sensors

MDPI

Article

A Privacy-Preserved ID-Based Secure Communication Scheme in 5G-IoT Telemedicine Systems

Tzu-Wei Lin [1,2]

[1] i. School, Feng Chia University, Taichung 402, Taiwan; tweilin@fcu.edu.tw
[2] Information Security Office, Office of Information Technology, Feng Chia University, Taichung 402, Taiwan

Abstract: 5G networks have an efficient effect in providing quality of experience and massive Internet of things (IoT) communication. Applications of 5G-IoT networks have been expanded rapidly, including in smart medical healthcare. Emergency medical services (EMS) hold an assignable proportion in our lives, which has become a complex network of all types of professionals, including care in an ambulance. A 5G network with EMS can simplify the medical treatment process and improve the efficiency of patient treatment. The importance of healthcare-related privacy preservation is rising. If the work of privacy preservation fails, not only will medical institutes have economic and credibility losses but also property losses and even the lives of patients will be harmed. This paper proposes a privacy-preserved ID-based secure communication scheme in 5G-IoT telemedicine systems that can achieve the features below. (i) The proposed scheme is the first scheme that integrates the process of telemedicine systems and EMS; (ii) the proposed scheme allows emergency signals to be transmitted immediately with decreasing risk of secret key leakage; (iii) the information of the patient and their prehospital treatments can be transmitted securely while transferring the patient to the destination medical institute; (iv) the quality of healthcare services can be assured while preserving the privacy of the patient; (v) the proposed scheme supports not only normal situations but also emergencies. (vi) the proposed scheme can resist potential attacks.

Keywords: telemedicine systems; 5G; IoT; emergency medical services; privacy preservation

Citation: Lin, T.-W. A Privacy-Preserved ID-Based Secure Communication Scheme in 5G-IoT Telemedicine Systems. *Sensors* **2022**, *22*, 6838. https://doi.org/10.3390/s22186838

Academic Editors: Tomas Cerny, Jiman Hong and Dongwan Shin

Received: 15 August 2022
Accepted: 6 September 2022
Published: 9 September 2022

1. Introduction

The 5G (fifth generation) networks are the newest standard of mobile telecommunication that is being deployed on the earth. 5G networks provide speed, capacity, and scalability, which have an efficient effect on energy consumption and provide quality of services (QoS) and amount of devices communication [1,2]. A device connects with a small base station through high-band spectrum technology and devices-to-devices communication [1,3,4]. 5G networks combine and connect virtual systems to the cloud and help derive different calculating models [5]. 5G networks will have a huge impact on connected services and devices through higher reliability, connectivity, and storage [5]. Internet of things (IoT) arranges objects as a part of network settings in a distributed network. IoT has become a concept of enclosing several technologies and a network between objects and human beings, which can interact and cooperate with other devices to communicate and share information. The vision of next-generation 5G wireless communications lies in providing very high data rates, extremely low latency, manifold an increase in base station capacity, and significant improvement in users' perceived quality of service compared to current 4G LTE networks [6]. 5G can significantly increase the capacity and speed to provide reliable and speedy connectivity to the future IoT and, moreover, provide reliable connections to thousands of devices at the same time [7]. 5G will be able to provide a massive connection of Internet of things (IoT), where billions of smart devices can be connected to the internet [7]. However, security and privacy issues of transmitted information

between objects are rising these years because wireless communications are vulnerable to many adversarial attacks, which is an important transmitting media of IoT networks.

Medical healthcare systems currently have many challenges, such as infrastructure, connections, professional requirements, data management, real-time monitoring, etc., and each challenge affects the quality of healthcare services [8]. Applications of 5G networks have been expanded rapidly, including in healthcare, and IoT with 5G environments provides solutions for network layers, including enhancing QoS to solve the challenges above [1,4]. On the other hand, the importance of healthcare-related privacy preservation is rising. If the work of privacy preservation fails, not only will medical institutes have economic and credibility losses but also property losses and even the lives of patients will be harmed. Maintaining the privacy of patient data, which is usually stored in conventional systems and difficult to share due to varying standards and data formats, is one of the important sectors of the healthcare industry. If the healthcare information of patients is the key to finding medical treatment, maintaining the privacy of patient data becomes a central issue that determines the success of medical practices [8].

Emergency medical services (EMS) hold an assignable proportion in our lives, which has become a complex network of all types of professionals, including care in an ambulance, serving as educators, practicing community paramedicine, and conducting research [9]. EMS has to be the first to respond and take care of minor and major injured patients while attending to calls coming from different situations, such as accidents, natural disasters, terrorism, pandemics, and patient transport. The state of California Emergency Medical Services Authority of US developed a search, alert, file, and reconcile (SAFR) model to reach goals of bidirectional data exchange between the EMS and the health information exchange (HIE) organization to enhance prehospital treatments, prehospital decision-making, better longitudinal patient record, and overall care [10]. The 5G network has the potential to bring benefits to individuals, organizations, and society, which enables ambulances to connect a patient who wears wearable devices to the emergency department of the destination hospital. Measured biodata is collected at the incident scene and transmitted to the servers of the destination hospital when the patient is being transported, which can allow the medical professional team at the destination hospital to immediately realize the condition of the patient, the prehospital treatment performed by a medical professional on an ambulance, and help decision-making. Measured biodata can be interconnected with hospital information systems, laboratory information systems, geographic information systems, picture archiving and communications systems, and document management systems, which enable medical professionals in destination hospitals to realize the historical medical records of patients, decide first-aid information, and issue examination sheets. 5G networks with EMS can simplify the medical treatment process and improve the efficiency of patient treatment [11].

This paper proposes a privacy-preserved ID-based secure communication scheme in 5G-IoT telemedicine systems that can achieve the features below. (i) The proposed scheme allows emergency signals to be transmitted immediately with decreasing risk of secret key leakage; (ii) the information of the patient and their prehospital treatments can be securely transmitted while transferring the patient to the destination medical institute; (iii) the quality of healthcare services can be assured while preserving the privacy of the patient; (iv) the proposed scheme supports not only normal situations but also emergencies. (v) the proposed scheme can resist potential attacks. The remaining organization of paper is sketched below. Telemedicine systems, federal identity management mechanisms, key insulation, and Chebyshev chaotic maps are introduced in Section 2. Section 3 introduces the proposed scheme, and security and performance analysis are detailed in Sections 4 and 5. Finally, the conclusion is drawn in Section 6.

2. Related Works

Telemedicine systems are a combination of healthcare, electronic messaging, and telecommunication technology [8,12,13]. Patients can transmit healthcare-related infor-

mation, which is usually important, sensitive, and private, to healthcare services through public networks when using telemedicine systems [8,12,13]. This means that medical professionals are able to know the health condition of a patient immediately and following up on the health condition of the patient becomes more convenient than before [12]. A general telemedicine system in 5G-IoT environments includes three types of telemedicine, which are synchronous telemedicine, asynchronous telemedicine, and remote health monitoring [2,14]. Synchronous telemedicine allows the patient and the medical professional to communicate directly through telecommunication technology, such as Microsoft Teams (version 1.5, Microsoft Corporation, Washington, US), Cisco Webex (version 42.9, Cisco Systems, San Jose, California, US), Zoom (version 5.11, Zoom Video Communications, Inc., San Jose, California, US), etc. Asynchronous telemedicine means that the medical professional can follow up on the patient's health condition through biodata continually transmitted by the patient and stored and analyzed by the server in the medical institute. Furthermore, the system can automatically notify the medical professional when the patient's health condition turns bad after analyzing and predicting the biodata. Remote health monitoring allows the medical professional in real-time to monitor the patient's health condition, and the medical professional can receive an alert immediately if an emergency happens to the patient through this type of telemedicine. This paper focuses on the scenarios of remote health monitoring and asynchronous telemedicine. Meanwhile, data transmission security will be discussed, such as eavesdropping, man-in-the-middle (MITM) attack, data tempering attack, message modification attack, data interception attack, etc. [8,15]. Technical support is not enough though famous regulations providing personal information privacy have been announced [8,15].

Shamir introduced an identity-based (ID-based) cryptosystem [16], and an ID-based cryptosystem derives the user's public key from the public and unique information of the user. Gentry et al. developed hierarchical ID-based cryptography (HIDC) based on the original ID-based cryptosystem, and HIDC has been proven to reduce the loading of private key generation and the risk of key escrow [17]. Several works have been proposed in the past two decades [18–21], including Santos et al.'s work, which is a lightweight federal identity management mechanism for IoT [22]. Moreover, Lin and Hsu [8] proposed a hierarchical ID-based cryptography for federal identity management in telemedicine in a 5G-IoT environment, which includes IoT gateways in the system structure. The proposed scheme applied a similar structure that the smart lamp replaces IoT gateway in the work of Lin and Hsu [8], and the scenario of the proposed scheme includes an emergency that is not included in Lin and Hsu's work [8].

Key insulation, which is introduced by Dodis et al., is one of the effective solutions to a key exposure problem [23]. More and more wearable healthcare devices are used, and they only have limited resources to protect keys. Any malicious adversary can easily obtain the key information of users or devices, which leads to the key exposure problem. Once a private key is compromised, a malicious adversary has the chance to use the exposed private key to submit a legitimate request [24]. In a public key cryptosystem that is key-insulated, a receiver has two types of secret keys, a decryption key and a helper key. The decryption key is a short-term key for decrypting ciphertexts and is periodically updated by the helper key. More specifically, the lifetime of a system is divided into discrete time periods, and the receiver can decrypt the ciphertext, which is encrypted at some time period, by using a decryption key updated by the helper key at the same time period. The decryption key is stored in a powerful but insecure device such as portable healthcare devices, and the helper key is stored in a physically secure but computationally limited device called a helper, such as a smartphone. Key-insulated encryption can significantly reduce the impact of the key exposure problem, and many researchers have taken several approaches to realize secure key-insulated cryptosystems. Many cryptographers have proposed several types of key-insulated cryptographic schemes, such as symmetric-key-based key-insulated encryption [23], key-insulated signatures [25], parallel key-insulated encryption [24,26], etc.

A chaotic system has features that can correspond to important features, confusion and diffusion of cryptosystems [27–29]. First, the result of a chaotic system is unpredictable if small changes in initial values happen [27,30]. Second, a chaotic system is a complex oscillation [27,30]. Third, a chaotic system has a qualitative change of character of solutions [27,30]. Cryptosystems based on Chebyshev chaotic maps have been widely discussed for decades, including lightweight solutions [13,28,29,31–33]. Mathematical definitions of Chebyshev chaotic maps are given in Table 1 [13,28,29,31–33]. Proposed schemes in this paper apply extended Chebyshev chaotic maps that satisfy definitions in Table 1.

Table 1. Mathematical definitions of Chebyshev chaotic maps.

Mathematical Definitions	Descriptions
Chebyshev polynomial	Chebyshev polynomial $T_n(x): \rightarrow [-1,1]$ is a polynomial in x of degree n, defined as $T_n(x) = \cos(n\cos^{-1}(x))$.
Recurrent relation	$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$ for any $n \geq 2$, $T_0(x) = 1$, and $T_1(x) = x$.
Semi-group property	$T_r(T_s(x)) = T_{rs}(x) = T_s(T_r(x))$ for any $(s, r) \in Z$ and $s \in [-1,1]$. Chebyshev polynomial restricted to interval [–1, 1] is a well-known chaotic map for all $n > 1$, which has a unique continuous invariant measure with positive Lyapunov exponent ln n. For $n = 2$, Chebyshev maps reduces to well-known logistic maps.
Extended Chebyshev polynomials	Zhang [34] proved that the semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$, and extended Chebyshev polynomials is defined as $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \bmod N$, where $n \geq 2$, $x \in (-\infty, +\infty)$, and N is a large prime number. Semi-group property holds, and extended Chebyshev polynomials also commute as $T_r(T_s(x)) \bmod N = T_{rs}(x) \bmod N = T_s(T_r(x)) \bmod N$.
Chaotic maps-based discrete logarithm problem (CMDLP)	Given two elements x and y, it is computationally infeasible to find the integer n such that $T_n(x) \bmod N = y$.
Chaotic maps-based Diffie-Hellman problem (CMDHP)	Given three elements x, $T_r(x) \bmod N$, and $T_s(x) \bmod N$, it is computationally infeasible to compute $T_{rs}(x) \bmod N$.

3. Proposed Scheme

In this paper, a scenario that includes a patient Pa_i, a smart lamp SL_j, an ambulance A_{ij}, and a server of a medical institute (MS) is focused as illustrated in Figure 1.

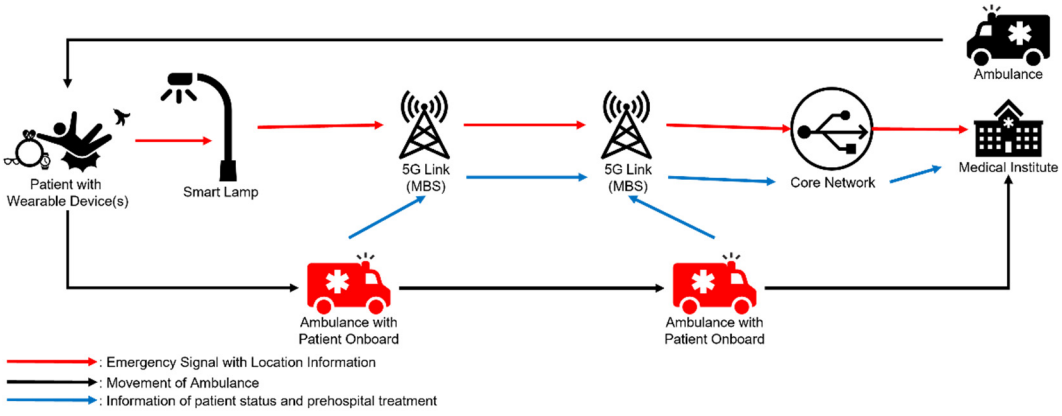

Figure 1. System structure of proposed scheme.

Once an emergency occurs to the patient, an emergency signal is sent by the wearable device(s) to a nearby smart lamp, and then the smart lamp transmits a signal to the nearest medical institute. Another way for the smart lamp to send an emergency signal is for other passersby nearby the patient to press the emergency button on the smart lamp, as in Figure 2. After receiving the signal, a medical institute resolves the location of the patient, transmits related information to EMS staff, and assigns an ambulance to the site. After EMS staff move the patient into the ambulance, EMS can send information about the patient, including status and prehospital treatments to the destination medical institute. The staff of the emergency department at the destination medical institute can provide

proper treatment according to the information on the prehospital treatments after receiving the patient. The interaction between 5G links and a core network should be secure, which may be guaranteed by functions in the core network, but secure communication between 5G links and a core network is not discussed in the proposed scheme.

Figure 2. Smart lamp with emergency button.

The proposed scheme has five phases: system initialization phase, registration phase, key update phase, emergency signal sending phase, and secure ambulance communication phase. In the system initialization phase, the server of the medical institute (MS) generates essential parameters and functions. The patient (Pa_i), smart lamp (SL_j), and ambulance (A_{ij}) become legitimate parties through a registration phase. In the key update phase, a patient's (Pa_i's) smartphone can help a patient (Pa_i) update keys and secure a component in the smart lamp that can help the smart lamp (SL_j) update keys. In the secure ambulance communication phase, the ambulance (A_{ij}) and the smart lamp (SL_j) authenticate each other and establish a session key for symmetric encryption for communication and transmitted information on the status and prehospital treatments. Notations are defined in Table 2.

Table 2. Notations of proposed scheme.

Notations	Definitions
PID_i	Identity of patient Pa_i
$SLID_j$	Identity of smart lamp SL_j.
AID_{ij}	Identity of ambulance A_{ij}.
k	Encryption/decryption key k.
$E_k(.)/D_k(.)$	A symmetric encryption/decryption algorithm with secret key k.
S_j	Private key of smart lamp SL_j.
S_{ij}	Private key of ambulance A_{ij}.
$sk_{SL_j \leftrightarrow A_{ij}}$	Session key of smart lamp SL_j and ambulance A_{ij}.
p, p_j, q_j	Large random prime numbers.
x, e_j, d_j	Random numbers.
$h_k(.)$	Collision-resistance secure one-way keyed chaotic hash function.
s_{MS}, ω_{MS}	The secrete values of server of medical institute (MS).
$\oplus$	Exclusive OR (XOR) operation.
A ?= B	Checking if value A is equal to B or not.
MAC_A	The message authentication code algorithm of A.
$Certificate_{HCA \rightarrow MS}$	Certification issued by healthcare certification authority to a server of a medical institute *(MS)*.
$Certificate_{MS \rightarrow SL_j}$	Certification issued by a server of a medical institute (MS) to a smart lamp SL_jthat is generated from $Certificate_{HCA \rightarrow MS}$.
$Certificate_{SL_j \rightarrow A_{ij}}$	Certification issued by a smart lamp SL_j to an ambulance A_{ij}that is generated from $Certificate_{MS \rightarrow SL_j}$.
w	Warrant including delegation information.
b_i, b_s	Number of key update time.
EM_i	Emergency signal.

3.1. System Initialization Phase

In the system initialization phase, a server of a medical institute (MS), which provides telemedicine services and is certified by a healthcare certification authority, sets up parameters by performing the following steps.

Step 1: The healthcare certification authority issues a certificate $Certificate_{HCA \to MS}$ to the server of a medical institute (MS) that provides telemedicine services and is certified by a healthcare certification authority.

Step 2: The server of a medical institute (MS) generates secret values $(s_{MS}, \omega_{MS}) \in Z_p^*$, a big prime p, and a random number $x \in (-\infty, +\infty)$ and computes P_{MS} and P_{HA} according to mathematical definitions of extended Chebyshev polynomials in Table 1.

$$P_{MS} = T_{s_{MS}}(x) \bmod p \tag{1}$$

$$P_{HA} = T_{\omega_{MS}}(x) \bmod p \tag{2}$$

Step 3: The server of a medical institute (MS) chooses a symmetric encryption algorithm $E_k(.)$, a symmetric decryption algorithm $D_k(.)$, collision-resistance one-way hash functions ($H_0(.)$, $H_1(.)$, $H_2(.)$) where $H : \{0, 1\}^* \to \{0, 1\}^n$ that takes a binary string $q \in \{0, 1\}^*$ of any arbitrary length as input and produces a binary string $H_q \in \{0, 1\}^n$ as an output, and a collision-resistance secure one-way chaotic keyed hash function $h_k(.)$.

Step 4: The server of a medical institute (MS) outputs public parameters $\{P_{MS}, P_{HA}, p, x, H_0(.), H_1(.), H_2(.), h_k(.), E_k(.), D_k(.)\}$ and private parameters (s_{MS}, ω_{MS}).

Step 5: The smart lamp (SL_j) generates two large random primes (p_j, q_j), and φ_j. Then, the smart lamp (SL_j) selects a random integer e_j, where $1 < e_j < \varphi_j$ and $\gcd(e_j, \varphi_j) = 1$, and makes it public. After that, the smart lamp (SL_j) computes d_j, where $1 < d_j < \varphi_j$ and $e_j d_j \equiv 1 \pmod{\varphi_j}$ and keeps d_j secretly.

3.2. Registration Phase

In this phase, the patient (Pa_i) and the smart lamp (SL_j) interact with the server of a medical institute (MS) for registration, and the ambulance (A_{ij}) interacts with the smart lamp (SL_j) for registration via a secure channel. To deal with the registration request submitted by the patient (Pa_i) and the smart lamp (SL_j), the server of a medical institute (MS) validates the legitimacy of the patient Pa_I and the smart lamp SL_j. After that, the server of a medical institute (MS) issues a private key (S_j) and a certificate $Certificate_{MS \to SL_j}$ via a secure channel while computing and sending σ_I to the patient (Pa_i). The ambulance (A_{ij}) submits registration information to the smart lamp (SL_j), and the smart lamp (SL_j) verifies the ambulance's (A_{ij}) legitimacy then issues private key (S_{ij}) and certificate $Certificate_{SL_j \to A_{ij}}$. Detailed descriptions are stated as follows and illustrated in Figure 3.

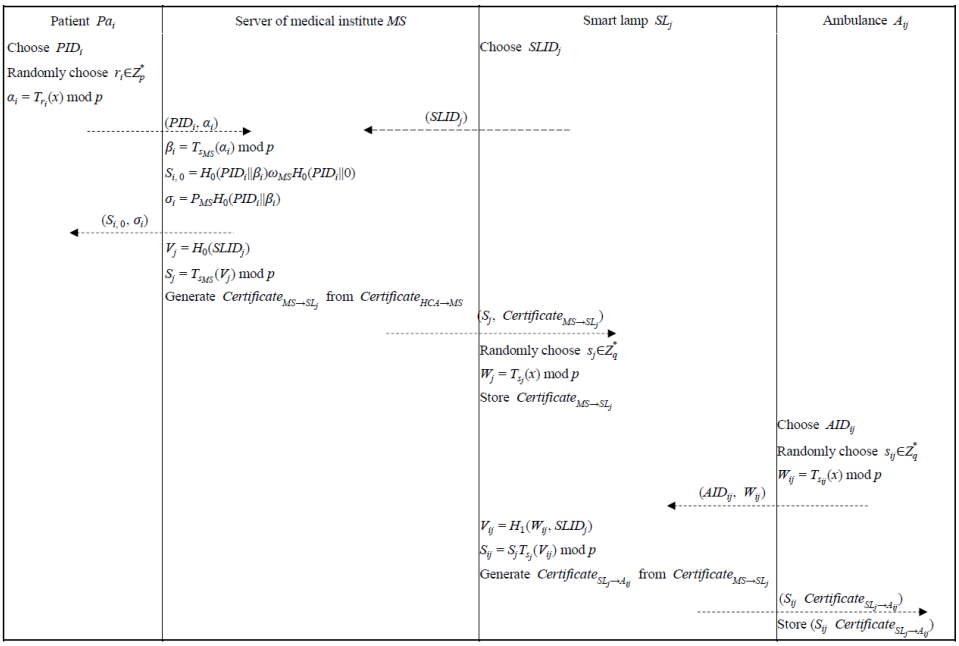

Figure 3. Registration phase.

Step 1: The patient, Pa_i, chooses an identifier, PID_i, and a random number, $r_i \in Z_p^*$, and computes α_i. After that, the patient, Pa_i, sends (PID_i, α_i) to the server of a medical institute (*MS*). Meanwhile, the smart lamp, SL_j, chooses an identifier, $SLID_j$, and submits to the server of a medical institute (*MS*).

$$\alpha_i = T_{r_i}(x) \bmod p \tag{3}$$

Step 2: After receiving (PID_i, α_i) from the patient (Pa_i) and $SLID_j$ from the smart lamp (SL_j), the server of a medical institute (*MS*) computes the elements below. Then, the server of a medical institute (*MS*) returns ($S_{i,0}$, σ_i) to the patient (Pa_i) and S_j with $Certificate_{MS \to SL_j}$, which is generated by the server of a medical institute (*MS*), to the smart lamp (SL_j).

$$\beta_i = T_{s_{MS}}(\alpha_i) \bmod p \tag{4}$$

$$S_{i,0} = H_0(PID_i || \beta_i) \omega_{MS} H_0(PID_i || 0) \tag{5}$$

$$\sigma_i = P_{MS} H_0(PID_i || \beta_i) \tag{6}$$

$$V_j = H_0(SLID_j) \tag{7}$$

$$S_j = T_{s_{MS}}(V_j) \bmod p \tag{8}$$

Step 3: The smart lamp (SL_j) chooses a random number $s_j \in Z_q^*$ as a secret value and computed W_j and stores $Certificate_{MS \to SL_j}$.

$$W_j = T_{s_j}(x) \bmod p \tag{9}$$

Step 4: The ambulance (A_{ij}) chooses an identifier (AID_{ij}) and a random number ($s_{ij} \in Z_p^*$) as a secret value, computes W_{ij}, and sends (AID_{ij}, W_{ij}) to the smart lamp (SL_j).

$$W_{ij} = T_{s_{ij}}(x) \bmod p \tag{10}$$

Step 5: After receiving AID_{ij} from the ambulance (A_{ij}), the smart lamp (SL_j) checks the format of AID_{ij}. If AID_{ij} is valid, the smart lamp SL_j computes a private key S_{ij} corresponding to the AID_{ij}, then generates the $Certificate_{SL_j \to A_{ij}}$ from the $Certificate_{MS \to SL_j}$, and sends ($S_{ij}$, $Certificate_{SL_j \to A_{ij}}$) to the ambulance ($A_{ij}$) via a secure channel.

$$V_{ij} = H_1(W_{ij}, SLID_j) \tag{11}$$

$$S_{ij} = S_j T_{s_j}(V_{ij}) \bmod p \tag{12}$$

Step 6: The ambulance (A_{ij}) stores (S_{ij}, $Certificate_{SL_j \to A_{ij}}$).

3.3. Key Update Phase

The patient's (Pa_i's) smartphone can help the patient (Pa_i) update keys through following the steps as illustrated in Figure 4.

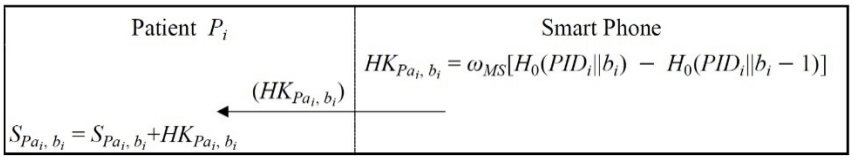

Figure 4. Key update phase.

Step 1: The smartphone computes and sends the helper key HK_{Pa_i, b_i} as below.

$$HK_{Pa_i, b_i} = \omega_{MS}[H_0(PID_i || b_i) - H_0(PID_i || b_i - 1)] \tag{13}$$

Step 2: After receiving HK_{Pa_i, b_i}, the patient (Pa_i) computes S_{Pa_i, b_i} to update the key.

$$S_{Pa_i,\, b_i} = S_{Pa_i,\, b_i} + HK_{Pa_i,\, b_i} \tag{14}$$

3.4. Emergency Signal Sending Phase

When an emergency happens to a patient (Pa_i) outdoors, the patient (Pa_i) can commission a nearby smart lamp (SL_j) to sign and send an emergency signal (EM_i) to a server of a medical institute (MS). The server of the medical institute (MS) can verify the message from patient (Pa_i) through the following steps as illustrated in Figure 5.

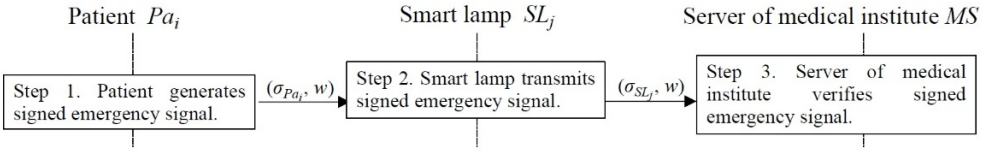

Figure 5. Emergency signal sending phase.

Step 1: The patient generates a signed emergency signal. The patient (Pa_i) computes ($\sigma_{Pa_i}1$, $\sigma_{Pa_i}2$) as below and sends (σ_{Pa_i}, w) to the smart lamp (SL_j) that w is a warrant including delegation information generated by patient (Pa_i).

$$\sigma_{Pa_i}1 = S_{Pa_i,\, b_i} r_i H_1(EM_i) \tag{15}$$

$$\sigma_{Pa_i}2 = \alpha_i \tag{16}$$

$$\sigma_{Pa_i} = (\sigma_{Pa_i}1,\ \sigma_{Pa_i}2,\ EM_i,\ b_i) \tag{17}$$

Step 2: The smart lamp transmits a signed emergency signal. After receiving (σ_{Pa_i}, w), the smart lamp (SL_j) computes ($\sigma_{SL_j}1$, $\sigma_{SL_j}2$, $\sigma_{SL_j}3$) as below and sends (σ_{SL_j}, w) to the server of the medical institute (MS).

$$\sigma_{SL_j}1 = \sigma_{Pa_i}1 S_{SL_j,\, b_j} r_i H_2(EM_i) r_i H_1(w) \tag{18}$$

$$\sigma_{SL_j}2 = \sigma_{Pa_i}2 \alpha_i \tag{19}$$

$$\sigma_{SL_j}3 = \alpha_i \tag{20}$$

$$\sigma_{SL_j} = (\sigma_{SL_j}1,\ \sigma_{SL_j}2,\ \sigma_{SL_j}3,\ EM_i,\ b_i,\ b_j) \tag{21}$$

Step 3: The server of the medical institute verifies the signed emergency signal. After receiving (σ_{SL_j}, w), the server of the medical institute (MS) verifies the message as below. If it holds, the server of the medical institute (MS) can confirm that the message was sent from the patient (Pa_i). The server of the medical institute (MS) utilizes information from the smart lamp ($\sigma_{SL_j}1$, $\sigma_{SL_j}2$, $\sigma_{SL_j}3$, EM_i, b_j) to compute verification parameters (ν_1, ν_2, ν_4, ν_5, ν_6, ν_7). In addition, the smart lamp (SL_j) sends information of the owner of the emergency signal patient Pa_i and b_i, so the medical institute (MS) is able to compute the verification parameter, ν_3. Finally, the medical institute (MS) verifies the validity of the emergency signal by checking the equality between ν_1 and (ν_2, ν_3, ν_4, ν_5, ν_6, ν_7) with P_{MS} and P_{HA}. The process of verification can be referred to in [35], which has been proven.

$$\nu_1 = T_{\sigma_{SL_j}1}(x) \bmod p \tag{22}$$

$$\nu_2 = T_{H_0(PID_i || \sigma_{SL_j}2)}(x) \bmod p \tag{23}$$

$$\nu_3 = T_{H_1(PID_i || b_i)}(x) \bmod p \tag{24}$$

$$\nu_4 = T_{H_1(EM_i)}(x) \bmod p \tag{25}$$

$$\nu_5 = T_{H_0(SLID_j || \sigma_{SL_j}3)}(x) \bmod p \tag{26}$$

$$\nu_6 = T_{H_1(SLID_j || b_j)}(x) \bmod p \tag{27}$$

$$\nu_7 = T_{H_2(EM_i)}(x) \bmod p \tag{28}$$

$$\nu_1 \, ? = \nu_2 P_{MS} \nu_3 P_{HA} \nu_4 \sigma_{P_i} 2 \nu_5 P_{MS} \nu_6 P_{HA} \nu_7 \sigma_{SL_j} 3 \tag{29}$$

3.5. Secure Ambulance Communication Phase

After the ambulance (A_{ij}) picks up the patient (Pa_i), the ambulance (A_{ij}) can initiate communication with the server of the medical institute (MS) through the smart lamp (SL_t). The smart lamp (SL_t) and the ambulance (A_{ij}) will execute mutual authentication to ensure further interaction between the smart lamp (SL_t) and the ambulance (A_{ij}). Detailed descriptions are stated as follows and illustrated in Figure 6.

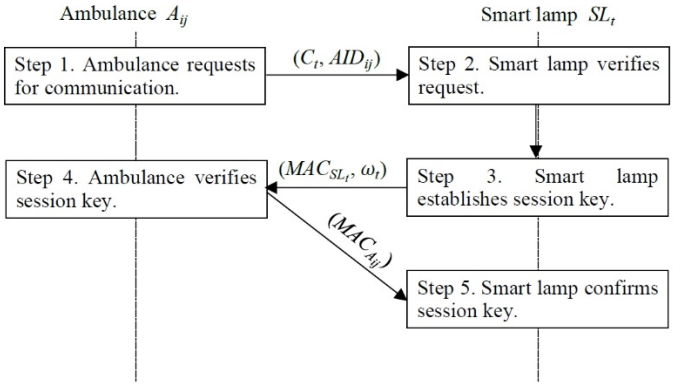

Figure 6. Secure ambulance communication phase.

Step 1: The ambulance requests for communication. The ambulance (A_{ij}) chooses a random number (a_{ij}), computes μ_{ij} and C_t, and sends (C_t, AID_{ij}) to the smart lamp (SL_t).

$$\mu_{ij} = T_{s_{ij}}(a_{ij}) \bmod p \tag{30}$$

$$C_t = (T_{e_t}(\mu_{ij} || a_{ij} || Certificate_{SL_j \to A_{ij}}) \bmod p) P_t \tag{31}$$

Step 2: The smart lamp verifies the request. After receiving (C_t, AID_{ij}), the smart lamp (SL_t) obtains $(\mu_{ij} || a_{ij} || Certificate_{SL_j \to A_{ij}})$ by decrypting P_t and verifies if the $Certificate_{SL_j \to A_{ij}}$ is valid. If the $Certificate_{SL_j \to A_{ij}}$ is valid, the smart lamp (SL_t) progresses to the steps below, or the smart lamp (SL_t) abandons the request.

$$(\mu_{ij} || a_{ij} || Certificate_{SL_j \to A_{ij}}) = (T_{d_t}(C_t) \bmod p) / P_t \tag{32}$$

Step 3: The smart lamp establishes a session key. The smart lamp (SL_t) computes (ω_t, $sk_{SL_t \leftrightarrow A_{ij}}$, P_j, P_{ij}, P_t, k, MAC_{SL_t}) and sends (MAC_{SL_t}, ω_t) to the ambulance (A_{ij}).

$$\omega_t = T_{s_t}(a_{ij}) \bmod p \tag{33}$$

$$sk_{SL_t \leftrightarrow A_{ij}} = H_2(T_{s_t}(\mu_{ij}) \bmod p) \tag{34}$$

$$P_j = H_1(SLID_j) \tag{35}$$

$$P_{ij} = H_1(W_{ij}, SLID_j) \tag{36}$$

$$P_t = H_0(SLID_t) \tag{37}$$

$$k = (P_j || W_0) \oplus (P_{ij} || W_i) \oplus \left(P_t || W_{ij}\right) \oplus \left(sk_{SL_t \leftrightarrow A_{ij}} || \omega_t\right) \tag{38}$$

$$MAC_{SL_t} = h_k(P_t, P_{ij}, \mu_{ij}) \tag{39}$$

Step 4: The ambulance verifies the session key. After receiving (MAC_{SL_t}, ω_t), the ambulance (A_{ij}) computes ($sk'_{SL_t \leftrightarrow A_{ij}}$, k') and verifies MAC_{SL_t}. If the result of the verification is true, the ambulance (A_{ij}) computes $MAC_{A_{ij}}$ and sends $MAC_{A_{ij}}$ to the smart lamp (SL_t).

$$sk'_{SL_t \leftrightarrow A_{ij}} = H_2\left(T_{s_{ij}}(\omega_t) \bmod p\right) \tag{40}$$

$$k' = \left(P_j || W_0\right) \oplus \left(P_{ij} || W_i\right) \oplus \left(P_t || W_{ij}\right) \oplus \left(sk'_{SL_t \leftrightarrow A_{ij}} || \omega_t\right) \tag{41}$$

$$h_{k'}\left(P_t,\ P_{ij},\ \mu_{ij}\right) ? = MAC_{SL_t} \tag{42}$$

$$MAC_{A_{ij}} = h_{sk'_{SL_t \leftrightarrow A_{ij}}}\left(P_{ij},\ P_t, \omega_t\right) \tag{43}$$

Step 5: The smart lamp confirms the session key. After receiving $MAC_{A_{ij}}$, the smart lamp (SL_t) verifies $MAC_{A_{ij}}$. If the result of the verification is true, a mutual authentication and key agreement is completed.

$$h_{sk_{SL_t \leftrightarrow A_{ij}}}(P_{ij},\ P_t, \omega_t) ? = MAC_{A_{ij}} \tag{44}$$

4. Security Analysis

This paper applies the random oracle model [36] and BAN logic [37] for formal security proof. The random oracle model [36] is used to prove the security of the emergency signal sending phase, and BAN logic [37] is used to prove the secure authentication of the secure ambulance communication phase. Note that the process of the random oracle model proof [36] can refer to other works using the random oracle model, including Liu's work [38], because of a similar process of proof that aims to prove that the schemes can against eavesdropping attack to the Diffie–Hellman key exchange scheme. In addition, the process of BAN logic [37] can refer to other works using BAN logic, including Lee et al.'s [32] and Lin and Hsu's [13] works, because of a similar process of proof that aims to prove that principals in schemes can believe established session keys. This paper will not describe the random oracle model and the BAN logic proof in detail. Informal security presents theoretical analyses that are present for proof of fulfillment of the security requirements of the proposed scheme.

4.1. Security of Secret Key

Assume an adversary wants to obtain the master secret key obtained by the server of the medical institute (MS), the smart lamp (SL_j), and the ambulance (A_{ij}), such that $P_{MS} = T_{s_{MS}}(x) \bmod p$ and $W_j = T_{s_j}(x) \bmod p$. The adversary must have to solve the question based on CMDLP. If the adversary wants to obtain the smart lamp's (SL_j's) secret key, the adversary is required to solve the question based on CMDLP. On the other hand, the smart lamp (SL_j) generates the secret key for the ambulance (A_{ij}) by performing $S_{ij} = S_j T_{s_j}(V_{ij}) \bmod p$. The smart lamp ($SL_j$) uses a private key ($S_j$) and a secret key ($s_j$) in the computing process, hence only the smart lamp (SL_j) is able to know the ambulance's (A_{ij}'s) secret key.

4.2. Key Confirmation and Security of Session Key

The ambulance (A_{ij}) can check the session key ($sk_{SL_t \leftrightarrow A_{ij}}$) by $MAC_{SL_t} ? = h_{k'}(P_t,\ P_{ij},\ \mu_{ij})$, and the smart lamp ($SL_t$) can also check the session key ($sk_{SL_t \leftrightarrow A_{ij}}$) through $MAC_{A_{ij}} ? = h_{sk_{SL_t \leftrightarrow A_{ij}}}\left(P_{ij},\ P_t, \omega_t\right)$ in the proposed scheme. If the adversary wants to obtain the session key ($sk_{SL_t \leftrightarrow A_{ij}}$), the adversary has to solve CMDHP. Moreover, the session key ($sk_{SL_t \leftrightarrow A_{ij}}$) is not the same every time because of the random number (a_{ij}). As a result, the proposed scheme achieves key confirmation while securing the session key.

4.3. Preventing Key-Compromise Impersonation Attacks

The ambulance's (A_{ij}'s) random number (s_{ij}) can be stored in the onboard unit of the ambulance, which is hard to obtain information. On the other hand, the adversary cannot obtain k due to not knowing s_t, and afterwards, the process cannot be completed by the adversary. As a result, the proposed scheme can prevent key-compromise impersonation attacks.

4.4. Mutual Authentication

In the secure ambulance communication phase, the ambulance (A_{ij}) and the smart lamp (SL_t) compute their session key k by public parameters ($SLID_t$, AID_{ij}, W_{ij}, $SLID_j$). In addition, each party generates a message authentication code (MAC_{SL_t}) and $MAC_{A_{ij}}$ by k and $sk_{SL_t \leftrightarrow A_{ij}}$ respectively to verify each other's validity. Moreover, because of the feature of HIDC, the smart lamp (SL_t) can realize that the ambulance (A_{ij}) comes from the cloud services provider by public parameter AID_{ij}.

4.5. Preventing MITM Attack

In order to prevent an MITM attack in the secure ambulance communication phase, the ambulance (A_{ij}) and the smart lamp (SL_t) can confirm whether the message is resent, modified, and replaced, by checking the information through message authentication codes MAC_{SL_t} and $MAC_{A_{ij}}$. This means that the adversary cannot modify the message authentication codes MAC_{SL_t} and $MAC_{A_{ij}}$ without the session key $sk_{SL_t \leftrightarrow A_{ij}}$. Thus, the proposed scheme can prevent an MITM attack.

4.6. Unforgeability

If the adversary wants to forge a validated anonymous identity, the adversary has to acquire smart lamp's (SL_j's) secret (s_j) and private key (S_j). The adversary has to solve CMDLP if the adversary wants to compute the smart lamp's (SL_j's) secret (s_j) and private key (S_j) from public parameter (W_j).

4.7. Without Assistance of Registration Center

The registration center (RC) is a third party for both sides of communication after the registration phase. A privilege or malicious insider attack may occur if the adversary is in the RC, and some risks may be led to, such as message leakage, verifications stolen, etc. If a privilege or malicious insider attack occurs in a telemedicine system, the patient's privacy and security may be damaged. Although works related to the security of the 5G networks have been proposed recently [3,4], the RC is included in the system structure of these works, which is no different from conventional networks. In the proposed scheme, the hierarchical system structure was introduced, which is suitable for 5G networks without a RC or a trusted third party.

4.8. Resistant to Bergamo et al.'s Attack

Bergamo et al. proposed an attack on Chebyshev chaotic maps-based cryptosystems based on two reasons as below [39]. First, an adversary is able to obtain related elements (x, a_{ij}, μ_{ij}, ω_j). Second, several Chebyshev polynomials go through the same point due to the periodicity of the cosine function. In the proposed scheme, an adversary is unable to obtain any related elements (x, a_{ij}, μ_{ij}, ω_j) because of being encrypted in transmitted messages where only the ambulance (A_{ij}) and the smart lamp (SL_j) can retrieve the decryption key. Moreover, the proposed scheme utilizes extended Chebyshev polynomials proposed by Zhang [34], in which the periodicity of the cosine function can be avoided. As a result, the proposed scheme can resist attack proposed by Bergamo et al. [39].

5. Computational Complexity Analysis

According to previous research that uses MIRACL Library and Ubuntu 16.0 operating system with 4 GB RAM and 2.7 GHz processor and get execution time [3,4,13], the time of performing a one-way hash function operation (T_h) is about 0.006 milliseconds (ms), and time for performing a Chebyshev chaotic maps operation (T_{ch}) is approximately equal with 42.04 times of performing a one-way hash function operation that is about 0.252 ms and using Chebyshev chaotic maps can be more efficient than using elliptic-curve cryptography. The time taken for computing XOR operations is ignored because the value is too low to influence the result. The results of computational complexity and performing time of the proposed scheme are presented and shown in Table 3. In the emergency signal

sending phase, the patient will take 0.006 ms, the smart lamp will take 0.012 ms, and the server of the medical institute will take 1.8 ms after receiving a message from the patient. The ambulance does not exist in the emergency signal sending phase. Performing the emergency signal sending phase will take at least 1.818 ms, according to the results above. In the secure ambulance communication phase, the ambulance will take 0.792 ms, and each smart lamp will take 0.774 ms after receiving a message from the ambulance. The patient and server of the medical institute do not exist in the secure ambulance communication phase. Performing the secure ambulance communication phase will take at least 1.566 ms, according to the results above. Although there are no requirements or standards about the recommendation of time to perform a cryptographic module, the proposed scheme has proven that is more efficient than the previous studies. For example, the time to perform the emergency signal sending phase is better than Abdel-Malek et al.'s work [40]; the process of the secure ambulance communication phase is similar to Lin and Hsu's [13] work so that the results can be referred to Lin and Hsu's [13] work.

Table 3. Performance analysis of proposed scheme.

Role \ Phase	Emergency Signal Sending Phase	Secure Ambulance Communication Phase
Patient Pa_i	T_h= 0.006ms	N/A
Smart lamp SL_j	$2T_h$= 0.012ms	$3T_{ch}$+$6T_h$ = (0.756 + 0.036) ms = 0.792 ms
Server of medical institute MS	$7T_{ch}$+$6T_h$ = (0.036 + 1.764) ms = 1.8 ms	N/A
Ambulance A_{ij}	N/A	$3T_{ch}$+$3T_h$ = (0.756 + 0.018) ms = 0.774 ms
Total	$7T_{ch}$+$9T_h$ = (0.054 + 1.764) ms = 1.818 ms	$6T_{ch}$+$9T_h$ = (1.512 + 0.054) ms = 1.566 ms

6. Conclusions

5G networks provide high-speed network, big capacity, and scalability, which has an efficient effect on energy consumption and provides quality of experience and amount of devices communication, and 5G can provide connection massive IoT. IoT with 5G environments provides solutions of the network layer, including enhancing the quality of service, to solve challenges of smart medical healthcare. EMS has become a complex network of all types of professionals, including care in an ambulance. 5G network with EMS can simplify the medical treatment process and improve the efficiency of patient treatment. The importance of healthcare-related privacy preservation is rising. If the work of privacy preservation fails, not only will medical institutes have economic and credibility losses but also property losses and even the lives of patients will be harmed. This paper proposes a privacy-preserved ID-based secure communication scheme in 5G-IoT telemedicine systems that can achieve the features below. The proposed scheme allows the emergency signal to be transmitted immediately with decreasing risk of secret key leakage. Information about the patient and their prehospital treatments can be transmitted securely while transferring the patient to the destination medical institute, and the quality of healthcare services can be assured while preserving the privacy of the patient through the proposed scheme. The proposed scheme supports not only normal situations but also emergencies. The proposed scheme applies key insulation to prevent key exposure problems on wearable devices and provides federated identity management, which can manage the identity of ambulances in a hierarchical structure efficiently. Finally, the proposed scheme can resist potential attacks and has been proven secure enough using the random oracle model [36] and BAN logic [37].

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Ahad, A.; Tahir, M.; Yau, K.L.A. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. *IEEE Access* **2019**, *7*, 100747–100762. [CrossRef]
2. Chettri, L.; Bera, R. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet Things J.* **2020**, *7*, 16–32. [CrossRef]
3. Ying, B.; Nayak, A. Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography. *J. Netw. Comput. Appl.* **2019**, *131*, 66–74. [CrossRef]
4. ul Haq, I.; Wang, J.; Zhu, Y. Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks. *J. Netw. Comput. Appl.* **2020**, *161*, 102660. [CrossRef]
5. Anwar, S.; Prasad, R. Framework for Future Telemedicine Planning and Infrastructure using 5G Technology. *Wirel. Pers. Commun.* **2018**, *100*, 193–208. [CrossRef]
6. Agiwal, M.; Roy, A.; Saxena, N. Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1617–1655. [CrossRef]
7. Li, S.; Xu, L.D.; Zhao, S. 5G Internet of Things: A survey. *J. Ind. Inf. Integr.* **2018**, *10*, 1–9. [CrossRef]
8. Lin, T.-W.; Hsu, C.-L. FAIDM for Medical Privacy Protection in 5G Telemedicine Systems. *Appl. Sci.* **2021**, *11*, 1155. [CrossRef]
9. EMS Agenda 2050. *A People-Centered Vision for The Future of Emergency Medical Services*; EMS Agenda 2050 Technical Expert Panel: Washington, DC, USA, 2019.
10. *Emergency Medical Services (EMS) Data Integration to Optimize Patient Care: An Overview of The Search, Alert, File, Reconcile (SAFR) Model of Health Information Exchange*; Office of the National Coordinator for Health Information Technology: Washington, DC, USA, 2017.
11. Mukhopadhyay, A.; Sreekumar, S.; Xavier, B.; Suraj, M. A Cloud-Based Smartphone Solution for Transmitting Bio-Signals from an Emergency Response Vehicle. *Int. J. E-Health Med. Commun.* **2019**, *10*, 22–38. [CrossRef]
12. Garai, Á.; Péntek, I.; Attila, A. Revolutionizing healthcare with IoT and cognitive, cloud-based telemedicine. *Acta Polytech. Hung.* **2019**, *16*, 163–181. [CrossRef]
13. Lin, T.-W.; Hsu, C.-L.; Le, T.-V.; Lu, C.-F.; Huang, B.-Y. A Smartcard-Based User-Controlled Single Sign-On for Privacy Preservation in 5G-IoT Telemedicine Systems. *Sensors* **2021**, *21*, 2880. [CrossRef] [PubMed]
14. Pramanik, P.K.D.; Pareek, G.; Nayyar, A. Chapter 14—Security and Privacy in Remote Healthcare: Issues, Solutions, and Standards. In *Telemedicine Technologies*; Jude, D.H., Balas, V.E., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 201–225. [CrossRef]
15. Zriqat, I.A.; Altamimi, A. Security and Privacy Issues in eHealthcare Systems: Towards Trusted Services. *Int. J. Comput. Sci. Appl.* **2016**, *7*. [CrossRef]
16. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 47–53.
17. Gentry, C.; Silverberg, A. Hierarchical ID-Based Cryptography. In *Advances in Cryptology—ASIACRYPT 2002*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 548–566.
18. Yan, L.; Rong, C.; Zhao, G. Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. In *Cloud Computing*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 167–177.
19. Park, Y.; Sur, C.; Rhee, K.-H. A Privacy-Preserving Location Assurance Protocol for Location-Aware Services in VANETs. *Wirel. Pers. Commun.* **2011**, *61*, 779–791. [CrossRef]
20. Shen, V.R.L.; Huang, W.-C. A Time-Bound and Hierarchical Key Management Scheme for Secure Multicast Systems. *Wirel. Pers. Commun.* **2015**, *85*, 1741–1764. [CrossRef]
21. Fremantle, P.; Aziz, B. Cloud-based federated identity for the Internet of Things. *Ann. Telecommun.* **2018**, *73*, 415–427. [CrossRef]
22. Santos, M.L.B.A.; Carneiro, J.C.; Franco, A.M.R.; Teixeira, F.A.; Henriques, M.A.A.; Oliveira, L.B. FLAT: Federated lightweight authentication for the Internet of Things. *Ad Hoc Netw.* **2020**, *107*, 102253. [CrossRef]
23. Dodis, Y.; Katz, J.; Xu, S.; Yung, M. Key-Insulated Public Key Cryptosystems. In *Advances in Cryptology—EUROCRYPT 2002*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 65–82.
24. Cui, J.; Lu, J.; Zhong, H.; Zhang, Q.; Gu, C.; Liu, L. Parallel Key-Insulated Multiuser Searchable Encryption for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4875–4883. [CrossRef]
25. Dodis, Y.; Katz, J.; Xu, S.; Yung, M. Strong Key-Insulated Signature Schemes. In *Public Key Cryptography—PKC 2003*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 130–144.
26. Libert, B.; Quisquater, J.-J.; Yung, M. Parallel Key-Insulated Public Key Encryption without Random Oracles. In *Public Key Cryptography—PKC 2007*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 298–314.
27. Kocarev, L. Chaos-based cryptography: A brief overview. *IEEE Circuits Syst. Mag.* **2001**, *1*, 6–21. [CrossRef]
28. Yoon, E.-J.; Jeon, I.-S. An efficient and secure Diffie–Hellman key agreement protocol based on Chebyshev chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **2011**, *16*, 2383–2389. [CrossRef]
29. Yoon, E.-J.; Yoo, K.-Y. Cryptanalysis of Group Key Agreement Protocol Based on Chaotic Hash Function. *IEICE Trans. Inf. Syst.* **2011**, *E94.D*, 2167–2170. [CrossRef]
30. Solev, D.; Janjic, P.; Kocarev, L. Introduction to Chaos. In *Chaos-Based Cryptography: Theory, Algorithms and Applications*; Kocarev, L., Lian, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 1–25. [CrossRef]

31. Lin, H.-Y. Improved chaotic maps-based password-authenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 482–488. [CrossRef]
32. Lee, T.-F.; Hsiao, C.-H.; Hwang, S.-H.; Lin, T.-H. Enhanced smartcard-based password-authenticated key agreement using extended chaotic maps. *PLoS ONE* **2017**, *12*, e0181744. [CrossRef]
33. Lin, T.-W.; Hsu, C.-L. Anonymous group key agreement protocol for multi-server and mobile environments based on Chebyshev chaotic maps. *J. Supercomput.* **2018**, *74*, 4521–4541. [CrossRef]
34. Zhang, L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos Solitons Fractals* **2008**, *37*, 669–674. [CrossRef]
35. Wu, W.; Mu, Y.; Susilo, W.; Seberry, J.; Huang, X. Identity-Based Proxy Signature from Pairings. In *Autonomic and Trusted Computing*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 22–31.
36. Bellare, M.; Rogaway, P. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax Virginia, VA, USA, 3–5 November 1993; pp. 62–73.
37. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
38. Liu, W. *Contributions to Cryptography with Restricted Conditions*; University of Wollongong: Wollongong, Australia, 2016.
39. Bergamo, P.; Arco, P.D.; Santis, A.D.; Kocarev, L. Security of public-key cryptosystems based on Chebyshev polynomials. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2005**, *52*, 1382–1393. [CrossRef]
40. Abdel-Malek, M.A.; Akkaya, K.; Bhuyan, A.; Ibrahim, A.S. A Proxy Signature-Based Swarm Drone Authentication with Leader Selection in 5G Networks. *IEEE Access* **2022**, *10*, 57485–57498. [CrossRef]