MAVs network is depicted in Figure 1. Despite these benefits, MAVs are not suitable for real-time or processor-intensive applications because to their limited memory and processing power [3].

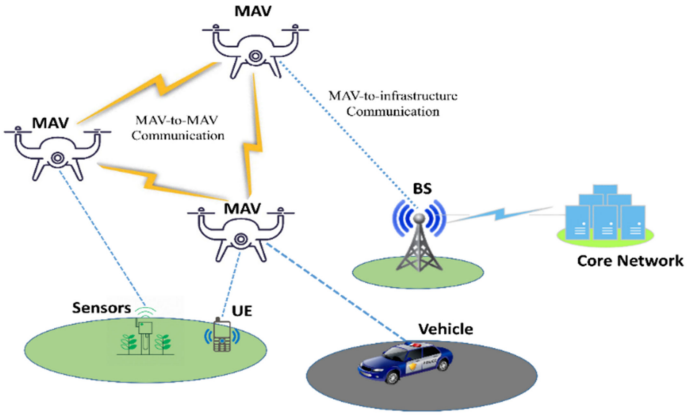

Figure 1. General architecture of MAVs network.

Apart from the aforementioned constraints, the security measures to fight against cyber-attacks are rarely considered during the design of MAVs [4]. The security and privacy of the network could be severely compromised due to this vulnerability, which would have a devastating effect on data transmission and storage. There are a variety of ways a malicious attacker can compromise the MAVs system. The malicious attacker can, for instance, send several reservation requests, eavesdrop on control messages, or fake data. Wi-Fi-connected MAVs are more vulnerable to cyber-attacks than cellular-connected ones because of their less-reliable connections and weaker security measures [5]. Tracking MAV locations, tampering with onboard hardware, illegal data access, message modification, and fabrication are examples of common privacy and security concerns across the MAV system [6,7]. A major security concern that compromises the privacy of MAVs is a Global Positioning System (GPS) spoofing attack [8–10], in which an attacker exploits GPS signals. In this method, an adversary sends an MAV slightly stronger GPS signals in order to deviate it from its original mission. Therefore, given their extensive usage in current military and commercial applications, there is an urgent need for enhanced security measures for MAVs.

Authentication and confidentiality are two of the most important aspects of any security protocol design for ensuring secure communication, and the same is applicable for MAVs security. Encryption and digital signatures provide solutions for confidentiality and authenticity respectively. When both attributes are required simultaneously and in a single logical step for devices with limited resources, such as MAVs, signcryption [11] is preferred. In addition, generalized signcryption is an extension of the signcryption scheme that not only offers encryption and digital signature simultaneously, but also has the option to offer both independently, if desired. Such a characteristic is useful if one of the two essential characteristics, confidentiality or authenticity, is desired [12]. Generalized signcryption can be used in ring configurations, known as ring signcryption, which offers advantageous characteristics such as anonymity, spontaneity, flexibility, and equal membership [13]. A conditional privacy preserving property can be implemented in addition to generalized ring signcryption to guarantee recipient and sender identify anonymity. In this approach, each entity encrypts their real identity using a common secret key between entity and PKG in the key generation process rather than using the real identities of sender and receiver. PKG must first locate the secret key and real identity after obtaining the encrypted identity. The encrypted identities of each user for signcryption and unsigncryption are then published by PKG.

Zhou et al. [14] proposed a concrete scheme for generalized ring signcryption in an identity-based framework. The proposed technique is based on bilinear pairing, and a random oracle model (ROM) is used for the security analysis. Due to the fact that the scheme [14] is based on bilinear pairing, which involves computationally expensive cryptographic operations, it is not suited for resource-constrained devices with low processing capabilities, such as MAVs, to conduct such operations. In addition, the proposed scheme lacks conditional privacy-preserving characteristics. Caixue Zhou [15] proposed a

certificate-based generalized ring signcryption method and a concrete methodology employing bilinear pairings for certificate-based cryptosystems. Using the ROM, the security hardness of the proposed system is evaluated. Again, this scheme [15] is not suitable for MAVs due to the high computation cost of bilinear pairing and the absence of conditional privacy-preserving attribute.

M. Luo and Y. Zhou [16] introduced an efficient conditional privacy-preserving authentication protocol based on generalized ring signcryption scheme. Generalized ring signcryption is proposed in this protocol to provide ring signature mode and ring signcryption mode inside a single algorithm in order to meet the diverse security needs of complicated application scenarios. A practical public verification technique is meant to make tracking results verifiable and more trustworthy. In addition, the protocol accomplishes secrecy, immutability, and Known Session-Specific Temporary Information Security (KSSTIS). However, the proposed protocol involves bilinear pairing-based multiplication, modular exponentials, and bilinear pairing in the combined ring signature and signcryption method, which is incompatible for MAVs. Khan et al. [17] presented an identity-based generalized signcryption with multi-access edge computing option to protect Flying Ad hoc Networks (FANETs). However, neither conditional privacy preservation nor ring signcryption are supported by the proposed scheme. Consequently, this scheme [17] does not ensure anonymity. Din et al. [18] presented an improved identity-based generalized signcryption scheme for secure multi-access edge computing-enabled FANETs. The proposed scheme supports neither conditional privacy preservation nor ring signcryption. Therefore, this approach [18] does not guarantee anonymity.

With the aforementioned facts and favorable features in mind, we provide a conditional privacy-preserving generalized ring signcryption scheme for MAVs in this work. Moreover, the proposed scheme is based on an Identity-based public key cryptosystem, which uses the user's name, IP address, etc. as his/her public key, hence eliminating the requirement for a public key certificate. Then, a trusted third party known as the PKG produces all users' private keys, which introduces a new issue known as the private key escrow problem. However, it is still quite beneficial in situations when the PKG is completely trusted. The following are the main contributions of the proposed scheme that distinguish it from existing schemes.

- We propose a conditional privacy-preserving generalized ring signcryption scheme for MAVs using the ECC operation.
- The proposed scheme is conditional privacy-preserving, meaning each entity encrypts its real identity using a common secret key between entity and PKG in the key generation process.
- The proposed scheme enables encryption and digital signature simultaneously as well as independently using generalized signcryption. In ring configurations mode, this scheme guarantees anonymity, spontaneity, flexibility, and equal membership.
- We conducted a formal security study using the Random Oracle Model (ROM) and found that the proposed scheme is secure against a wide range of cyber-attacks.
- Finally, the proposed scheme's efficiency is compared to its counterparts, validating its low computation cost, communication cost and memory overhead.

The structure of the article is as follows: Section 2 provides preliminary information, the network model, and the syntax of the proposed scheme. In contrast, Section 3 includes a security analysis of the proposed scheme. In Section 4, performance analysis is discussed. The conclusion is contained in Section 5.

2. Preliminaries, Network Model and Syntax of the Proposed Scheme

This section includes preliminaries (elliptic curve cryptography, the elliptic curve decisional Diffie–Hellman problem, the elliptic curve discrete logarithm problem), syntax of the proposed scheme, network model and notations for the proposed scheme as shown in Table 1.

Table 1. Notation table.

S. No	Notation	Descriptions
1	GCN	Ground core network
2	PKG	Private key generator
3	Ж	Public parameter param
4	$Ц_1$,$Ц_2$, $Ц_3$	Irreversible and collision resistant hash functions
5	δ_{GCN}	Master secret key of ground core network
6	δ_{GCN}	Master public key of ground core network
7	ξ	Generator of group G_{ECC}
8	G_{ECC}	Finite cyclic group on the elliptic curve E_{ECC}
9	E_{ECC}	The elliptic curve defined on $V^2 = U^3 + sU + t$
10	EId_{MAV}	Encrypted identity of MAV
11	MAV	It represents a Micro Aerial Vehicle (MAV)
12	EId_X	Encrypted identity of everything (X)
13	Id_{MAV}	Real identity of MAV
14	Id_X	Real identity of everything (X)
15	f_q	Finite field on the elliptic curve E_{ECC} of order q
16	Φ_{MAV}	Private key of MAV
17	Φ_X	Private key of everything (X)
18	λ_X	Public key of everything (X)
19	λ_{MAV}	Public key of MAV
20	Δ	Identities of ring group $\{EId_{MAV\ 1}$, $EId_{MAV\ 2}, EId_{MAV\ 3}, \ldots\ldots, EId_{MAVn}\}$
21	γ_{MAV}	Encryption and decryption key for real identity of MAV
22	γ_X	Encryption and decryption key for real identity of everything (X)
23	Ψ	Encryption and decryption key for message MAV and everything (X)
24	$\oplus$	Used for Encryption and decryption

2.1. Preliminaries

2.1.1. Elliptic Curve Cryptography (*ECC*)

Suppose G_{ECC} is a finite cyclic group on the elliptic curve (E_{ECC}), f_q is the finite field of E_{ECC} with prime order q, let $q > 3$, and ξ is the generator of group G_{ECC}; the elliptic can be defined as follows: $V^2 = U^3 + sU + t$ on f_q. Suppose $(U, V) \in f_q \times f_q$ based on the point, which is called infinity point on elliptic curve $\left(\hat{O}\right)$ and congruence $V^2 \equiv U^3 + sU + t mod\ q$, where the values $(s, t) \in f_q$ satisfying $4s^3 + 27t^2 mod\ q$.

2.1.2. Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP)

Assume ξ is the generator of group G_{ECC} with prime order q, and given ($\Omega \cdot \xi$, $\theta \cdot \xi, \xi$, $K \in G_{ECC}$), extracting θ and Ω from $K = \Omega \cdot \theta \cdot \xi$ is called ECDDHP.

2.1.3. Elliptic Curve Discrete Logarithm Problem (ECDLP)

Assume ξ is the generator of group G_{ECC} with prime order q, and given ($\theta.\xi$,ξ, $K \in G_{ECC}$), extracting θ from $K = \theta.\ \xi$ is called ECDLP.

2.2. Syntax

The syntax of the proposed scheme consists of the five sub-algorithms listed below.

1. Initialization: The ground core network (GCN) can play the role private key generator (PKG), in which he/she can sets $ß_{GCN}$ as his/her secret key, δ_{GCN} as his/her public key, and generates a public parameter set Ж.
2. Key Generation: The device that participates in a network as a legal user will send $(EId_i,\ \Omega_i)$ to GCN by using open channel. Based on $(EId_i,\ \Omega_i)$, GCN first compute γ_i and recover the real identity Id_i. Then, GCN computes λ_i, Φ_i and send $(\Phi_i,\ \lambda_i)$ to the legitimate user by using secure channel.
3. Generalized Ring Signcryption: This algorithm will run by Micro Aerial Vehicle (*MAV*), in which the *MAV* take input that are $(EId_{MAV}, m, \lambda_X, £_X, \delta_{GCN})$ and produce the tuple $(\kappa, Л, \Gamma)$.
4. Generalized Ring Signcryption Verifications: Given the tuple $(EId_X, \lambda_{MAV}, £_{MAV}, \delta_{GCN}, \kappa, Л, \Gamma, \Phi_X.)$, a user can verify $(\kappa, Л, \Gamma)$.

2.3. Network Model

Figure 2 depicts the network model of the proposed scheme, which includes entities such as MAVs and Base Station (BS) deployed to provide monitoring of a certain region. The proposed network model relies heavily on MAVs, which are outfitted with a camera, IMU, sensors, and GPS devices capable of handling a wide range of use cases. It allows for interaction between many MAVs and also between MAVs and fixed facilities. To establish a connection with the BS, the MAV makes use of 5G and Wi-Fi wireless technologies. The MAVs are able to talk to one another over Wi-Fi. The primary goal of a hybridised approach is to capitalise on the strengths of both technologies.

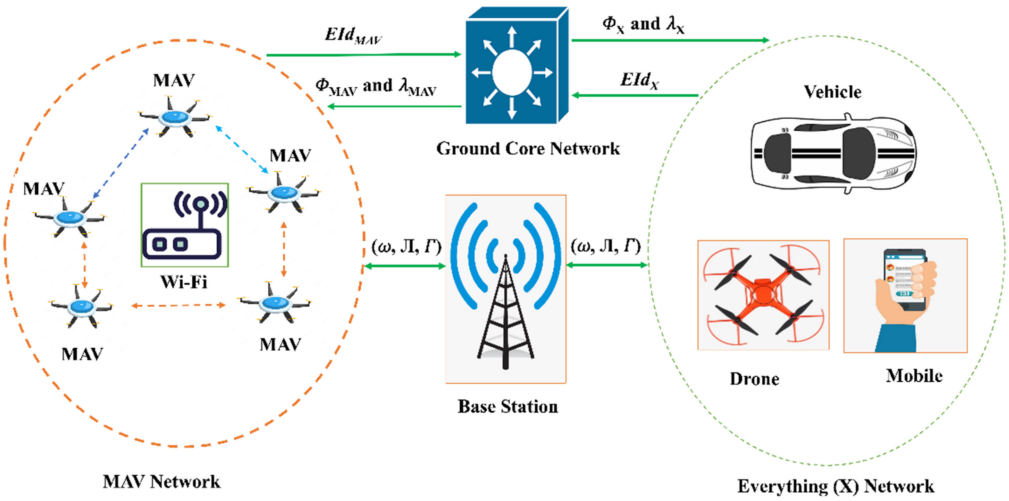

Figure 2. Network model of the proposed scheme.

3. Proposed Scheme Construction

The construction of the proposed scheme includes the following steps.

Initialization: In this sub algorithm, a ground core network (GCN) can play the role private key generator (PKG) that can first choose his own secret key $ß_{GCN} \in f_q$ and compute a master public key as $\delta_{GCN} = ß_{GCN} \cdot \xi$. then, GCN chooses three hash functions $(Ц_1, Ц_2, Ц_3)$ that are irreversible and collision resistant. At the end, GCN produces a public param $Ж = (f_q, \delta_{GCN}, \xi,\ _{1,\ 2,3})$.

Key Generation: In this sub algorithm, a device which participated in a network as a legal user will send his encrypted real identity $EId_i = \gamma_i \oplus Id_i$, and $\Omega_i = \alpha_i \cdot \xi$, to GCN by using open channel, where $\gamma_i = \alpha_i \cdot \delta_{GCN}$ and $\alpha_i \in f_q$. Based on $(EId_i,\ \Omega_i)$, GCN firs compute $\gamma_i = ß_{GCN} \cdot \Omega_i$ and recover the real identity Id_i as $Id_i = EId_i \oplus \gamma_i$. Then, GCN choose $\eta_i \in f_q$, compute $\lambda_i = \eta_i \cdot \xi$, $£_i = Ц_1(Id_i, \lambda_i)$, calculate $\Phi_i = \eta_i + £_i \cdot ß_{GCN}$, and send $(\Phi_i,\ \lambda_i)$ to the legitimate user by using secure channel.

Generalized Ring Signcryption: This algorithm will run by MAV, in which the MAV first select his identity (EId$_{MAV}$) from $\Delta = \{EId_{MAV\,1},\ EId_{MAV\,2}, EId_{MAV\,3}, \ldots\ldots, EId_{MAVn}\}$ and perform the following steps.

- MDN choose $\chi_{MAV} \in f_q$ and compute $\beth = \chi_{MAV} \cdot \xi$.
- Compute $\Psi = \chi_{MAV}\ (\lambda_X + £_X \cdot \delta_{GCN})$ *and* $\Gamma = \amalg_2(\Psi) \oplus (m, EId_{MAV}\ )$.
- Compute $\omega = \amalg_3(EId_{MAV}\ , \lambda_{MAV}, \lambda_X, \beth, \Gamma)$ *and* $\kappa = \chi_{MAV}\ + \omega \cdot \Phi_{MAV}$.
- MAV send $(\omega, \beth, \Gamma)$ to everything (X).

Generalized Ring Signcryption Verifications: With the encrypted identity (EId_X), a user upon reception of $(\omega, \beth, \Gamma)$ can perform the following steps.

- Compare if $\kappa \cdot \xi = \beth + \omega \cdot (\lambda_{MAV} + £_{MAV} \cdot \delta_{GCN})$ is holds, where $\omega = \amalg_3(EId_{MAV}, \lambda_{MAV}, \lambda_X, \beth, \Gamma)$.
- Compute $\Psi = \Phi_X \cdot \beth$ and $(m, EId_{MAV}) = \Gamma \oplus \amalg_2(\Psi)$.

Correctness Analysis

The device at receiving end (X) can verify the signature as follows.

$$\begin{gathered}\kappa \cdot \xi = \beth + \omega \cdot (\lambda_{MAV} + £_{MAV} \cdot \delta_{GCN}) = (\chi_{MAV} + \omega \cdot \Phi_{MAV}) \cdot \xi = (\chi_{MAV} \cdot \xi + \\ \omega \cdot \Phi_{MAV} \cdot \xi) = (\chi_{MAV} \cdot \xi + \omega \cdot (\eta_{MAV} + £_{MAV} \cdot ß_{GCN}) \cdot \xi) = (\chi_{MAV} \cdot \xi + \\ \omega \cdot (\eta_{MAV} \cdot \xi + £_{MAV} \cdot ß_{GCN} \cdot \xi)) = (\beth + \omega \cdot (\lambda_{MAV} + £_{MAV} \cdot \delta_{GCN}))\end{gathered} \tag{1}$$

hence proved.

Furthermore, a device at receiving end (X) can made the decryption key as follows.

$$\begin{gathered}\Psi = \Phi_X \cdot \beth = (\eta_X + £_X \cdot ß_{GCN}) \cdot \chi_{MAV} \cdot \xi = (\eta_X \cdot \xi + £_X \cdot ß_{GCN} \cdot \xi) \cdot \chi_{MAV} = \\ (\lambda_X + £_X \cdot \delta_{GCN}) \cdot \chi_{MAV} = \chi_{MAV}(\lambda_X + £_X \cdot \delta_{GCN})\end{gathered} \tag{2}$$

hence proved.

4. Security Analysis

In this section, we first show that the proposed scheme is secure against breaches of confidentiality and forgeability under the Random Oracle Model (ROM). Then, using an informal security analysis, we show that the proposed scheme is secure against an adversary attempting to violate sender and recipient anonymity. The subsequent theorems demonstrate that the proposed scheme provides security properties such as confidentiality, unforgeability, sender anonymity, and recipient anonymity, respectively.

Theorem 1. ***Confidentiality:*** *The proposed generalized ring signcryption is indistinguishable against intruder INT under the ROM, if ECDDHP is hard.*

Proof. Suppose the instances of elliptic curve $(\Omega \cdot \xi,\ \theta \cdot \xi, \xi, K \in G_{ECC})$ is given to C_{ECDDHP}. To find θ and Ω from $K = \Omega \cdot \theta \cdot \xi$, C_{ECDDHP} will play the following Game with INT.

Initialization: C_{ECDDHP} can first choose the secret key $ß_{GCN} \in f_q$, public key δ_{GCN}, public parameter set Ж. Then, C_{ECDDHP} sends Ж to INT.

Phase 1: Here, INT can made the following queries with C_{ECDDHP}.

$\amalg_1$ Query: INT send a request for $\amalg_1$ Query with identity (Id_i) C_{ECDDHP} check for a tuple $(Id_i, \lambda_i, £_i)$ in the list $L_{\amalg_1}$, if $(Id_i, \lambda_i, £_i)$ is found, C_{ECDDHP} returns $£_i$ to INT. Otherwise, C_{ECDDHP} choose the value for $£_i$ randomly and returns it to INT.

$\amalg_2$ Query: INT send a request for $\amalg_2$ Query with identity (Id_i) C_{ECDDHP} check for a tuple $(\Psi_i, £_{1i})$ in the list $L_{\amalg_2}$, if $(\Psi_i, £_{1i})$ is found, C_{ECDDHP} returns $£_{1i}$ to INT. Otherwise, C_{ECDDHP} choose the value for $£_{1i}$ randomly and returns it to INT.

$\amalg_3$ Query: INT send a request for $\amalg_3$ Query with identity (Id_i) C_{ECDDHP} check for a tuple $(EId_i, \lambda_i, \Gamma_i, \beth_i, \omega_i)$ in the list $L_{\amalg_3}$, if $(EId_i, \lambda_i, \Gamma_i, \beth_i, \omega_i)$ is found, C_{ECDDHP} returns ω_i to INT. Otherwise, C_{ECDDHP} choose the value for ω_i randomly and returns it to INT.

User Public Key Query: INT send a request for User Public Key Query with (Id_i, λ_i), C_{ECDDHP} check for a tuple (Id_i, λ_i) in the list L_{UPK}, if (Id_i, λ_i) is found, C_{ECDDHP} returns λ_i to INT. Otherwise, C_{ECDDHP} perform the following two steps.

- At *jth* query, if $i = j$, C_{ECDDHP} set $\lambda_i = \Omega \cdot \xi$.
- Else, compute $\lambda_i = \eta_i \cdot \xi$, where it selects η_i randomly.
- At the end, C_{ECDDHP} returns λ_i to INT.

User Private Key Query: INT send a request for User Private Key Query with $(Id_i, \lambda_i, \Phi_i)$, C_{ECDDHP} check for a tuple $(Id_i, \lambda_i, \Phi_i)$ in the list L_{UPRK}, if $Id_i = Id$, C_{ECDDHP} stop further processing, otherwise he found the tuple $(Id_i, \lambda_i, \Phi_i)$ and returns Φ_i to INT.

Generalized Ring Signcryption Query: INT send a request for Generalized Ring Signcryption with m, EId_{MAV} and EId_X, where $EId_{MAV} \in \Delta = \{EId_{MAV\,1}, EId_{MAV\,2}, EId_{MAV\,3}, \ldots\ldots, EId_{MAVn}\}$ and C_{ECDDHP} perform the following steps.

- If $EId_{MAV} != Id$, It choose $\chi_{MAV} \in f_q$ and compute $\beth = \chi_{MAV} \cdot \xi - \omega(\lambda_{MAV} + \pounds_{MAV} \cdot \delta_{GCN})$.
- Compute $\Psi = \chi_{MAV}(\lambda_X + \pounds_X \cdot \delta_{GCN})$ *and* $\Gamma = \amalg_2(\Psi) \oplus (m, EId_{MAV})$.
- Compute $\omega = \amalg_3(EId_{MAV}, \lambda_{MAV}, \lambda_X, \beth, \Gamma)$ *and* $\kappa = \chi_{MAV} + y$, *where y is randomly selected now here.*
- C_{ECDDHP} send $(\kappa, \beth, \Gamma)$ to INT.

Generalized Ring Signcryption Verification Query: If $EId_X = Id$, C_{ECDDHP} shows the tuple $(\kappa, \beth, \Gamma)$ is invalid. Otherwise, it normally Generalized Ring Signcryption Verification algorithm.

Challenge: INT send the tuple $(m_{101}, m_{102}, EId_{MAV}, EId_X)$ to C_{ECDDHP}, where m_{101}, m_{102} are the two plaintexts with same size but contains different contents. If $EId_X = Id$, C_{ECDDHP} pick $\iota \in \{0, 1\}$ and perform the following computations.

- It computes $\beth = \Omega \cdot \xi$.
- Compute $\Psi = K + \pounds_X \cdot \delta_{GCN}$ *and* $\Gamma = \amalg_2(\Psi) \oplus (m, EId_{MAV})$.
- Compute $\omega = \amalg_3(EId_{MAV}, \lambda_{MAV}, \lambda_X, \beth, \Gamma)$ *and* $\kappa = \omega \cdot \Phi_{MAV} + y + \Omega$, *where y is randomly selected here.*
- C_{ECDDHP} returns $(\kappa, \beth, \Gamma)$.

Phase 2: In this phase, INT executes $\amalg_1$ Query, $\amalg_2$ Query, $\amalg_3$ Query, User Public Key Query, Generalized Ring Signcryption Query, and Generalized Ring Signcryption Verification Query, respectively. Note that at this stage INT should not perform User Private Key Query on encrypted identity EId_X and requested message corresponding to the Generalized ring signcrypted text.

Guess: INT return $\iota^{/} \in \{0, 1\}$, if $\iota = \iota^{/}$, C_{ECDDHP} outputs 1. Otherwise, C_{ECDDHP} outputs 0.

Probability Analysis: Suppose $Q\amalg_1, Q\amalg_1, Q\amalg_1, Q_{UPK}$, and Q_{UPRK} represent $\amalg_1$ Query, $\amalg_2$ Query, $\amalg_3$ Query, User Public Key Query, and User Private Key Query, respectively. So, we express the following events.

1. $\Theta_1 : C_{ECDDHP}$ succeeded in User Private Key Query.
2. $\Theta_2 : C_{ECDDHP}$ succeeded in Generalized Ring Signcryption Verification Query.
3. $\Theta_2 : C_{ECDDHP}$ succeeded in in challenge phase.

After denoting the above events, we can easily receive the following outcomes. $\Pr(\Theta_1) = 1 - \frac{Q_{UPRK}}{Q_{UPK}}$, $\Pr(\Theta_2) = 1 - \frac{1}{2^j}$, and $\Pr(\Theta_3) = \frac{1}{Q_{UPK} - Q_{UPRK}}$, then $\Pr(C_{ECDDHP}\ sucess) = \Pr(\Theta_1 \wedge \Theta_2 \wedge \Theta_3) = \Pr(\Theta_1) \cdot \Pr(\Theta_2) \cdot \Pr(\Theta_3) = \left(1 - \frac{Q_{UPRK}}{Q_{UPK}}\right)\left(1 - \frac{1}{2^j}\right)\left(\frac{1}{Q_{UPK} - Q_{UPRK}}\right) \approx \left(\frac{1}{Q_{UPK}}\right) \approx \frac{\epsilon}{Q_{UPK}}$, where ϵ represent the advantage of INT. □

Theorem 2. Unforgeability. *Our proposed generalized ring signcryption is indistinguishable against intruder INT under the random oracle model, if ECDLP is hard.*

Proof. Suppose the instance of elliptic curve $(\Omega \cdot \xi, \xi, K \in G_{ECC})$ is given to C_{ECDLP} so, to find Ω from $K = \Omega \cdot \xi$, C_{ECDLP} will play the following Game with INT.

Initialization: C_{ECDLP} can first choose the secret key $ß_{GCN} \in f_q$, public key δ_{GCN}, public parameter set Ж. Then, C_{ECDDHP} send Ж to INT.

Queries: All the queries are processed is same as executed in Theorem 1-Confidentiality.

Forgery: INT wants to generate and verify combined ring signature and signcryption, in which he needs the private key of MAV and X (Φ_{MAV}, Φ_X). INT can generate the forge signature as follows.

- INT choose $\chi_{INT} \in f_q$ and compute $\beth = \chi_{INT} \cdot \xi$.
- Compute $\Psi = \chi_{INT}(\lambda_X + £_X \cdot \delta_{GCN})$ *and* $\Gamma = \amalg_2(\Psi) \oplus (m, EId_{MAV})$.
- Compute $\omega = \amalg_3(EId_{MAV}, \lambda_{INT}, \lambda_X, \beth, \Gamma)$ *and* $\kappa = \chi_{INT} + \omega \cdot \Phi_{INT}$.
- Returns $(\omega, \beth, \Gamma)$.

In the above process for forging a signature, *INT* can solve two-time ECDLP such as finding the values (χ_{MAV}, Φ_{MAV}).

Probability Analysis: Suppose $Q\amalg_1$, $Q\amalg_1$, $Q\amalg_1, Q_{UPK}$, and Q_{UPRK} represent $\amalg_1$ Query, $\amalg_2$ Query, $\amalg_3$ Query, User Public Key Query, and User Private Key Query, respectively. So, we express the following events.

4. $\Theta_1 : C_{ECDDHP}$ succeeded in User Private Key Query.
5. $\Theta_2 : C_{ECDDHP}$ succeeded in Generalized Ring Signcryption Verification Query.
6. $\Theta_2 : C_{ECDDHP}$ succeeded in in challenge phase.

After denoting the above events, we can easily receive the following outcomes. $\Pr(\Theta_1) = 1 - \frac{Q_{UPRK}}{Q_{UPK}}$, $\Pr(\Theta_2) = 1 - \frac{1}{2^j}$, and $\Pr(\Theta_3) = \frac{1}{Q_{UPK} - Q_{UPRK}}$, then $\Pr(C_{ECDDHP}\ sucess) = \Pr(\Theta_1 \wedge \Theta_2 \wedge \Theta_3) = \Pr(\Theta_1) \cdot \Pr(\Theta_2) \cdot \Pr(\Theta_3) = \left(1 - \frac{Q_{UPRK}}{Q_{UPK}}\right)\left(1 - \frac{1}{2^j}\right)\left(\frac{1}{Q_{UPK} - Q_{UPRK}}\right) \approx \left(\frac{1}{Q_{UPK}}\right) \approx \frac{€}{Q_{UPK}}$, where € represents the advantage of *INT*. □

Theorem 3. Sender Anonymity. *In the key generation phase, the sender device called MAV will send his encrypted real identity* $EId_{MAV} = \gamma_{MAV} \oplus Id_{MAV}$, *and* $\Omega_{MAV} = \alpha_{MAV} \cdot \xi$, *to GCN by using open channel, where* $\gamma_{MAV} = \alpha_{MAV} \cdot \delta_{GCN}$ *and* $\alpha_{MAV} \in f_q$. *Based on* $(EId_{MAV}, \Omega_{MAV})$, *GCN firs compute* $\gamma_{MAV} = ß_{GCN} \cdot \Omega_{MAV}$ *and recover the real identity* Id_{MAV}*as* $Id_{MAV} = EId_i \oplus \gamma_{MAV}$. *Here, if INT wants the real identity* Id_{MAV}*of MAV, he will pass the following two cases.*

1. INT first struggle to access α_{MAV} from $\Omega_{MAV} = \alpha_{MAV} \cdot \xi$ to made $\gamma_{MAV} = \alpha_{MAV} \cdot \delta_{GCN}$.
2. Secondly *INT* can access $ß_{GCN}$ from $\delta_{GCN} = ß_{GCN} \cdot \xi$ to made $\gamma_{MAV} = ß_{GCN} \cdot \Omega_{MAV}$.

In both the above cases, *INT* can solve *ECDLP* which will be infeasible for him/her.

Theorem 4. Receiver Anonymity. *In the key generation phase, the receiver device called X will send his encrypted real identity* $EId_X = \gamma_X \oplus Id_X$, *and* $\Omega_X = \alpha_X \cdot \xi$, *to GCN by using open channel, where* $\gamma_X = \alpha_X \cdot \delta_{GCN}$ *and* $\alpha_X \in f_q$. *Based on* (EId_X, Ω_X), *GCN firs compute* $\gamma_X = ß_{GCN} \cdot \Omega_X$*and recover the real identity* Id_X*as* $Id_X = EId_X \oplus \gamma_X$. *Here, if INT wants the real identity* Id_X *of X, he will pass the following two cases.*

1. INT first struggle to access α_X from $\Omega_X = \alpha_X \cdot \xi$ to made $\gamma_X = \alpha_X \cdot \delta_{GCN}$.
2. Secondly INT can access $ß_{GCN}$ from $\delta_{GCN} = ß_{GCN} \cdot \xi$ to made $\gamma_X = ß_{GCN} \cdot \Omega_X$.

In both the above cases, *INT* can solve *ECDLP,* which will be infeasible for him/her.

5. Performance Comparison

This section compares the performance of the proposed scheme with the relevant existing counterparts proposed by Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16].

5.1. Computation Cost

The computation cost represents the operational expenses spent by each user during the proposed generalized ring signcryption process and existing comparable schemes proposed by Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16]. In Table 2, we

list the key operations of the proposed scheme, including Elliptic Curve Point Multiplication (ECC_{PM}), Bilinear Pairing Based Multiplication (BP_{BM}), Modular Exponentials (MD_{EXP}), and Bilinear Pairing (BP_{OP}). Table 3 contains the operating expenses, measured in milliseconds (ms), for the proposed scheme, as well as those of Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16]. The time requires for a single ECC_{PM} takes 0.97 ms, BP_{BM} , 4.31 ms, MD_{EXP} , 1.25 ms and BP_{OP} takes 14.90 [19]. The Multi-Precision Integer and Rational Arithmetic C Library (MIRACL) [20] is used to assess the performance of the proposed scheme by testing the runtime of the core cryptographic operations up to 1000 times. Observations are made on a workstation with the following specifications: 8 GB RAM and the Windows 7 Home Basic 64-bit operating system [21]. As seen in Figure 3, the proposed scheme has a lower computation cost than the schemes proposed by Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16].

Table 2. Comparison of computation cost with major operations.

Schemes	Sender	Receiver	Total
Zhou et al. [14]	$7BP_{BM} + 1MD_{EXP} + 1BP_{OP}$	$1BP_{BM} + 3BP_{OP}$	$8BP_{BM} + 1MD_{EXP} + 4BP_{OP}$
Zhou et al. [15]	$10BP_{BM} + 3MD_{EXP} + 2BP_{OP}$	$3BP_{BM} + 4BP_{OP}$	$13BP_{BM} + 3MD_{EXP} + 6BP_{OP}$
Luo and Zhou [16]	$7BP_{BM} + 2MD_{EXP}$	$1BP_{BM} + 1MD_{EXP} + 2BP_{OP}$	$8BP_{BM} + 3MD_{EXP} + 2BP_{OP}$
Proposed Scheme	$4ECC_{PM}$	$4ECC_{PM}$	$8ECC_{PM}$

Table 3. Comparison of computation cost (in ms).

Schemes	Sender	Receiver	Total
Zhou et al. [14]	$7 \times 4.31 + 1 \times 1.25 + 1 \times 14.9 = 46.32$	$1 \times 4.31 + 3 \times 14.90 = 49.01$	$8 \times 4.31 + 1 \times 1.25 + 4 \times 14.90 = 95.33$
Zhou et al. [15]	$10 \times 4.31 + 3 \times 1.25 + 2 \times 14.90 = 76.65$	$3 \times 4.31 + 4 \times 14.90 = 72.53$	$13 \times 4.31 + 3 \times 1.25 + 6 \times 14.90 = 149.18$
Luo and Zhou [16]	$7 \times 4.31 + 2 \times 1.25 = 32.67$	$1 \times 4.31 + 1 \times 1.25 + 2 \times 14.90 = 35.36$	$8 \times 4.31 + 3 \times 1.25 + 2 \times 14.90 = 68.03$
Proposed Scheme	$4 \times 0.97 = 3.88$	$4 \times 0.97 = 3.88$	$8 \times 0.97 = 7.76$

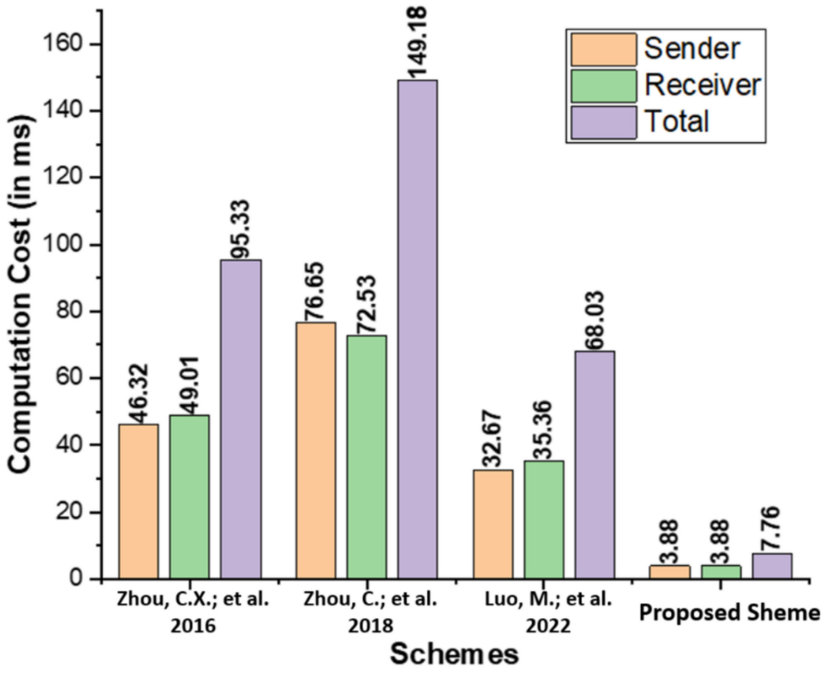

Figure 3. Comparison of computation cost (in ms) [14–16].

5.2. Communication Cost

In this subsection, the proposed scheme is compared to existing schemes, namely those proposed by Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16], in terms of communication cost. We list the communication cost incurred based on the Elliptic Curve Parameter Size ($|ECC\ q|$), Bilinear Pairing Parameter Size ($|BP\ G|$), and a message size ($|m|$) for the proposed and those of Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16]. We have selected the bit values 160, 1024, and 1024 bits for ($|ECC\ q|$), ($|m|$), and ($|BP\ G|$) from [19]. In addition, the communication cost analysis between Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16] and the proposed scheme are provided in Table 4. As seen in Figure 4, the proposed scheme has a lower communication cost than the schemes proposed by Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16].

Table 4. Comparison of communication cost (in bits).

Schemes	Communication Cost	Communication Cost in Bits
Zhou et al. [14]	$\|m\| + 3\|BP_G\|$	$\|1024\| + 3 \times \|1024\| = 4096$
Zhou et al. [15]	$\|m\| + 3\|BP_G\|$	$\|1024\| + 3 \times \|1024\| = 4096$
Luo and Zhou [16]	$\|m\| + 5\|BP_G\|$	$\|1024\| + 5 \times \|1024\| = 6144$
Proposed Scheme	$\|m\| + 2\|ECC_q\|$	$\|1024\| + 2 \times \|160\| = 1344$

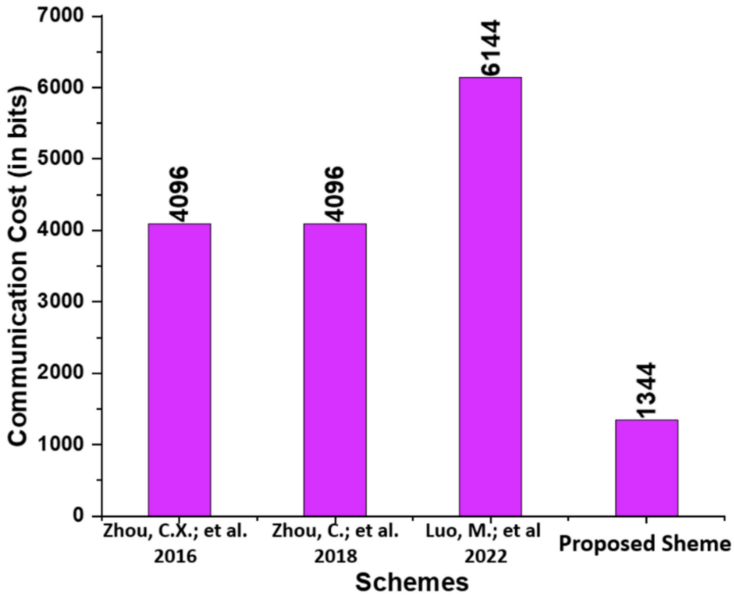

Figure 4. Comparison of communication cost (in bits) [14–16].

5.3. Memory Overhead

The proposed scheme is compared in terms of memory overhead to existing schemes proposed by by Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16]. Table 5 describes the primary operations, and Table 6 compares the memory overhead in bits of the proposed scheme to that of relevant existing schemes. A significant reduction in memory space is achieved, as shown in Figure 5.

Table 5. Memory Overhead Analysis.

Schemes	Sender	Receiver	Total
Zhou et al. [14]	$9 \mid BP_G\mid+3\mid H\mid+\mid m\mid$	$3 \mid BP_G\mid+2\mid H\mid+\mid m\mid$	$12 \mid BP_G\mid+5\mid H\mid+2\mid m\mid$
Zhou et al. [15]	$11 \mid BP_G\mid+4\mid H\mid+\mid m\mid$	$4 \mid BP_G\mid+4\mid H\mid+\mid m\mid$	$15 \mid BP_G\mid+8\mid H\mid+2\mid m\mid$
Luo and Zhou [16]	$11 \mid BP_G\mid+4\mid H\mid+\mid m\mid$	$5 \mid BP_G\mid+2\mid H\mid+\mid m\mid$	$16 \mid BP_G\mid+6\mid H\mid+2\mid m\mid$
Proposed Scheme	$10 \mid ECC_q\mid+1\mid H\mid+\mid m\mid$	$8 \mid ECC_q\mid+1\mid H\mid+\mid m\mid$	$18 \mid ECC_q\mid+2\mid H\mid+2\mid m\mid$

Note: $\mid ECC_q\mid = 160$, $\mid H\mid = 256$, $\mid BP_G\mid = 1024$, and $\mid m\mid = 1024$.

Table 6. Memory Overhead Analysis in Bits.

Schemes	Sender	Receiver	Total
Zhou et al. [14]	$9\mid 1024\mid+3\mid 256\mid+\mid 1024\mid = 10996$	$3 \mid 1024\mid+2\mid 256\mid+\mid 1024\mid = 4608$	$12 \mid 1024\mid+5\mid 256\mid+2\mid 1024\mid = 15604$
Zhou et al. [15]	$11 \mid 1024\mid+4\mid 256\mid+\mid 1024\mid = 13312$	$4 \mid 1024\mid+4\mid 256\mid+\mid 1024\mid = 6144$	$15 \mid 1024\mid+8\mid 256\mid+2\mid 1024\mid = 19456$
Luo and Zhou [16]	$11 \mid 1024\mid+4\mid 256\mid+\mid 1024\mid = 13312$	$5 \mid 1024\mid+2\mid 256\mid+\mid 1024\mid = 6656$	$16 \mid 1024\mid+6\mid 256\mid+2\mid 1024\mid = 19968$
Proposed Scheme	$10 \mid 160\mid+1\mid 256\mid+\mid 1024\mid = 2880$	$8 \mid 160\mid+1\mid 256\mid+\mid 1024\mid = 2560$	$18 \mid 160\mid+2\mid 256\mid+2\mid 1024\mid = 5440$

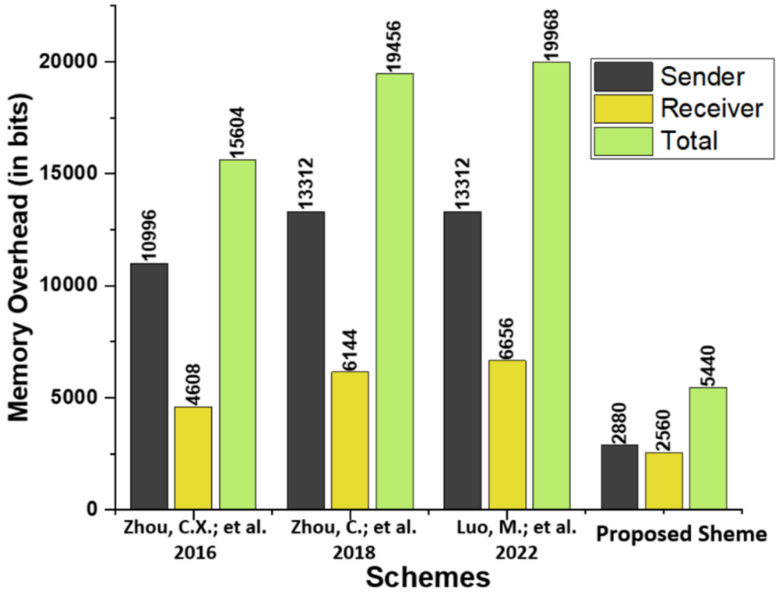

Figure 5. Comparison of memory overhead (in bits) [14–16].

6. Conclusions

In this article, we proposed a conditional privacy-preserving generalized ring signcryption scheme for MAVs using an identity-based cryptosystem. The proposed scheme is developed using the Elliptic Curve Cryptography concept (ECC). A comprehensive security analysis of ROM indicates that the proposed method is robust to a number of attacks. Comparing the proposed scheme to similar schemes presented by Zhou et al. [14], Zhou et al. [15], and Luo and Zhou [16] with regard to commutation and communication costs. The results reveal that the proposed scheme is more cost-effective in terms of computation and communication costs than its current alternatives. In addition, the results demonstrate that the proposed method is suitable for MAV systems due to the algorithm's functionality and reduced computation cost, communication cost and memory overhead.

Author Contributions: Conceptualization, I.U. and M.A.K.; Methodology, I.U., M.A.K., S.A.H.M. and A.M.A.; Software, A.M.A., S.A.H.M. and F.N.; Validation, M.A.K., F.N. and I.U.; Formal analysis, I.U. and M.A.K.; Investigation, I.U. and M.A.K.; Resources, M.A.K., F.A., N.I., S.A.H.M. and A.M.A.; Data curation, M.A.K., A.M.A., F.A., N.I. and S.A.H.M.; Writing—original draft preparation, M.A.K., S.A.H.M. and A.M.A.; Writing—review and editing, M.A.K., S.A.H.M. and A.M.A.; Visualization, A.M.A.; Funds Acquisitions, N.I.; Supervision, F.N. and M.A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by AlMaarefa University, Riyadh, Saudi Arabia (TUMA-2021-57).

Data Availability Statement: Not applicable.

Acknowledgments: Nisreen Innab would like to express her gratitude to AlMaarefa University, Riyadh, Saudi Arabia, for providing funding (TUMA-2021-57) to do this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mohsan, S.A.H.; Othman, N.Q.H.; Khan, M.A.; Amjad, H.; Żywiołek, J. A Comprehensive Review of Micro UAV Charging Techniques. *Micromachines* **2022**, *13*, 977. [CrossRef] [PubMed]
2. Liu, X.; Chen, S.W.; Nardari, G.V.; Qu, C.; Ojeda, F.C.; Taylor, C.J.; Kumar, V. Challenges and Opportunities for Autonomous Micro-UAVs in Precision Agriculture. *IEEE Micro* **2022**, *42*, 61–68. [CrossRef]
3. Ahmed, F.; Mohanta, J.C.; Keshari, A.; Yadav, P.S. Recent Advances in Unmanned Aerial Vehicles: A Review. *Arab. J. Sci. Eng.* **2022**, *47*, 7963–7984. [CrossRef] [PubMed]
4. Noor, F.; Khan, M.A.; Al-Zahrani, A.; Ullah, I.; Al-Dhlan, K.A. A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics. *Drones* **2020**, *4*, 65. [CrossRef]
5. Khan, M.A.; Kumar, N.; Mohsan, S.A.H.; Khan, W.U.; Nasralla, M.M.; Alsharif, M.H.; Zywiolek, J.; Ullah, I. Swarm of UAVs for Network Management in 6G: A Technical Review. *IEEE Trans. Netw. Serv. Manag.* **2022**. [CrossRef]
6. Khan, M.A.; Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Shah, J.A.; Uddin, I.I.; Alsharif, M.H.; Algarni, F. A Provable and Privacy-Preserving Authentication Scheme for UAV-Enabled Intelligent Transportation Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3416–3425. [CrossRef]
7. Krishna, C.G.L.; Murphy, R.R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, China, 11–13 October 2017; pp. 194–199.
8. Guo, Y.; Wu, M.; Tang, K.; Tie, J.; Li, X. Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6557–6564. [CrossRef]
9. Eldosouky, A.R.; Ferdowsi, A.; Saad, W. Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. *IEEE Internet Things J.* **2019**, *7*, 2840–2854. [CrossRef]
10. Arteaga, S.P.; Hernandez, L.A.M.; Perez, G.S.; Orozco, A.L.S.; Villalba, L.J.G. Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. *IEEE Access* **2019**, *7*, 51782–51789. [CrossRef]
11. Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997; Springer: Berlin/Heidelberg, Germany, 1997; pp. 165–179.
12. Han, Y.; Yang, X.; Wei, P.; Wang, Y.; Hu, Y. ECGSC: Elliptic curve based generalized signcryption. In Proceedings of the Third International Conference Ubiquitous Intelligence and Computing of Lecture Notes in Computer Science, Wuhan, China, 3–6 September 2006; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4159, pp. 956–965.
13. Wang, L.; Zhang, G.; Ma, C. A Secure Ring Signcryption Scheme for Private and Anonymous Communication. In Proceedings of the 2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007), Dalian, China, 18–21 September 2007; Springer: Berlin/Heidelberg, Germany, 1997; pp. 107–111.
14. Zhou, C.X.; Cui, Z.M.; Gao, G.Y. Efficient identity-based generalized ring signcryption scheme. *KSII Trans. Internet Inf. Syst.* **2016**, *10*, 5553–5571.
15. Zhou, C.; Gao, G.; Cui, Z.; Zhao, Z. Certificate-based generalized ring signcryption scheme. *Int. J. Found. Comput. Sci.* **2018**, *29*, 1063–1088. [CrossRef]
16. Luo, M.; Zhou, Y. An Efficient Conditional Privacy-preserving Authentication Protocol Based on Generalized Ring Signcryption for VANETs. *IEEE Trans. Veh. Technol.* **2022**, *71*, 10001–10015. [CrossRef]
17. Khan, M.A.; Ullah, I.; Nisar, S.; Noor, F.; Qureshi, I.M.; Khanzada, F.; Khattak, H.; Aziz, M.A. Multi-access Edge Computing (MEC) Enabled Flying Ad-hoc Networks with Secure Deployment Using Identity Based Generalized Signcryption. *Mob. Inf. Syst.* **2020**, *2020*, 8861947.
18. Din, N.; Waheed, A.; Zareei, M.; Alanazi, F. An Improved Identity-Based Generalized Signcryption Scheme for Secure Multi-Access Edge Computing Empowered Flying Ad Hoc Networks. *IEEE Access* **2021**, *9*, 120704–120714. [CrossRef]

19. Khan, M.A.; Ullah, I.; Alsharif, M.H.; Alghtani, A.H.; Aly, A.A.; Chen, C.M. An Efficient Certificate-Based Aggregate Signature Scheme for Internet of Drones. *Secur. Commun. Netw.* **2022**, *2022*, 9718580. [CrossRef]
20. Shamus Sofware Ltd. Miracl Library. Available online: http://github.com/miracl/MIRACL (accessed on 2 August 2022).
21. Zhou, C.; Zhao, Z.; Zhou, W.; Mei, Y. Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings. *Secur. Commun. Netw.* **2017**, *2017*, 8405879. [CrossRef]