cryptography

MDPI

Article

ES-HAS: ECC-Based Secure Handover Authentication Scheme for Roaming Mobile User in Global Mobility Networks

Suvidha K. S. [1], Jothi Rangasamy [1], Shyam S. Kamath [1] and Cheng-Chi Lee [2,3,*]

[1] Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Surathkal Srinivasnagar PO, Mangalore 575025, India; suviks22@gmail.com (S.K.S.); jothiram@nitk.edu.in (J.R.); shyam@nitk.edu.in (S.S.K.)

[2] Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, No. 510, Zhongzheng Rd., Xinzhuang Dist., New Taipei City 24205, Taiwan

[3] Department of Computer Science and Information Engineering, Asia University, Wufeng Shiang, Taichung 41349, Taiwan

* Correspondence: cclee@mail.fju.edu.tw; Tel.: +886-2-2905-3372; Fax: +886-2-2901-7405

Abstract: The design and implementation of two-factor schemes designed for roaming mobile users for global mobility networks in smart cities requires attention to protect the scheme from various security attacks, such as the replay attack, impersonation attack, man-in-the-middle attack, password-guessing attack and stolen-smart-card attack. In addition to these attacks, the scheme should achieve user anonymity, unlinkability and perfect forward secrecy. In the roaming scenario, as mobile users are connected to the foreign network, mobile users must provide authentication details to the foreign network to which they are connected. The foreign network forwards the authentication messages received from the mobile users to their home network. The home network validates the authenticity of the mobile user. In the roaming scenario, all communication between the three entities is carried over an insecure channel. It is assumed that the adversary has the capabilities to intercept the messages transmitted over an insecure channel. Hence, the authentication scheme designed must be able to resist the above-mentioned security attacks and achieve the security goals. Our proposed scheme ES-HAS (elliptic curve-based secure handover authentication scheme) is a two-factor authentication scheme in which the mobile user possesses the password, and the smart card resists the above-mentioned security attacks. It also achieves the above-mentioned security goals. We also extended our two-factor authentication to a multi-factor authentication scheme using the fingerprint biometric technique. The formal security analysis using BAN logic and the formal security verification of the proposed scheme using the widely accepted AVISPA (automated validation of internet security protocols and applications) tool is presented in this article. In comparison with the related schemes, the proposed scheme is more efficient and robust. This makes the proposed scheme suitable for practical implementation.

Keywords: GLOMONET; AVISPA; BAN logic; security; elliptic curve cryptography; multi-factor authentication scheme; roaming; biometric

Citation: K. S., S.; Rangasamy, J.; Kamath, S.S.; Lee, C.-C. ES-HAS: ECC-Based Secure Handover Authentication Scheme for Roaming Mobile User in Global Mobility Networks. *Cryptography* **2021**, *5*, 35. https://doi.org/10.3390/cryptography5040035

Academic Editors: Seyit A. Camtepe and Josef Pieprzyk

Received: 4 October 2021
Accepted: 10 December 2021
Published: 13 December 2021

1. Introduction

With the widespread usage of the internet, there has been an increased demand for internet services. Users are able to access internet services through mobile devices over wireless networks. Hence, securing the network in order to achieve network security goals, such as confidentiality, integrity and availability, becomes imperative. The global mobility network (GLOMONET) facilitates a roaming service for the mobile user (MU) to access various kind of services provided by the home network (HN) while roaming in a foreign network (FN). Authenticating MU in the roaming network is an important security issue. In order to address this issue, researchers have proposed many two-factor and

multi-factor authentication schemes in GLOMONET. In two-factor authentication schemes, MU possesses the password and the smart card. In multi-factor authentication schemes, along with the password and the smart card, biometric techniques, such as fingerprint scan, iris scan, etc. are used. When MU roams into any FN, he/she should get authenticated to access the HN services in the FN. Hence, mutual authentication between the MU and the FN becomes important. The mutual authentication process must be supported by the HN. Before any communication takes place in GLOMONET, there are three phases involved in the communication between the three entities. The first is the registration phase, which is carried over a secure channel; the second is the login and the authentication phase; and the third is the password change phase. In the registration phase, MU registers to HN to get access to the HN services, whereas the login and authentication phase is carried over an insecure channel and hence messages transmitted during these phases are vulnerable to security attacks. Hence, securing the messages over an insecure channel becomes important. In order to secure the messages, symmetric key cryptosystem algorithms are used. Another important security property that should be addressed in GLOMONET is the user anonymity. During the message transmission over an open channel, an adversary listening to the open channel can intercept the messages and impersonate the legal MU. So, the protection of the user's information is also an important task for the researchers.

1.1. Multi-Factor Authentication Schemes in GLOMONET

Many biometric-based user authentication protocols [1–5] have been presented to improve the security flaws associated with the mobile device authentication. Biometric-based schemes are difficult to guess or duplicate or forge, and cannot be stolen or lost.

1.2. Security and Function Requirements

Based on the literature review on the authentication schemes for the roaming MU in GLOMONET, the observation is made that the designed authentication scheme has to satisfy the set of security requirements and functions listed below:

1. **Quick wrong password detection**: MUs use different network-based applications which provide the credentials for users to access their services. To prove the authenticity of the MU using the services, the MU has to input the pair of identity and password. In the event of wrong input of the password, there must be a mechanism to prompt the user about the wrong input login credentials. The mechanism developed must verify the credentials and reject the request of the MUs with invalid credentials, which saves further computational and communication costs.
2. **Mutual authentication**: In the roaming scenario, the MU is away from the HN. Therefore, the MU cannot access the services from the HN. Therefore, the foreign network serves the roaming MU present in the cell area of the FN. To access the services from the FN, the MU has to authenticate HN and FN. The FN forwards the authentication messages sent by the MU to the HN. The HN verifies the authenticity of the MU. After receiving successful verification of the MU credentials, the FN grants access to the services to the MU. In such a roaming environment, where the FN is semi-trusted, the roaming MU is not trusted and the HN is assumed to be fully trusted and thus mutual authentication between all the participating entities in the communication becomes imperative to resist security attacks, such as the man-in-the-middle attack, replay attack, and impersonation attack.
3. **Fairness of session key**: The session key is derived between the FN and the roaming MU to establish secure communication over the insecure channel. The session key establishment requires a contribution from both communicating entities, such as the FN and MU. The derived session should not be known to the third party. Even the HN should not have knowledge of the session key agreed between the FN and MU.
4. **Session key update**: To avoid security attacks, such as the replay attack, etc., the session is updated for every new session that is initiated between the MU and FN. To

achieve the freshness of the random numbers for every session, fresh random values are chosen.

5. **User anonymity**: User anonymity is an important security feature that the developed authentication scheme must protect. The identity of the MU should not be disclosed.
6. **Unlinkability**: An attacker should not be able to trace the location of the MU by linking the two different sessions of the same MU.
7. **Resistance of well known security attacks**: The designed authentication scheme should resist the security attacks, such as the replay attack, impersonation attack, stolen-smart-card attack, password-guessing attack, and the man-in-the-middle attack.

1.3. Motivation

The literature survey on the existing authentication schemes for roaming MUs in GLOMONET reveals that the authentication schemes found in the literature survey [6–10] are vulnerable to several security attacks and could not meet the security requirements mentioned in Section 1.2.

1. The authentication schemes for the roaming MUs [6–10] are vulnerable to the well-known security attacks, such as the insider attack, replay attack, impersonation attack, and password-guessing attack, in GLOMONETS.
2. The session key update phase is a critical security requirement and hence must be implemented carefully while designing the authentication scheme for roaming MUs. The session key update phase maintains the freshness of the random numbers for every new session established between the MU and FN. The literature survey reveals that the authentication schemes designed for roaming MUs in GLOMONET [5,10–12] Could not provide the session key update phase in their proposed schemes.
3. The authentication schemes developed for roaming MUs in GLOMONET should satisfy all the security requirements presented in Section 1.2.
4. The design and development of lightweight secure authentication schemes are essential for resource-constrained mobile devices relative to computing power, memory and battery capacity.

1.4. Contributions of Our Research Work

1. We design an efficient and more secure ECC-enabled authentication scheme for roaming MUs in GLOMONET that can potentially resist various known attacks. In the proposed scheme, a roaming MU and a serving network or FN mutually authenticate among each other during the authentication phase, and they also establish a common session key among them for secure communication.
2. The BAN logic-based formal security analysis [13] proves the strength of our proposed scheme. Using such a security analysis, it is shown that the proposed scheme provides the session key security. Furthermore, to ensure other existing known attacks, the informal (non-mathematical) security analysis is also presented.
3. The proposed scheme is simulated with the help of the broadly accepted automated validation of internet security protocols and applications (AVISPA) tool [14]. AVISPA tools perform formal security verification of the proposed scheme. The simulation results prove that the proposed scheme is secure against passive/active attacks, such as replay attacks and man-in-the-middle attacks.
4. In addition, the proposed scheme is shown to be comparable with other existing schemes in terms of the communication and the computation costs, and it also provides better security and functionality features in comparison to those of other existing schemes. The comparative study shows that the proposed scheme is efficient and more robust for the authentication of roaming MUs as compared to other authentication schemes in GLOMONET.

1.5. Organization of the Paper

The literature survey on previous authentication schemes is briefed in Section 2. Mathematical preliminaries are explained in Section 3. The system model is presented in Section 4. The proposed scheme is explained in Section 5. Detailed description of the formal security analysis using BAN logic is described in Section 7. Formal security verification of the proposed scheme using the AVISPA tool is illustrated in Section 8. The performance comparison is described in Section 9. Conclusion is given in Section 10.

2. Literature Survey

In 1995, Hwang et al. [15] worked on securing communication over teleconference by sharing a common secret key. In 1999, Hwang [16] further worked on the same topic, securing teleconference, and proposed a new scheme. In 2000, L. Buttyan et al. [17] worked on authentication protocols and came up with a new scheme. The proposed scheme explained the various security attacks to which the authentication schemes designed for GLOMONETs are vulnerable. In 2003, Hwang et al. [18] worked on the authentication schemes of Hwang et al. [15] and L. Buttyan et al. [17]. They proposed a new scheme to provide a secure and efficient authentication scheme.

In 2004, Zhu et al. [19] pointed out that most authentication schemes fail to preserve user anonymity.

Later in 2006, Lee et al. [20] worked on the authentication scheme of Zhu et al. [19]. The study revealed that their scheme is susceptible to forgery attacks and mutual authentication. To overcome the security pitfalls of the scheme of Zhu et al., Lee et al. [20] came up with a new scheme. Later, Wei et al. [21] worked on the scheme of Lee et al. [20]. With a thorough understanding of their scheme, Wei et al. found that their scheme failed to preserve user anonymity and untraceability. Further, Wei et al. also stated that their scheme suffered from password-guessing attacks. To improvise the scheme and to enhance performance, Wei et al. [21] came up with a new scheme.

In 2014, Huang et al. [22] cryptanalyzed the scheme of Juang et al. [23] based on passive attacks and active attacks. The cryptanalysis on the scheme of Juang et al. stated that their scheme has limitations over the smart-card attack, password attack and session key extraction.

In 2015, Ding Wang et al. [24] reviewed the scheme of Tsai et al. [25]. The cryptanalysis was based on the well-known attack in two-factor authentication schemes. For the smart-card-loss attack, with the stolen smart card parameters, the adversary could change the password by initiating the password change phase.

In 2018, Xu et al. [26] reviewed Gope and Hwang's protocol [27] and identified some of the limitations of the scheme, such as the storage consumption problem, computational burden and replay attack. The scheme of Xu et al. contributes to overcoming the identified limitations.

In 2019, Ref. [28] proposed a privacy-preserving authentication scheme for roaming consumers in GLOMONET. Their work revealed the cryptanalysis of schemes such as those of Arshad et al. [29], Li et al. [4], and Chen et al. [30,31] based on session-specific information attacks. The proposed scheme of Arezou et al. provided countermeasures to the identified security weaknesses. Their scheme achieved security, such as impersonation attack resistance, modified attack resistance, strong MU anonymity and unlinkability, insider attack resistance, replay attack resistance, password-guessing attack resistance, known session-specific temporary information attack resistance, desynchronization attack resistance, known key attack resistance, denial-of-service attack resistance, and stolen verifier attack resistance, as well as security goals, such as perfect forward secrecy. In 2020, in Ref. [32], Wei et al. proposed two-factor authentication for roaming users in GLOMONET. Their scheme is based on the digital signature algorithm. They attempted to achieve the user anonymity using digital signature algorithms. The scheme of Ding et al. [33] cryptanalysed the scheme of Li et al. [34] and claimed that the scheme security proof of Li et al. to protect user anonymity has some weaknesses. Another proof validation

was made on the offline password guessing attack and they claimed that the scheme proof of Li et al. has some limitations. The scheme of Ding et al. provided the claim to overcome these identified weaknesses.

In 2013, Shin et al. [35] proposed a secure authentication scheme with user anonymity for roaming users in ubiquitous networks. Later, Farash et al. [36] cryptanalysed the scheme of Shin et al. The cryptanalysis proved that the scheme of Shin et al. is vulnerable to security attacks, such as user traceability, user and server impersonation attacks and session key disclosure. To countermeasure the security attacks identified in the scheme [35], Farash et al. [36] proposed an enhanced secure authentication protocol for ubiquitous networks. The strengths of their proposed scheme are as follows:

- Their scheme provides the mobile node authentication and the FN authentication.
- Their scheme also protects user anonymity and achieves untraceability.
- Their scheme is resistant to the offline password guessing attack.
- No verification table is maintained at the server side for the password. This protects the scheme from such attacks as stolen verifier and modification attacks.

In 2016, Karuppiah et al. [37] reviewed the scheme of Farash et al. [36]. The cryptanalysis on the scheme [36] resulted in the findings of some security weaknesses to the identified attacks: their scheme is vulnerable against replay, forgery, and offline password guessing attacks. In addition, their scheme fails to protect user anonymity, with no local password verification and session key disclosure. Karuppiah et al. [37] proposed a secure lightweight authentication scheme for roaming mobile users. The strengths of their proposed scheme are as follows: user anonymity is protected, user untraceability is achieved, and mutual authentication between the MU, FA and HA are achieved. Their scheme is resistant to such security attacks as the replay attack, offline password guessing attack, forgery attack, stolen verifier and modification attacks, insider attack, man-in-the-middle attack, and known key attack. In addition, forward secrecy and local password verification are achieved.

Gope and Hwang [27] reviewed the scheme of He et al. [38]. The cryptanalysis on the scheme of He et al. revealed their proposed scheme having several security weaknesses, such as vulnerability to forgery attack and unfair key agreement, compromising the untraceability and disclosure of the user identity. Gope and Hwang [27] proposed an efficient mutual authentication and key agreement. Their proposed scheme is resilient to the identified security weaknesses in the scheme of He et al. The security strengths of their proposed scheme are as follows: accomplishment of mutual authentication, fair key agreement, strong user anonymity, resistant to forgery attacks and security assurance in the case of lost smart card.

In 2017, Odelu et al. [39] first reviewed the work proposed by Zhao et al. [40]. The cryptanalysis on the scheme [40] revealed that the scheme is vulnerable to several security attacks, such as known session key attack, and insider attack, with no provision for revocation and reregistration. Odelu et al. [39] proposed a secure anonymity-preserving authentication scheme for roaming mobile users in global mobility networks. The strengths of the proposed scheme are as follows: provides user anonymity; resists impersonation attack, replay attack, man-in-the-middle attack, offline password-guessing attack, and insider attack; provides session key security; provides local password verification; and provides provision for revocation and re-registration.

In 2018, Fan wu et al. [41] proposed a smart healthcare systems under global mobility networks. Their proposed scheme provides security strength against such security attacks as insider attack, offline password guessing attack, forgery attack, de-synchronization attack, replay attack, known key attack, tracking attack and strong forward security.

In 2018, Banerjee et al. [42] proposed an anonymity-preserving group formation-based authentication protocol in global mobility networks. The security strength of the proposed scheme is as follows: protects both user anonymity and untraceability; and the scheme is resilient to security attacks such as impersonation attack, replay attack, man-in-the-middle attack, privileged-insider attack, offline password-guessing attack and stolen-smart-card attack.

In 2018, Madhusudhan and Shashidhara [5] reviewed the scheme of Karuppiah and Saravanan [43]. The cryptanalysis of their scheme [43] demonstrated that it is vulnerable to security attacks such as insider attack, stolen verifier attack, offline password-guessing attack with smart cards, impersonation attack, denial-of-service attack, clock synchronization problem, unfair key agreement and disclosure of user anonymity. Madhusudhan and Shashidhara [5] proposed a secure and lightweight authentication scheme for roaming service in GLOMONETs. The proposed scheme [5] resists the security weaknesses identified in the scheme of [43]. The strengths of the proposed scheme [5] are as follows: user anonymity and untraceability is achieved, mutual authentication is achieved, the proposed scheme is resilient to security attacks such as impersonation attack, replay attack, insider attack, offline dictionary attack, stolen verifier attack and smart-card-loss attack. Their scheme achieves fair key agreement and provides local password verification.

In 2019, Lu et al. [44] reviewed the scheme of Gope and Hwang [45]. The cryptanalysis on the scheme [45] demonstrated that the scheme is vulnerable to security attacks such as known session-specific temporary information attack. To address the identified security weaknesses found in the scheme [45], Lu et al. [44] proposed an elliptic curve cryptography (ECC) based authentication scheme to achieve secure implementation in GLOMONET. The security strengths of the proposed scheme [44] are as follows: mutual authentication is achieved, known session-specific temporary information attack, unlinkability, anonymity and untraceability. The scheme is resilient to security attacks such as forgery attack, insider attack, and stolen-smart-card attack.

In 2019, Aghili et al. [46] proposed authentication and key agreement schemes for IoT environments. The proposed scheme is resilient to security attacks, such as man-in-the-middle attack, impersonation attack, session key security, replay attack, and entity compromised attack, while preserving user anonymity and user untraceability.

In 2020, Wan et al. [47] proposed a roaming authentication protocol based on a heterogeneous fusion mechanism for the IoT environment. Their proposed scheme is resilient to various security attacks, and the experimental results show that their scheme incurs lower packet loss rate and lower energy consumption.

In 2020, Ghahramani et al. [48] reviewed the protocol of Li et al. protocol [4]. The cryptanalysis on the scheme [4] revealed several security weaknesses, such as vulnerability to insider attack, forward and backward security, resistance to offline guess attack, impersonation attack, offline guess attack, and insecure key distributions. Ghahramani et al. [48] proposed a secure biometric authentication scheme for GLOMONETs. The security strength of their proposed scheme is as follows: resilience to offline guess attack, impersonation attack, insider attack, and forward and backward security, and secure key distribution.

Table 1 provides the information about various authentication schemes designed to provide security to the roaming users during handover in GLOMONETs. The strengths and the weaknesses of the authentication schemes are presented in Table 1.

Table 1. Literature survey on two-factor authentication schemes in GLOMONET.

Authors	Year	Strengths	Weaknesses
Jiang et al. [49]	2012	Protects user anonymity, user untraceability and provides two-factor security. Mutual authentication between MU , FN and HN are achieved.	Session key agreement is static and depends on static key agreement.
Kuo et al. [6]	2014	Their scheme protects user anonymity with untraceability. Their scheme is resilient to security attacks such as impersonation attack, replay attack, smart-card-loss attack and man-in-the-middle attack. In addition, their scheme also achieves mutual authentication and secrecy of the session key.	User untraceability is not achieved.

Table 1. *Cont.*

Authors	Year	Strengths	Weaknesses
Guo et al. [7]	2016	Protects user anonymity and untraceability resists impersonation attack, stolen-smart-card attack, server masquerading attack and replay attacks, achieves mutual authentication and perfect forward security.	Their scheme is vulnerable to insider attack and the scheme provides no session key update.
CC Lee et al. [8]	2017	Protects user anonymity, resilient to masquerade attack, man-in-the-middle attack, stolen-smart-card attack, and offline password-guessing attack. In addition, their scheme achieves perfect forward and backward secrecy.	Their scheme cannot resist replay attacks.
Marimuthu et al. [9]	2017	Provides untraceability and secure against security attacks such as known key, insider, offline password-guessing, replay, stolen verifier, forgery and man-in-the-middle attacks. Achieves mutual authentication, user friendliness and local password verification.	Security pitfalls of their scheme are as follows: absence of user anonymity and vulnerable to security attacks, such as offline password guessing and impersonation attacks, has no password change option and no local password verification.
Shashidhara et al. [5]	2018	Protects user anonymity, and their scheme is resilient to forgery and replay attacks.	Scheme does not provide session key update phase.
Xiong Li et al. [4]	2018	Resists security attacks such as session key, replay, forgery, device lost, and denial-of-service attacks and achieves user anonymity, untraceability and mutual authentication.	Their scheme does not provide local password verification, perfect forward secrecy is not achieved, and is vulnerable to denial-of-service attack.
Madhusudhan and Shashidhara [11]	2020	Resists security attacks such as insider, offline password guessing attack, impersonation attack, bit flipping attack, replay, stolen verifier attack. In addition, their scheme achieves user anonymity, local password verification, perfect forward secrecy and mutual authentication.	Their scheme does not protect user untraceability and does not provide session key update.
Bander et al. [10]	2020	Their scheme achieves user anonymity and untraceability, resilient to security attacks, such as stolen verifier attack, insider attack, stolen-smart-card attack, forgery attack, and known session-specific parameter attack. In addition, their scheme achieves user anonymity and protects user untraceability, perfect forward secrecy and mutual authentication.	Their scheme does not protect against password guessing and does not provide session key update.
Kang et al. [12]	2020	Their scheme achieves user anonymity and untraceability, resilient to security attacks such as mobile node impersonation attack, insider attack, foreign bypass attack and session-key-derived attack. In addition, their scheme achieves perfect forward secrecy and mutual authentication.	Their scheme does not provide session key update.

3. Mathematical Preliminaries

In this, we discuss the mathematical background of the cryptographic primitives used in the design of the proposed scheme.

3.1. Basics of Elliptic Curve Cryptography

An elliptic curve defined over finite prime filed F_p is a curve given by the equation of the form

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \quad (1)$$

There is also a condition that Equation (1) must satisfy $4a^3 + 27b^2 \neq 0$, where $a, b \in Z_p$. A non-singular elliptic curve $E_p(a, b)$ is the set of points (x, y) with $(x, y) \in Z_p \times Z_p$ which

satisfy Equation (1). The elements of Z_p are $Z_p = \{0, 1, ..., p-1\}$. Let θ be the point at infinity in $E_p(a, b)$. So, E is the set of points on the elliptic curve $E_p(a, b)$ that satisfy Equation (1) along with the point at infinity. Thus,

$$E = \{(x, y) \mid y^2 \equiv x^3 + ax + b \pmod{p}\} \bigcup \{\theta\}.$$

3.2. Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve $E_p(a, b)$ defined over a finite prime field F_p, consider two points $P, Q \in E_p(a, b)$ where $Q = rP$ where $r \in Z_p^*$ is scalar. Computing k from the point P, Q is computationally infeasible if the prime p is a sufficiently large prime number (for example, 160 bits).

3.3. Scalar Multiplication

In ECC, the scalar multiplication of a point $P \in E_p(a, b)$ is denoted by rP where r is a scalar and rP is achieved using repeated point additions and point doubling operations.

3.4. Elliptic Curve Diffie–Hellman Problem (ECDHP)

Given an elliptic curve $E_p(a, b)$ defined over a finite prime field F_p and points $P, \alpha P$, $\beta P \in E_p(a, b)$, it is difficult to compute $\alpha\beta P$, without the knowledge of either $\{\alpha\}$ or $\{\beta\}$ [50].

3.5. Elliptic Curve Diffie–Hellman (ECDH)

ECDH is a key exchange protocol. This protocol allows the communicating entities across the networks to establish a common shared secret key by agreeing to use the shared public domain parameters of ECC explained in Section 5.1.

Steps for Algorithm to compute the shared secret key:

1. End system A selects the private key $\alpha \in Z_p^*$ where $1 \leq \alpha < n$. A computes the public key as $PB_A = \alpha G$, where G is a generator point in the EC domain parameter. Let the private and public key pair of end system A be $\{\alpha, PB_A\}$, respectively. A computes point P with the co-ordinates $P = (x_P, y_p) = \alpha G$.
2. End system A transmits $P = (x_P, y_p) = \alpha G$ to end system B over an insecure channel.
3. End system B selects the private key $\beta \in Z_p^*$, where $1 \leq \beta < n$. B computes the public key as $PB_B = \beta G$, where G is a generator point in the EC domain parameter. Let the private and public key pair of end system A be $\{\beta, PB_B\}$, respectively. B computes point Q with co-ordinates $Q = (x_Q, y_Q) = PB_B G$.
4. End system B transmits its public key $Q = (x_Q, y_Q) = PB_B G$ to end system A over an insecure channel.
5. The shared secret key is computed as

$$\alpha PB_B = \alpha\beta G = \beta\alpha G = \beta PB_A.$$

3.6. One-Way Hash Function

Hash functions are used to achieve security goals, such as data integrity and message authentication. Hash takes the input of variable length and produces an output of fixed length. $h : \{0,1\}^* \rightarrow \{0,1\}^l$

A one-way hash function satisfies the following properties [13,51].

1. Preimage resistance: For the given input x, it is computationally feasible to compute the hash value of x as $h(x) = y$. However, it is computationally infeasible to compute for the value x with the output value y.
2. Second preimage resistance: It is computationally infeasible to obtain the second input which results in the same hash value output. Ex: If x is one input and y is the other input where $x \neq y$ such that $h(x) = h(y)$.
3. Collision resistance: A collision resistant one-way hash function $h : \{0,1\}^* \rightarrow \{0,1\}^\ell$ takes the variable length input and generates a fixed length output of ℓ bits. The pair

of inputs $(i_1, i_2) \in_R A$ indicates that an attacker randomly chooses the pair of inputs i_1, i_2. It is computationally infeasible for a pair of inputs i_1, i_2 where $i_1 \neq i_2$ to result in the same hash value such that $h(i_1) = h(i_2)$.

3.7. Pseudo-Random Number Generators

A sequence of pseudo-random numbers is generated by a deterministic algorithm and should simulate a sequence of independent and uniformly distributed random variables on the interval $[0, 1]$. In order to be acceptable, a sequence of pseudorandom numbers must pass a variety of statistical tests for randomness.

Definition 1. *A pseudo-random number generator (PRNG) is defined by a tuple (Q, μ, f, U, g), where Q is a finite set of states, μ is the probability distribution on Q for the initial state called seed, $f : Q \to Q$ is the transition function, U is the output space and $g : Q \to U$ is the output function. The generator P generates the numbers in the following way.*

1. *Select the seed $q_0 \in Q$ based on μ. The first number is $u_0 = g(q_0)$.*
2. *At each step $i \geq 1$, the state of the PRNG is $Q_i = f(Q_{i-1})$ and output is $u_i = g(q_i)$. These output $u_i n$ of the PRNG are the pseudo-random numbers, where n is some positive integer considered to be the period of the sequence [52].*

3.7.1. Properties of Pseudo-Random Function

Here, we list a few of the important properties of the pseudo-random function. A PRNG is called good if it satisfies the below stated properties:

1. Uniformity: This property states that the elements in the output space U generated by the pseudo-random function are divided into M equal sub-intervals, and the expected number of samples (e_k) in each sub-interval k, $\{1 \leq k \leq M\}$ is equal; that is, $\forall k, e_k = N \mid M$, where N is the range of the numbers uniformly distributed over the interval $[0, 1]$.
2. Independence: The generated numbers in the outspace U should be independent of each other, and there should not exist any correlation between the numbers generated in succession. This implies that, given any length of output sequence $u_i = g(q_i)$ where $i \geq 1$, one should not be able to predict the next number in the sequence by observing the given numbers.
3. Large period: The PRNG is considered to be good if its period is large.
4. Reproducibility: This property ensures that for the same seed s_0, the same sequence of numbers is generated.
5. Cryptographically Secure: The generated output sequence by the PRNGs should be cryptographically secure to be used in cryptographic applications.

3.8. Fuzzy Extractors

Biometrics information, such as fingerprint and iris scans, are noisy data that cannot be reproduced precisely and cannot be used directly in traditional cryptographic algorithms. Fuzzy extractor [53] is an ideal technique to handle noisy data. Noisy data are received from biometric information such as fingerprinting and iris scanning. A fuzzy extractor is composed of two procedures (Gen, Rep).

1. Gen $(B_i) = (R_i, P_i)$. Gen is a probabilistic algorithm. On the biometric input B_i, it extracts string R_i and an auxiliary string P_i.
2. Rep $(B_i^{'}, P_i) = R_i$. Rep is a deterministic algorithm. Rep produces the string R_i on the biometric input from any vector $B_i^{'}$ close to B_i along with the auxiliary string P_i.

4. System Model

The proposed system model consists of three communicating entities: home network (HN), foreign network (FN) and mobile user (MU). The system model consists of four major steps:

1. **Registration phase**: The mobile user registers to the home network by providing credentials, identity and password. The registration phase is carried out over a secure channel. In the registration phase, the HN, after receiving the mobile user request, computes for the secret parameters. HN agrees to the domain parameters of ECC with the mobile user. These are the public key of HN, symmetric encryption key, one-way hash function. P is the generator point on ECC, a, b, n and p, where p is a large prime number and n is the order of the elliptic curve (EC).
2. **Login or authentication phase**: In the roaming scenario, the mobile user moves from their home network to the foreign network. To access services from the foreign network, the mobile user provides their identity to the foreign network. The login messages are transmitted using a wireless network through radio waves. An adversary listening to the communication channel has full control over the channel, that is, he/she can intercept, modify or alter the messages.
3. The foreign network forwards the request received from the MU to the home network for the verification of the MU's authenticity. The communication between the foreign network and the home network is considered secure.
4. The home network verifies the authentication request of the mobile user received via the foreign network.
5. If the MU is authentication is verified and the MU is authenticated, FN accepts the MU's request and allows the roaming user to access the FN services. Otherwise, the FN rejects the login/authentication request sent by the MU.

Figure 1 presents the proposed system model for a roaming MU.

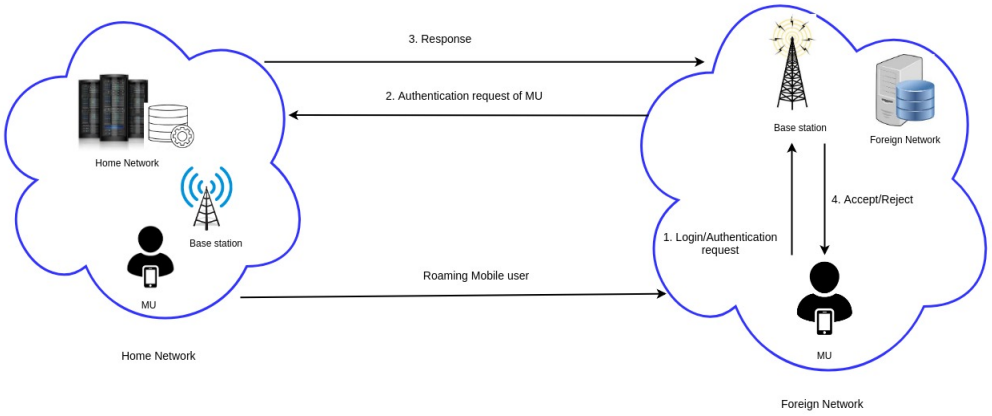

Figure 1. System model for roaming mobile user.

4.1. Trust Model

In the scenario of roaming mobile users in GLOMONET, the communicating entities are the mobile users (MU), foreign network (FN) and home network (HN). MUs are not trusted entities; the FNs are semi-trusted; and the HN is fully trusted.

4.2. Adversary Model

In this section, we illustrate the attacker model during a roaming scenario in the GLOMONET under the two-factor authentication schemes for informal analysis.

1. The "Dolev–Yao threat model (DY model)" [54] is considered in our proposed scheme.
2. The DY model provides an insecure channel for the communication between the entities MU, FN and HN. The FN is considered to be semi-trusted, whereas the HN is a fully trusted service provider. An attacker listening to an insecure channel has the capability to intercept the messages. The eavesdropped messages can be altered, modified or deleted.
3. According to [24], there exist two dictionary spaces for mobile user's identity and password, respectively: $|DID| \leq |DPW| \leq 10^6$. Since the dictionary space is finite,

an adversary can guess a pair of $\{ID^*_{MU}, PW^*_{MU}\}$ in polynomial time. However, it is hard for an attacker to summarize the hash results and the random numbers.

4. According to [55], the adversary has full control over the public channel or insecure channel; an adversary can eavesdrop the messages transmitted over an insecure channel and then modify, alter or delete the messages to breach the security services. However, the adversary does not have any control over the secure channel.
5. According to [56], the adversary can extract the stored information in the smart card through power consumption.
6. An adversary can store all previous session keys. However, if the freshness of the random numbers is changed for every session, then it is difficult for an adversary to arrive at the session keys, even with the knowledge of previous session keys. This property is known as strong forward secrecy.

5. Proposed Scheme

The proposed scheme is divided into four phases: the initialization phase, registration phase that is carried over a secure channel, login and authentication phase, session key update phase that is carried over an insecure channel, and password change phase, which provides local password verification for the MU and is carried over secure channel. The elliptic curve Diffie–Hellman protocol is used to compute the shared secret key between FN and HN to achieve mutual authentication in the proposed scheme. The design goals of our proposed protocol are as follows:

- To establish mutual authentication among the communicating entities under the premise of anonymity;
- To derive and agree on the session key between the communicating entities fairly;
- To resist security attacks, such as stolen-smart-card attack, replay attack attack, offline password-guessing attack and impersonation attack;
- To reduce computational cost and communication cost.

The proposed scheme is simulated using the AVISPA tool. Each phase is explained in detail below. Notations and their representation used in this article are defined in Table 2.

Table 2. Notations and their representation.

Notation	Representation
MU	Mobile User
FN	Foreign Network
HN	Home Network
ID_i	MU's identity
PW_i	MU's password
ID_{HN}	HN's identity
ID_{FN}	FN's identity
SK_{FN}	Secret key of FN
PK_{HN}	Public key of HN
mk	Server master key is a symmetric key of 128 bit
SK	Session key exchanged with FN and MU
X	Secret key of HN
P	Generator point
p	Large prime number
n	Elliptic curve order
h	Cryptographic hash function, $h : \{0,1\}^* \rightarrow \{0,1\}^l$, where l = 160 bits
$E_{mk}(.)$	symmetric encryption algorithm
Z^*_n	$Z^*_n = \{a \mid gcd(a,n) = 1\}$ where a $\in Z_n$

5.1. Initialization Phase

The domain parameters $\{E_{(F_p)}, G, a, b, n, p\}$ of the elliptic curve cryptography are shared among the three communicating entities.

HN performs the following steps to initialize the system parameters:

S1: The HN considers a non-singular elliptic curve $E_p(a, b)$ of the form $y^2 = x^3 + ax + b(modp)$ over a prime (finite) field $Z_p = \{0, 1, ..., p-1\}$. P is chosen as a generator point on the elliptic curve (EC).

S2: The HN chooses random number $x \in Z_p^*$ as its private key and computes the HN's public key as $PK_{HN} = xP$.

S3: The symmetric encryption key mk of 128 bits is shared with the MU by storing it in the smart card.

S4: HN computes the secret key for the foreign network as $SK_{FN} = h(ID_{FN}||PK_{HN}||mk)$

S5: HN selects the one-way hash function of the form $h : \{0,1\}^* \rightarrow \{0,1\}^\ell$. The input can be a variable bit length string but the output should be of a fixed length.

5.2. Registration Phase

The registration phase of the proposed scheme is presented in Figure 2.

Step 1: MU $\rightarrow$ HN: $\{h(ID_i), PID\}$

In the registration phase, the MU is free to choose his/her identity ID_i and password PW_i. After choosing ID_i, PW_i and random number r_m, the MU computes the following

$$PID = h(h(ID_i||PW_i) \oplus h(r_m))$$

The MU submits $\{h(ID_i), PID\}$ to the HN through a secure channel.

Step 2: HN $\rightarrow$ MU:$\{E_p, P, n, a, b, PK_{HN}, S, E_{mk}(.), h(.)\}$.

The HN receives the request from the MU and the HN chooses its random number r_h. HN's server public key PK_{HN} is computed as

$$\begin{aligned} PK_{HN} &= xP \\ SK_{FA} &= h(ID_{FA}||PK_{HN}||mk) \\ S &= PID \oplus h(mk). \end{aligned}$$

where x is a random number $\in Z_n$, and P is a generator point on the elliptic curve. For every foreign network FN, the HN computes secret key SK, where mk is the server shared symmetric key with 128 bits. The HN stores $\{h(ID_i), S\}$ in its database for future communication. The HN sends the smart card with the parameters $\{E_p, P, n, a, b, PK_{HN}, S, E_{mk}(.), h(.)\}$ to the MU through a secure channel.

Step 3: MU : $\{E_p, P, n, a, b, PK_{HN}, S, E_{mk}(.), h(.)\}$

With the received message, the MU computes the following

$$RPW = S \oplus h(h(ID_i||PW_i) \oplus h(r_m)).$$

The computed value of RPW is stored in the smart card. The smart contains the parameters $\{E_p, P, n, a, b, PK_{HN}, RPW, S, r_m, E_{mk}(.), h(.)\}$.

5.3. Login Phase

The login and authentication phase is presented in Figure 3. The detailed description of the steps are stated below.

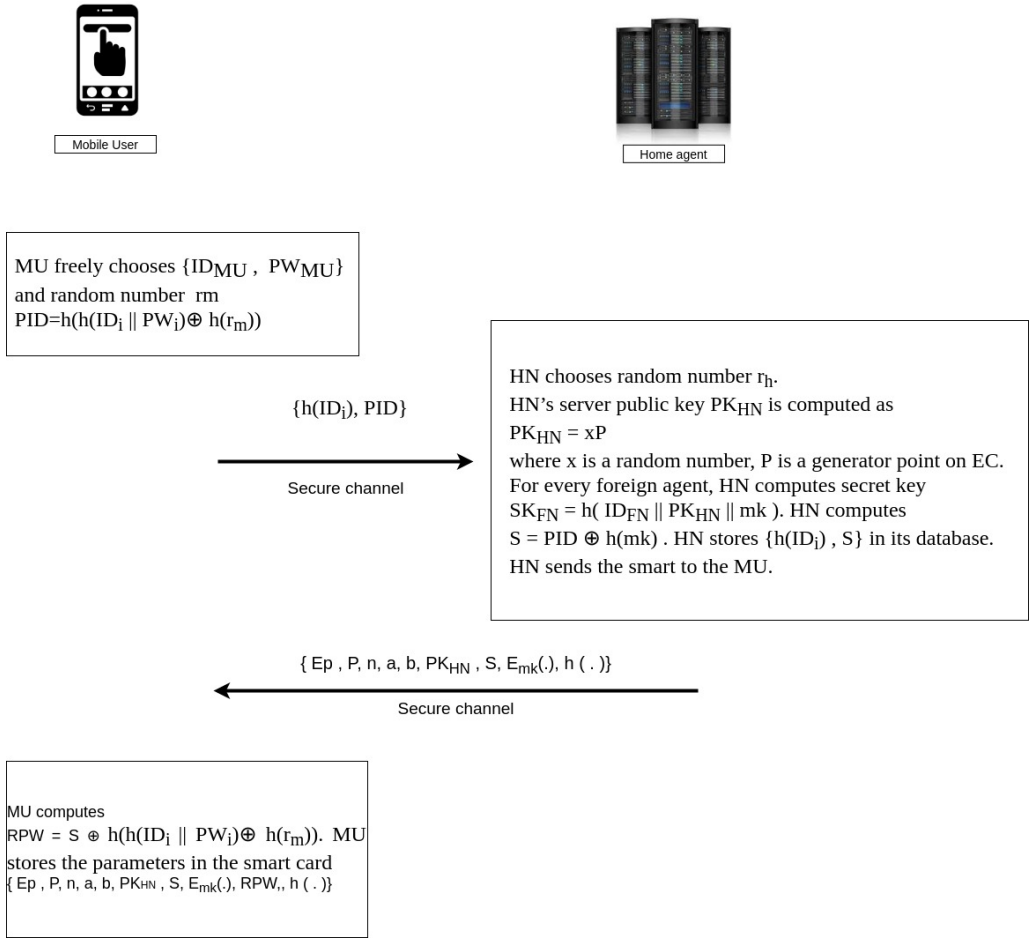

Figure 2. Registration phase.

Step 1: MU $\rightarrow$ FN: $M_1 = \{R_1, AID_{new}, Q_m\}$ Smart card is inserted into the smart card terminal by the MU. The smart card terminal asks for the input of ID_i and password PW_i of the MU. After entering the input, smart card chooses two random numbers r_{new} and $\alpha \in Z_n^*$. The smart card verifies if

$$h(h(ID_i||PW_i) \oplus h(r_m)) \stackrel{?}{=} RPW \oplus S.$$ If it holds true, the smart card computes

$$R_1 = \alpha P$$
$$AID_{new} = E_{mk}(h(ID_i)||r_{new})$$
$$Q_m = r_{new} \oplus h(S||r_{new}||R_1)$$

The MU sends the message $M_1 = \{R_1, AID_{new}, Q_m\}$ to FN over insecure channel.

Step 2: FN $\rightarrow$ HN: $M_2 = \{Q_f, R_2, R_1, V_f, ID_{FN}\}$
After receiving the message $M_1 = \{R_1, AID_{new}, Q_m\}$ from MU. FN generates random number $\beta \in Z_n^*$ and computes the following

$$R_2 = \beta P$$
$$Q_f = Q_m \oplus h(SK_{FN})$$
$$V_f = h(Q_f||Q_m||SK_{FN}||R_1||R_2)$$

where SK_{FN} is a secret key of FN, computed by HN. ID_{FN} is the identity of the FN. FN sends $M_2 = \{Q_f, R_2, R_1, V_f, ID_{FN}\}$ to HN.

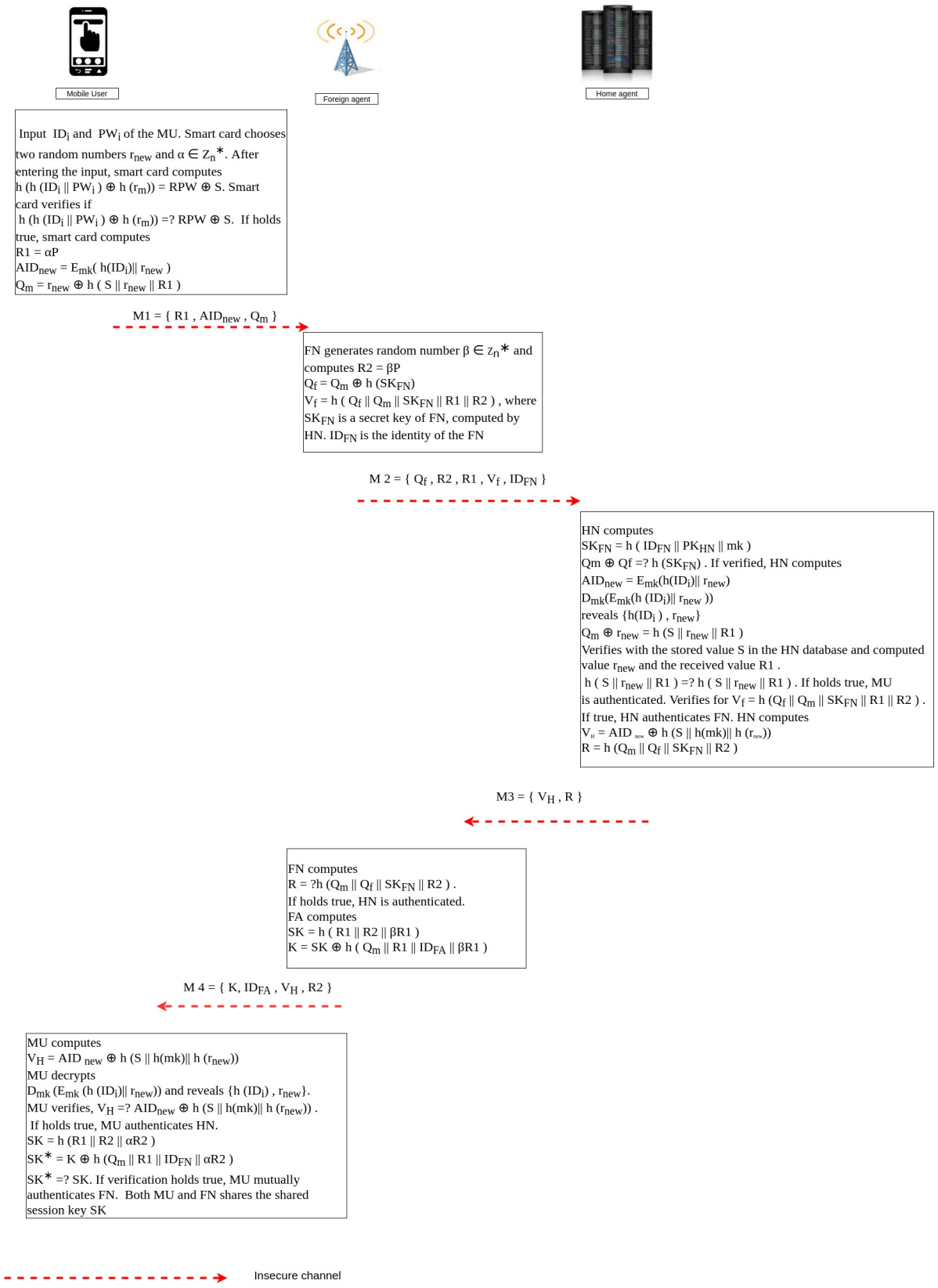

Figure 3. Mutual authentication and key agreement phase.

5.4. Authentication Phase

Step 1: HN $\rightarrow$ FN: $M_3 = \{V_H, R\}$

The HN computes the following:

$$SK_{FN} = h(ID_{FN}||PK_{HN}||mk)$$
$$Q_m \oplus Q_f \stackrel{?}{=} h(SK_{FN})$$

If verified, the HN computes the following,

$$AID_{new} = E_{mk}(h(ID_i)||r_{new})$$
$$D_{mk}(E_{mk}(h(ID_i)||r_{new}))$$
$$\text{reveals } h(ID_i), r_{new}$$
$$Q_m \oplus r_{new} = h(S||r_{new}||R_1)$$

verified with the stored value S in the HN database and computed value r_{new} and the received value R_1.

$h(S||r_{new}||R_1) \stackrel{?}{=} h(S||r_{new}||R_1)$. If it holds true, the MU is authenticated.
$V_f \stackrel{?}{=} h(Q_f||Q_m||SK_{FN}||R_1||R_2)$. If true, the HN authenticates the FN.

After the authentication verification is completed between the MU and FN, the HN computes the following:

$$V_H = AID_{new} \oplus h(S||h(mk)||h(r_{new}))$$
$$R = h(Q_m||Q_f||SK_{FN}||R_2).$$

After all the computations, the HN sends the message $M_3 = \{V_H, R\}$ to the FN over a secure channel.

Step 2: Foreign Network $\rightarrow$ Mobile User: $M_4 = \{K, ID_{FN}, V_H, R_2\}$

After receiving the message M_3 from the HN, the FN computes the following:

$$R \stackrel{?}{=} h(Q_m||Q_f||SK_{FN}||R_2).$$

If it holds true, the HN is authenticated. The FN computes the following:

$$SK = h(R_1||R_2||\beta R_1)$$
$$K = SK \oplus h(Q_m||R_1||ID_{FN}||\beta R_1)$$

The FN sends a message $M_4 = \{K, ID_{FN}, V_H, R_2\}$ to the MU over an insecure channel.

Step 3: MU: $M_4 = \{K, ID_{FN}, V_H, R_2\}$

After receiving the message M_4 from the foreign network, the mobile user computes the following:

$$h(S||h(mk)||h(r_new)) = AID_{new} \oplus V_H$$
$$\text{The MU decrypts } D_{mk}(E_{mk}(h(ID_i)||r_{new})) \text{ and reveals } \{h(ID_i), r_{new}\}.$$
$$V_H \stackrel{?}{=} AID_{new} \oplus h(S||h(mk)||h(r_{new})).$$
$$\text{If verification holds true, the MU authenticates the HN.}$$
$$SK = h(R_1||R_2||\alpha R_2)$$
$$SK^* = K \oplus h(Q_m||R_1||ID_{FN}||\alpha R_2)$$
$$SK^* \stackrel{?}{=} SK$$

If verification holds true, the MU mutually authenticates the FN. Both the MU and FN share the shared session key SK.

5.5. Session Key Update Phase

The detailed description of the session key update phase steps is stated below.

Step 1: MU $\rightarrow$ FN: $M_5 = \{R_1^* = \alpha^* P\}$

The roaming mobile user periodically updates the session key to achieve freshness in the random numbers. The session key update phase is presented in Figure 4. The MU chooses a new random number $\alpha^* \in Z_n^*$ and computes.

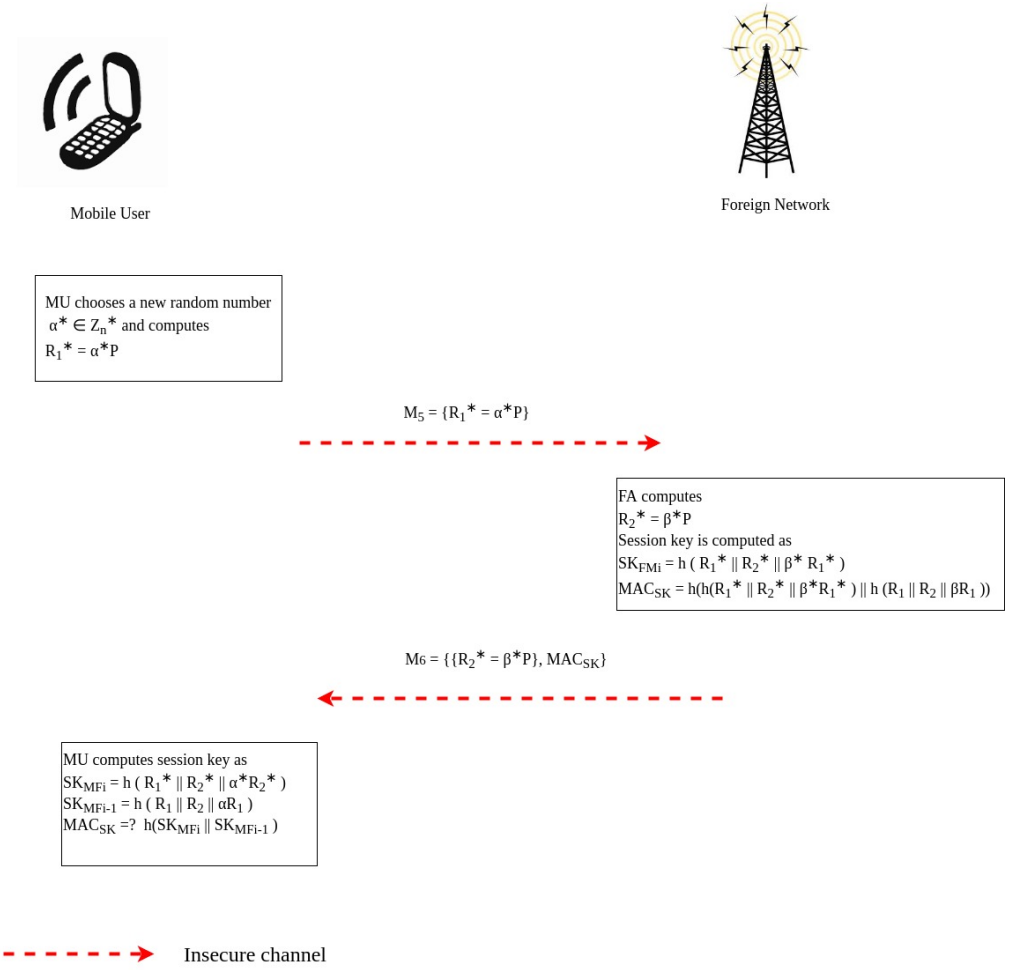

Figure 4. Session key update phase.

$$R_1^* = \alpha^* P$$

The MU sends message $M_5 = \{R_1^* = \alpha^* P\}$ to the FN over an insecure channel.

Step 2: FN $\rightarrow$ MU: $M_6 = \{R_2^* = \{\beta^* P\}, MAC_{SK}\}$

After receiving message M_5 from the MU, the FN chooses a new random number $\beta^* \in Z_n^*$. The FN computes the following:

$$R_2^* = \beta^* P$$
$$SK_{FM_i} = h(R_1^* || R_2^* || \beta^* R_1^*)$$
$$MAC_{SK} = h(h(R_1^* || R_2^* || \beta^* R_1^*) || h(R_1 || R_2 || \beta R_1))$$

The FN sends message $M_6 = \{R_2^* = \{\beta^* P\}, MAC_{SK}\}$ to the MU.

Step 3: Mobile User: $M_6 = \{R_2^* = \{\beta^* P\}, MAC_{SK}\}$

After receiving $M_6 = \{R_2^* = \{\beta^* P\}, MAC_{SK}\}$ from the FN, the MU computes the following:

$$SK_{MF_i} = h(R_1^* || R_2^* || \alpha^* R_1^*)$$
$$SK_{MF_{i-1}} = h(R_1 || R_2 || \alpha R_2)$$
$$h(SK_{MF_i} || SK_{MF_{i-1}}) \stackrel{?}{=} MAC_{SK}.$$

If the verification holds true, message integrity is achieved and message authentication is verified. Therefore, the MU updates the session key as

$$SK^* = h(R_1^*||R_2^*||\alpha^* R_2^*)$$

5.6. Password Change Phase

In the password change phase, the terminal allows the MU to change the current password PW_i with the new password PW_i^{new}. The MU has to insert his/her smart card into the terminal. After insertion, the MU has to provide his/her credentials to the terminal. Once the MU has entered ID_i and current password PW_i, the terminal processes the information. Then the smart card computes the following:

Step 1: $h(h(ID_i||PW_i) \oplus h(r_m)) = RPW \oplus S$.

Verifies if $h(h(ID_i||PW_i) \oplus h(r_m)) \stackrel{?}{=} RPW \oplus S$.

Step 2: If it holds true, the smart card allows the MU to update the current password PW_i with the new password PW_i^{new}. The smart card asks the MU to enter the new password PW_i^{new}. After that, the smart card computes
$RPW^{'} = S^{'} \oplus h(h(ID_i||PW_i^{new}) \oplus h(r_m))$.
The parameter RPW, which is stored in the smart card, is replaced with $RPW^{'}$.

5.7. Proposed Two-Factor Authentication Scheme Extended to Multi-Factor Authentication Scheme

The multi-factor authentication schemes includes biometric input from the MU along with the password and the smart card that a MU possesses. Many devices use biometric authentication, such as fingerprint identification. Fingerprint identification is one of the most commonly used biometric technologies integrated in many mobile devices. In our proposed scheme, we describe how the three-factor authentication scheme is implemented during the registration phase. The three-factor authentication provides more security to the authentication schemes for the roaming MU for GLOMONET in the smart city to conform to the security goals designed for the ideal authentication scheme.

5.8. Registration Phase

The registration phase of the proposed multi-factor authentication scheme is as follows.

Step 1: MU $\rightarrow$ HN: $\{h(ID_i), PID\}$

In the registration phase, the MU is free to choose his/her identity ID_i and password PW_i along with the biometric fingerprint. The mobile device extracts the fingerprint information from the fuzzy extractor technique $Gen(B_{MU}) = (R_{MU}, P_M)$. After choosing ID_i, PW_i and random number r_m, the MU computes the following:

$$PID = h(h(ID_i||PW_i) \oplus h(r_m))$$

The MU submits $\{h(ID_i), PID, R_{MU}\}$ to the HN through a secure channel.

Step 2: HN $\rightarrow$ MU:$\{E_p, P, n, a, b, PK_{HN}, S, E_{mk}(.), Gen, Rep, P_M, h(.)\}$.

The HN receives the request from the MU and the HN chooses its random number r_h. The HN's server public key PK_{HN} is computed as

$$PK_{HN} = xP$$
$$S = PID \oplus h(mk) \oplus R_{MU}.$$

where x is a random number $\in Z_n$, and P is a generator point on the elliptic curve. HN stores $\{h(ID_i), S\}$ in it's database for future communication. HN sends the smart card with the parameters
$\{E_p, P, n, a, b, PK_{HN}, S, E_{mk}(.), Gen, Rep, P_M, h(.)\}$ to the MU through secure channel.

Step 3: MU : $\{E_p, P, n, a, b, PK_{HN}, S, E_{mk}(.), Gen, Rep, P_M, h(.)\}$

With the received message, MU computes the following

$$RPW = S \oplus h(h(ID_i||PW_i) \oplus h(r_m)).$$

The computed value of RPW is stored in the smart card. The smart card contains the parameters $\{E_p, P, n, a, b, PK_{HN}, S, E_{mk}(.), Gen, Rep, P_M, RPW, h(.)\}$.

6. Informal Security Analysis of the Proposed Scheme (ES-HAS)

In this section, through the informal security methods, we prove that the proposed scheme ES-HAS is resilient to the security attacks briefly explained below.

Informal security methods are demonstrated using the knowledge reasoning of the analysis of the protocol messages exchanged between the communicating entities over an insecure channel. With the informal security methods, we can prove the security of the protocol if it is weak or resilient to the security attacks in question.

6.1. Security against User Anonymity

User anonymity is an important security feature in GLOMONETs. The two-factor authentication schemes designed for GLOMONETs should protect user anonymity. In the proposed scheme, during the AESK phase, if an adversary intercepts the message $M_1 = \{R_1, AID_{new}, Q_m\}$ transmitting on the public channel and gains access to the parameters in M_1, it is of no use, as the value of ID_i is hashed, encrypted with the shared server secret key, and concatenated with the random number r_{new}. To get r_{new} from the computation $D_{mk}(E_{mk}(h(ID_i)||r_{new}))$, an adversary must know the decryption key mk, which is server's secret key shared between the MU through a secure channel. Therefore, the adversary will not be successful in revealing the ID_i, the MU's identity. Thus, the scheme protects user anonymity.

6.2. Security against Stolen Smart Card Attack

With the stolen smart card parameters $\{E_p, G, n, a, RPW, b, PK_{HN}, S, E_{mk}(.), r_m, h(.)\}$ and the intercepted login message $M_1 = \{R_1, AID_{new}, Q_m\}$, if an adversary tries to reveal ID_i and PW_i, it is impossible to compute, due to the fact that the parameter RPW is computed as $RPW = S \oplus h(h(ID_i||PW_i) \oplus h(r_m))$. To arrive at the identity and password of the MU, an adversary has to guess both ID_i and PW_i accurately and in addition to this, it must also guess the parameter S, which is computed as $S = PID \oplus SK_{HN}$. Thus, even if an adversary possesses the smart card, he/she will still be unsuccessful in revealing the identity and password of the MU. Therefore, the scheme is resilient to the stolen-smart-card attack.

6.3. Security against Offline Password-Guessing Attack

With the interception of the login messages $M_1 = \{R_1, AID_{new}, Q_m\}$ and $M_2 = \{Q_f, R_2, R_1, V_f, ID_{FN}\}$ during the AESK phase along with the stolen smart card parameters $\{E_p, G, n, a, RPW, b, PK_{HN}, S, E_{mk}(.), r_m, h(.)\}$, if an adversary makes a trial to reveal PW_i by computing $S = RPW \oplus h(h(ID_i||PW_i) \oplus h(r_m))$, to arrive at the correct value of S, he/she should guess the accurate values of ID_i and PW_i. Guessing two parameters at a given time becomes complex, and the hash operations on ID_i and PW_i makes the guessing more complex. Thus, the scheme is resilient to the password-guessing attack.

6.4. Security against Replay Attack

Suppose, by intercepting the login messages during the AESK phase, that an adversary tries to replay the messages $M_1 = \{R_1, AID_{new}, Q_m\}$ and $M_2 = \{Q_f, R_2, R_1, V_f, ID_{FN}\}$ as $M_1^{'}$ and $M_2^{'}$ and then sends it to the HN. The HN, on receiving the messages $M_1^{'}$ and $M_2^{'}$, computes for the secret key SK_{FN} and checks for the freshness of the random number r_{new}. Both the parameters can be computed only by the valid HN. After computing, the HN verifies if $V_f \stackrel{?}{=} h(Q_f||Q_m||SK_{FN}||R_1||R_2)$. If the parameter V_f holds true, then the HN authenticates both the FN and MU. Otherwise, the HN terminates the connection request. It is difficult for an adversary to compute SK_{FN} (the secret key of FN), as SK_{FN} is concealed with PK_{HN} (the public key of the HN) and mk (the secret key of the HN). The random number r_{new} is concealed with S, the secret parameter of the HN. Hence, even if an adversary tries to replay the messages and sends it to the HN which checks for the freshness of the random number r_{new} and also checks for the correctness of the message. If the verification fails, the HN terminates the request. The random number r_{new} is the

output sequence generated by the pseudo-random function, satisfying the properties as mentioned in Section 3.7.1. Thus, the proposed scheme is resilient to the replay attack.

6.5. Perfect Forward Secrecy

The session key is computed using the elliptic curve Diffie–Hellman Protocol (ECDHP) as $SK = h(R_1||R_2||\beta R_1)$ by FN. During the AESK phase, if an adversary intercepts the messages $M_4 = \{V_H, ID_{FN}, K, R_2\}$ and $M_1 = \{R_1, , AID_{new}, Q_m\}$ and tries to compute $SK = K \oplus h(Q_m||R_1||ID_{FN}||\alpha R_2)$, even with the disclosure of the session key, it is difficult to calculate the value of $\beta \in Z_n^*$ due to the fact that, given an elliptic curve E defined over a finite prime field F_p and points $P, \alpha P, \beta P \in E(F_p)$, it is difficult to compute $\alpha\beta P$ due to the hardness of the ECDH problem. For every new login request, a session key is computed, which makes it difficult for an adversary to arrive at the session key for every new login session. Thus, the scheme achieves perfect forward secrecy.

6.6. Security against Impersonation Attack

1. Impersonate a FN.
   If an adversary intercepts the message $M_1 = \{R_1, AID_{new}, Q_m\}$ and $M_2 = \{Q_f, R_2, R_1, V_f, ID_{FN}\}$ transmitting over an insecure channel during the AESK phase and sends the same message M_2 to HN, on receiving M_2, the HN computes $SK_{FN} = h(ID_{FN}||PK_{HN}||mk)$. PK_{FN} is a public key and mk is a secret key computed by the HN.

   $$V_f \stackrel{?}{=} h(Q_f||Q_m||SK_{FN}||R_1||R_2).$$

   The HN verifies if $V_f \stackrel{?}{=} h(Q_f||Q_m||SK_{FN}||R_1||R_2)$.
   If it holds true, the HN authenticates the FN based on its secret key computed by the HN. Thus, it is difficult for an adversary to impersonate a legal FN.
2. Impersonate a MU.
   With the interception of message $M_1 = \{R_1, AID_{new}, Q_m\}$ transmitting over an insecure channel, the adversary tries to reveal the identity of the parameters by capturing message M_1 and thus $AID_{new} = E_{mk}(h(ID_i)||r_{new})$. The HN uses its secret key for encrypting the identity and random number of MU. To perform decryption, an adversary must have the server secret key. Thus, it is difficult to impersonate a valid MU.

6.7. Man-in-the-Middle Attack

The man-in-the-middle attack is an active security attack. An attacker has the capability to eavesdrop the online authentication messages transmitted over an insecure channel. The intercepted messages are then replayed by an attacker to establish a session among the entities involved in the communication. The entities believe that the communication is carried between the legitimate entities. The legitimate entities are not aware of the session establishment with an attacker. The entire communication channel is controlled by an attacker.

In the proposed scheme, it is difficult for an attacker to mount such an attack. An attacker can eavesdrop all the messages transmitted over the insecure channel as shown in Figure 5. With the interception of the authentic messages $\{M_1, M_4\}$, the attacker would not be able to derive the session key without the knowledge of the private key β due to the complexity of the elliptic curve discrete logarithm problem (ECDLP). (The ECDLP is explained in Section 3.2).

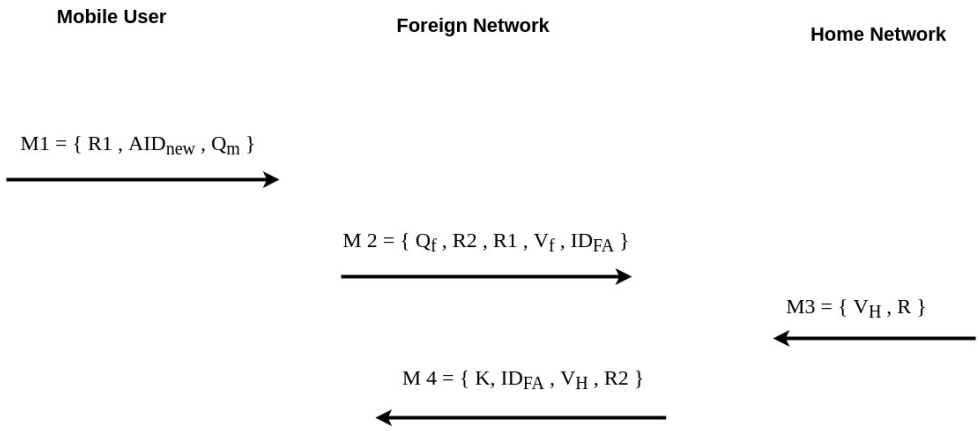

Figure 5. Message flow of login and authentication phase.

6.8. Local Password Verification

In the login phase of the proposed scheme, the mobile device validates the MU credentials through prompting the MU to input the $\{ID_{MU}, PW_{MU}\}$. After the MU input, the following computations are performed.

$$h(h(ID_i||PW_i) \oplus h(r_m)) \stackrel{?}{=} RPW \oplus S.$$

After successful verification, further computations are performed and the login request message M_1 is sent to the FN. An attacker cannot compute the correct $h(h(ID_i||PW_i) \oplus h(r_m))$ without the knowledge of $\{ID_{MU}, PW_{MU}, r_m\}$ to succeed the verification step $h(h(ID_i||PW_i) \oplus h(r_m)) \stackrel{?}{=} RPW \oplus S$. Therefore, the proposed authentication scheme is designed to avoid unauthorized use of mobile devices by verifying the password locally.

6.9. Security against User Untraceability

In the proposed scheme, the login message $M_1 = \{R_1, AID_{new}, Q_m\}$ carries the identity of the MU, which is encrypted with the shared symmetric key between MU and HN. If an attacker attempts to eavesdrop the login message $AID_{new} = E_{mk}(h(ID_i)||r_{new})$ transmitted over an insecure channel, decryption of the ID_{MU} without the decryption key is not possible. To trace a MU, an adversary keeps track of the authentication sessions between the MU and FN. For every session, the message $\{AID_{new}\}$ contains the fresh random value. Furthermore, $\{AID_{new}\}$ varies in each session because it is generated by the random number r_{new}. Hence, the proposed scheme satisfies user anonymity and untraceability.

7. Formal Security Analysis of the Proposed Scheme (ES-HAS) Using BAN Logic

In this section, the formal security verification of the proposed scheme ES-HAS using BAN Logic [13] is presented.

BAN logic is a formal tool that enables to analyze the correctness of an authentication protocol. It includes mutual authentication and key distribution. The notations P and Q denote principals; X and Y denote statements; and K is the cryptographic key. Table 3 provides the meaning for the BAN logic symbols.

Table 3. Notations used in BAN logic.

Notation	Definition
$P\mid\equiv X$	P believes X: P would be entitled to believe X.
$P \lhd X$	P sees X: P can receive and read X
$P\mid\sim X$	P said X: P once said X
$P\mid\Rightarrow X$	P controls X: P has jurisdiction over X
$\#(X)$	Fresh (X): The formula X is fresh
$\langle X\rangle_y$	X is integrated with y; y should be kept secret
$P \overset{K}{\leftrightarrow} Q$	K is used as a shared key between P and Q
$P \overset{y}{\rightleftharpoons} Q$	The formula y is shared between two principals P and Q
$Y = (X)_h$	Y is hash of X

Logic postulates of BAN logic

1. Message meaning rule for shared secrets: $\frac{P\mid\equiv Q\overset{y}{\rightleftharpoons}P, P\lhd\langle X\rangle_y}{P\mid\equiv Q\mid\sim X}$
2. Nonce-verification rule: $\frac{P\mid\equiv\#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$
3. Jurisdiction rule: $\frac{P\mid\equiv Q\mid\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$
4. Receiving rule: $\frac{P\lhd(X,Y)}{P\lhd X}$ and $\frac{P\lhd\langle X\rangle_y}{P\lhd X}$
5. Freshness-propagation rule: $\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$
6. Session-key rule: $\frac{P\mid\equiv\#(K), P\mid\equiv Q\mid\equiv X}{P\mid\equiv P\overset{K}{\leftrightarrow}Q}$

According to the analytic procedure of BAN logic, the proposed scheme must satisfy the following goals to prove the system is secure. G $\rightarrow$ Goal

G1 : $FN\mid\equiv R1$
G2 : $FN\mid\equiv MU\mid\equiv R1$
G3 : $HN\mid\equiv\#(R1, R2)$
G4 : $HN\mid\equiv HN \overset{SK_{FN}}{\leftrightarrow} FN$
G5 : $FN\mid\equiv FN \overset{SK}{\leftrightarrow} MU$

We summarize the proposed protocol in the following generic form:

1. Message M1: $MU \rightarrow FN : \{R_1, AID_{new}, Q_m\}$
   $R_1 = \alpha P$, $AID_{new} = E_{mk}(h(ID_i)||r_{new})$
   $Q_m = r_{new} \oplus h(S||r_{new}||R_1)$.
2. Message M2: $FN \rightarrow HN : \{Q_f, R_2, R_1, V_f, ID_{FN}\}$
   $R_2 = \beta P$, $Q_f = Q_m \oplus h(SK_{FN})$
   $V_f = h(Q_f||Q_m||SK_{FN}||R_1||R_2)$. Where SK_{FN} is a secret key of FN, computed by HN.
3. Message M3: $HN \rightarrow FN : \{V_H, R\}$
   $V_H = AID_{new} \oplus h(S||h(mk)||r_{new})$
   $R = h(Q_m||Q_f||SK_{FN}||R_2)$.
4. Message M4: $FN \rightarrow MU : \{K, ID_{FN}, V_H, R_2\}$
   $K = SK \oplus h(Q_m||R_1||ID_{FN}||\beta R_1)$.

Hypothesis 1. *The following assumptions about the initial states are made to analyze the proposed scheme:*

I_1. $MU\mid\equiv MU \overset{R1}{\longleftrightarrow} FN$
I_2. $FN\mid\equiv FN \overset{R2}{\longleftrightarrow} MU$
I_3. $MU\mid\equiv MU \overset{SK}{\rightleftharpoons} FN$
I_4. $FN\mid\equiv FN \overset{SK}{\rightleftharpoons} MU$

I_5. $MU| \equiv \#(\alpha)$
I_6. $MU| \equiv \#(r_{new})$
I_7. $HN| \equiv \#(R1)$
I_8. $FN| \equiv \#(\beta)$
I_9. $FN| \equiv HA| \Rightarrow SK_{FN}$
I_{10}. $MU| \Rightarrow R_1$
I_{11}. $FN| \equiv \#(R1)$
I_{12}. $FN| \equiv MU| \sim R1$
I_{13}. $HA| \equiv \#(R2)$
I_{14}. $HN| \equiv MU| \Rightarrow R_1$
I_{15}. $HN| \equiv FN| \Rightarrow R_2$
I_{16}. $HN| \equiv \#(R2)$
I_{17}. $HN| \equiv \#(SK_{FN})$

The generic form of the proposed scheme is transformed into the idealized form. The following assumptions are made to analyze the proposed scheme. The main proofs are stated as follows.

- From message M_1, we have the following:
  S_1: $FN \lhd R_1$. From jurisdiction rule R3 and I_{11}, we have
  $\frac{FN|\equiv MU|\Rightarrow R1, MU|\equiv FN|\equiv R1}{FN|\equiv R1}$ (Goal G1)
- From message M_2, I_{12}, I_{13} , we have
  $\frac{FN|\equiv \#(R1), FN|\equiv MU| \sim R1}{FN|\equiv MU|\equiv R1}$ (Goal G2)
- From message M_3, I_7, I_{15}, I_{16}, I_{17} and freshness propagation rule 5, we have
  $\frac{HN|\equiv \#(R1)}{HN|\equiv \#(R1,R2)}$. (Goal G3)
  From session-key rule 6 and I_9, I_{18}, we have
  $\frac{HN|\equiv \#(SK_{FN}), HN|\equiv FN|\equiv SK_{FN}}{HN|\equiv HN \overset{SK_{FN}}{\leftrightarrow} FN}$ (Goal G4)
- From message M_4, I_1, I_2, I_3, I_4 and session-key rule 6, we have
  $\frac{FN|\equiv \#(SK), FN|\equiv MU|\equiv SK}{FN|\equiv FN \overset{SK}{\leftrightarrow} MU}$ (Goal G5)

8. Formal Security Verification of the Proposed Scheme (ES-HAS) Using AVISPA Tool

To provide the results of the formal security verification of the proposed scheme, the automated validation of internet security protocols and applications (AVISPA) tool is used. The proposed scheme is simulated and verified against active and passive security attacks. Firstly, the AVISPA tool is introduced; secondly, the implementation details of the proposed scheme using AVISPA are presented; and finally, the output of the simulation is presented.

8.1. Overview of AVISPA

AVISPA is a tool which is widely accepted for the verification of the cryptographic protocols. One of the major advantages of the AVISPA tool is that the same protocol specification can be verified by different verification techniques. The cryptographic protocol is written in HLPSL (high level protocol specification language). HLPSL is an expressive, modular, role-based, formal language. The cryptographic protocol written in HLPSL is first converted into an intermediate format (IF) by the HLPSL2IF translator. Later, this IF is executed by the backend that the AVISPA tool uses. Backend tools supported by AVISPA are on-the-fly model-checker (OFMC), constraint logic based attack searcher (CL-AtSe), SAT-based model checker (SATMC) and tree automata based on automatic approximations for the analysis of security protocols (TA4SP). The AVISPA tool uses the OFMC/CL-AtSe back-end to execute IF, which is then converted to output format (OF) [14]. OF includes the sections which are explained in detail below.

1. SUMMARY: It summarizes about the executed protocol safe or unsafe property, where safe signifies that the tested protocol is safe and unsafe signifies that the tested protocol is insecure.

2. DETAILS: This section gives details about the conditions that are used in the test to make the protocol safe or unsafe.
3. PROTOCOL: This section provides the name of the protocol that is to be tested.
4. GOAL: The test's goal is specified in this section.
5. BACKEND: The backend name that is used to execute the test is specified in this section.
6. COMMENTS and STATISTICS: This section demonstrates the attacker simulation if the test is unsafe.

The HLPSL basic types are listed below:

1. agent: It indicates the principal roles used in the HLPSL language and i denotes the intruder.
2. const: It indicates constants.
3. public_key: It indicates the public key used by agents in the test.
4. symmetric_key: It specifies about the symmetric key used by the agents in the test.
5. text: This can be used for nonces or sometimes for messages.
6. nat: This signifies the natural numbers that are used in non-message contexts.

In HLPSL, concatenation operation is denoted by the declaration, such as played_by X indicating that X is an agent and knowledge indicating the intruder's knowledge. $X =|> Y$ represents the immediate reaction transitions.

8.2. HLPSL Implementation

HLPSL uses three basic roles: mobileuser played_by the MU, foreignagent played_by the FN, and homeagent played_by the HN. The three supporting roles used in the HLPSL implementation are environment, session and role.

The output of the program using back-end OFMC is presented in Figure 6. The output of the program using back-end CL-ATSE is presented in Figure 7.

Figure 6. Output analysis using OFMC back-end.

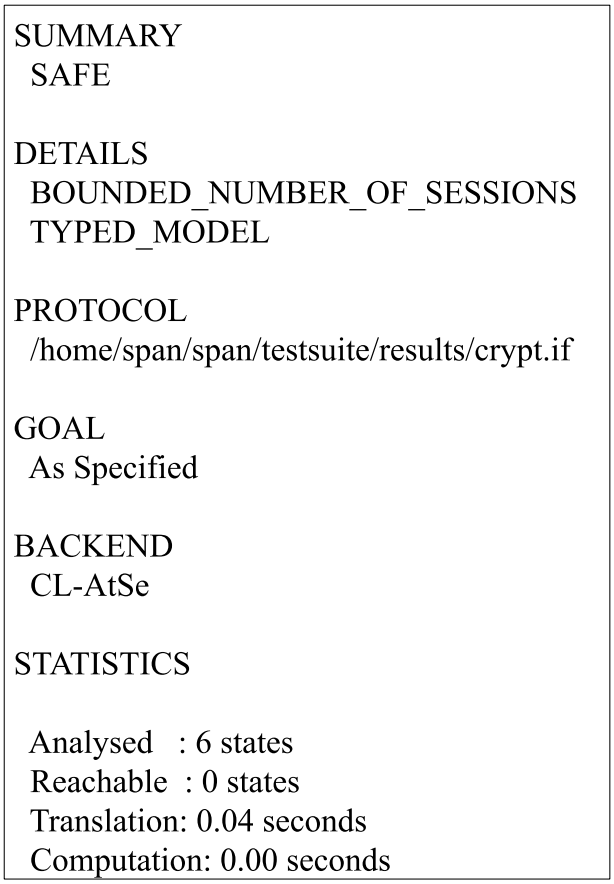

Figure 7. Output analysis using CL-Atse back-end.

9. Performance Analysis and Comparison

This section evaluates performance of the proposed scheme with the other authentication schemes proposed for GLOMONET. These seven authentication schemes are based on the elliptic curve cryptosystem. The proposed authentication scheme is also based on the elliptic curve cryptosystem. These seven schemes are introduced by Mahadi et al. [57], Ghahramani et al. [48], Li et al. [4], Zhao [40], Odelu et al. [39], Banerjee et al. [42] and Li et al. [58], respectively.

The proposed scheme makes the following assumptions to compute the communication overhead during the login phase. The symmetric encryption key length is 128 bits, the one-way hash function output is 160 bits in length, the random number is 128 bits in length, the identity is 32 bits in length, and the elliptic curve point is 256 bits. The proposed scheme establishes four communication rounds with the server. Considering the communication overhead of messages transmission in one authentication session for our proposed scheme, within the login phase, the length of the user's login request message $M_1 = \{R_1, AID_{new}, Q_m\}$ is 672 bits, the visited network request to the HN to authenticate the MU's login request message $M_2 = \{Q_f, R_2, R_1, V_f, ID_{FN}\}$ is 704 bits in length. The HN server message $M_3 = \{V_H, R\}$ is 448 bits in length and the response message $M_4 = \{K, ID_{FN}, V_H, R_2\}$ from the visited network to the MU is 896 bits in length. Table 4 compares the security features of the proposed scheme with the four other authentication schemes. The proposed scheme achieves all the listed security features compared to the other schemes. Our scheme requires no intervention of the server during the password change phase, which otherwise creates hassle and increases the communication cost. The password is verified locally in the proposed scheme. Our scheme is secure and efficient with minimal communication overhead compared to the other four schemes to perform handover procedures in GLOMONET.

Table 4. Comparison on security features.

	S1	S2	S3	S4	S5	S6	S7	S8	S9
Mahadi et al. [57]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ghahramani et al. [48]	Yes	No	Yes	No	No	No	Yes	No	No
Li et al. [4]	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Zhao [40]	No	No	No	Yes	Yes	Yes	No	Yes	No
Odelu et al. [39]	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No
Banerjee et al. [42]	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Li et al. [58]	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Ours	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

S1—user anonymity; S2—resistance to stolen-smart-card attack; S3—resistance to offline password-guessing attack; S4—resistance to replay attack; S5—mutual authentication; S6—resistance to impersonation attack; S7—resistance to man-in-the-middle attack; S7—local password verification; S8—perfect forward secrecy; S9—user untraceability.

Table 5 gives the computational costs performed both at the user side and server side within the three different phases, including the registration phase, login phase and password change phase. In the proposed scheme, the user side computes three one-way hash functions to compute the parameter $PID = h(h(ID_i||PW_i) \oplus h(r_m))$. At the server side, the proposed scheme executes two hash functions and one multiplication of a number over a point on the elliptic curve to compute the secret values $SK_{FN} = h(ID_{FN}||PK_{HN}||mk)$ and $S = PID \oplus h(mk)$. Similarly, the login phase at the user side requires seven hash functions, two symmetric functions and two multiplications of a number over a point on the elliptic curve. The login phase at the server side requires four hash functions and three multiplication of a number over a point on the elliptic curve. The password phase at the user side requires two hash functions.

- T_h time taken to execute one hash function.
- T_{symm} time taken to execute one symmetric encryption/decryption operation.
- T_{EC_M} time taken to execute multiplication operation on elliptic curve.
- T_f time of a fuzzy extractor.
- T_{asymm} time taken to execute one asymmetric encryption/decryption operation.
- T_a time taken to perform ECC point addition.
- T_{se} time taken for sign operation.
- T_v time of signature verification.

Table 6 tabulates the communication overhead between the propossed and the other schemes. Based on each round of messages exchange during login and authentication phase, the signal overhead is computed. Figure 8 compares the signal overhead between the proposed scheme and other schemes.

Table 5. Comparison on computational cost.

	Total Computations
Mahadi et al. [57]	$17T_h + 7T_{ecc} + 4T_{asymm} + 2T_{symm}$
Ghahramani et al. [48]	$22T_h + 13T_{ecc} + 1T_f$
Li et al. [4]	$21T_h + 10T_{ecc} + 1T_f + 2T_p$
Zhao [40]	$11T_{ecc} + 6T_{symm} + 2T_{asymm} + 15T_h$
Odelu et al. [39]	$15T_{ecc} + 2T_a + 2T_{symm} + 2T_v + 17T_h$
Banerjee et al. [42]	$9T_{ecc} + 8T_{se} + 1T_f + 13T_h$
Li et al. [58]	$16T_h + 6T_{ecc}$
Ours	$27T_h + 5T_{ecc} + 3T_{symm}$

Table 6. Comparison on communication cost.

	Communication Cost
Mahadi et al. [57]	2144
Ghahramani et al. [48]	3424
Li et al. [4]	3424
Zhao [40]	7424
Odelu et al. [39]	5888
Banerjee et al. [42]	3072
Li et al. [58]	3296
Ours	3168

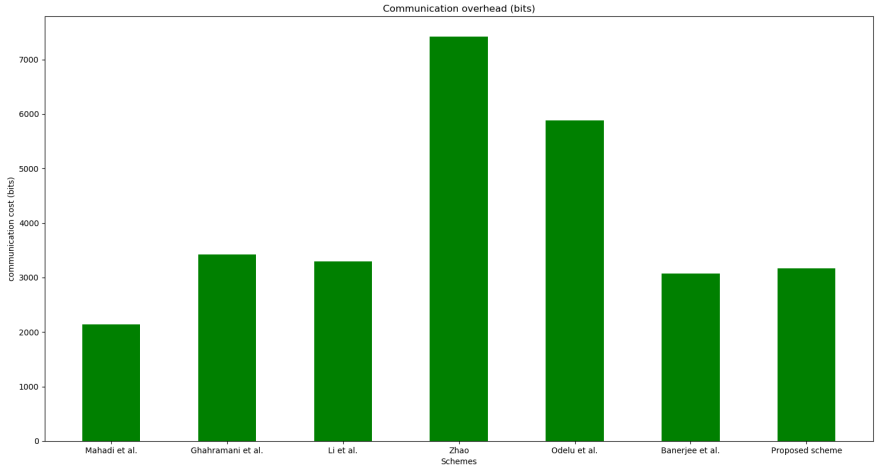

Figure 8. Comparison on communication cost in (bits).

10. Conclusions

In this article, the proposed ES-HAS scheme provides secure services to roaming mobile users. The proposed ES-HAS scheme is resilient to security attacks, such as MU impersonation, stolen-smart-card, offline password-guessing, man-in-the-middle and replay attacks. The ES-HAS scheme also achieves security goals such as user anonymity, user untraceability, perfect forward secrecy and mutual authentication. The shared secret key is computed using elliptic curve cryptography, and this secret key is exchanged between the two communicating entities, FN and HN, during communication to authenticate each other. The proposed scheme is proved using the formal security tool, BAN logic. Furthermore, the ES-HAS scheme is simulated using the AVISPA tool to formally verify whether the proposed scheme is secure against replay and man-in-the-middle attacks. The security features achieved by the different authentication schemes and the proposed scheme are compared. The comparison results shows that the proposed scheme achieves all the security features mentioned. The informal security analysis of the proposed scheme proves that the ES-HAS scheme achieves all the mentioned security features. In comparison with the computational cost and communication overhead of the proposed scheme with the other related schemes, the proposed scheme operates with minimal communication overhead in order to provide better security. Therefore, the proposed scheme is lightweight and practical to implement.

Author Contributions: Conceptualization, S.K.S.; methodology, S.K.S., J.R.; software, S.K.S.; validation, J.R.; formal analysis, S.K.S.; investigation, J.R., S.S.K.; resources, S.K.S., J.R., S.S.K.; data curation, S.K.S.; writing, S.K.S., J.R.; supervision, C.-C.L.; project administration, C.-C.L.; funding acquisition, C.-C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in article.

Acknowledgments: The author would like to thank the anonymous reviewers for their very constructive comments and suggestions, which helped to greatly improve the manuscript.

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

References

1. Odelu, V.; Das, A.K.; Goswami, A. An efficient biometric-based privacy-preserving three-party authentication with key agreement protocol using smart cards. *Secur. Commun. Netw.* **2015**, *8*, 4136–4156. [CrossRef]
2. Park, Y.; Park, Y. Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. *Sensors* **2016**, *16*, 2123. [CrossRef] [PubMed]
3. Yu, S.; Lee, J.; Park, Y.; Park, Y.; Lee, S.; Chung, B. A secure and efficient three-factor authentication protocol in global mobility networks. *Appl. Sci.* **2020**, *10*, 3565. [CrossRef]
4. Li, X.; Niu, J.; Kumari, S.; Wu, F.; Choo, K.K.R. A robust biometrics based three-factor authentication scheme for global mobility networks in smart city. *Future Gener. Comput. Syst.* **2018**, *83*, 607–618. [CrossRef]
5. Madhusudhan, R.; Shashidara, R. A secure and lightweight authentication scheme for roaming service in global mobile networks. *J. Inf. Secur. Appl.* **2018**, *38*, 96–110. [CrossRef]
6. Kuo, W.C.; Wei, H.J.; Cheng, J.C. An efficient and secure anonymous mobility network authentication scheme. *J. Inf. Secur. Appl.* **2014**, *19*, 18–24. [CrossRef]
7. Guo, D.; Wen, F. A More Robust Authentication Scheme for Roaming Service in Global Mobility Networks Using ECC. *Int. J. Netw. Secur.* **2016**, *18*, 217–223.
8. Lee, C.C.; Lai, Y.M.; Chen, C.T.; Chen, S.D. Advanced secure anonymous authentication scheme for roaming service in global mobility networks. *Wirel. Pers. Commun.* **2016**, *94*, 1281–1296. [CrossRef]
9. Karuppiah, M.; Kumari, S.; Li, X.; Wu, F.; Das, A.K.; Khan, M.K.; Saravanan, R.; Basu, S. A dynamic id-based generic framework for anonymous authentication scheme for roaming service in global mobility networks. *Wirel. Pers. Commun.* **2017**, *93*, 383–407. [CrossRef]
10. Alzahrani, B.A.; Chaudhry, S.A.; Barnawi, A.; Al-Barakati, A.; Alsharif, M.H. A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks. *Symmetry* **2020**, *12*, 287. [CrossRef]
11. Madhusudhan, R.; Shashidhara, R. Mobile user authentication protocol with privacy preserving for roaming service in GLOMONET. *Peer-to-Peer Netw. Appl.* **2020**, *13*, 82–103. [CrossRef]
12. Kang, D.; Lee, H.; Lee, Y.; Won, D. Lightweight user authentication scheme for roaming service in GLOMONET with privacy preserving. *PLoS ONE* **2021**, *16*, e0247441. [CrossRef] [PubMed]
13. Burrows, J.H. *Secure Hash Standard*; Technical Report; Department of Commerce: Washington, DC, USA, 1995.
14. AVISPA. Automated Validation of Internet Security Protocols and Applications. 2019. Available online: http://www.avispa-project.org/ (accessed on 1 March 2019).
15. Hwang, M.; Yang, W. Conference key distribution schemes for secure digital mobile communication network. *IEEE J. Select. Areas Commun.* **1995**, *13*, 416–420. [CrossRef]
16. Hwang, M. Dynamic participation in a secure conference scheme for mobile communications. *IEEE Trans. Veh. Technol.* **1999**, *48*, 1469–1474. [CrossRef]
17. Buttyan, L.; Gbaguidi, C.; Staamann, S.; Wilhelm, U. Extensions to an authentication technique proposed for the global mobility network. *IEEE Trans. Commun.* **2000**, *48*, 373–376. [CrossRef]
18. Hwang, K.; Chang, C. A self-encryption mechanism for authentication of roaming and teleconference services. *IEEE Trans. Wirel. Commun.* **2003**, *2*, 400–407. [CrossRef]
19. Zhu, J.; Ma, J. A new authentication scheme with anonymity for wireless environments. *IEEE Trans. Consum. Electron.* **2004**, *50*, 231–235.
20. Lee, C.; Hwang, M.; Liao, I. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans. Ind. Electron.* **2006**, *53*, 1683–1687. [CrossRef]
21. Wei, Y.; Qiu, H.; Hu, Y. Security analysis of authentication scheme with anonymity for wireless environments. In Proceedings of the 2006 International Conference on Communication Technology, Guilin, China, 27–30 November 2006; pp. 1–4.
22. Huang, X.; Chen, X.; Li, J.; Xiang, Y.; Xu, L. Further observations on smart-card-based password-authenticated key agreement in distributed systems. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *25*, 1767–1775. [CrossRef]
23. Juang, W.S.; Chen, S.T.; Liaw, H.T. Robust and efficient password-authenticated key agreement using smart cards. *IEEE Trans. Ind. Electron.* **2008**, *55*, 2551–2556. [CrossRef]
24. Wang, D.; He, D.; Wang, P.; Chu, C.H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 428–442. [CrossRef]
25. Tsai, J.L.; Lo, N.W.; Wu, T.C. Novel anonymous authentication scheme using smart cards. *IEEE Trans. Ind. Inform.* **2012**, *9*, 10. [CrossRef]
26. Xu, G.; Liu, J.; Lu, Y.; Zeng, X.; Zhang, Y.; Li, X. A novel efficient MAKA protocol with desynchronization for anonymous roaming service in global mobility networks. *J. Netw. Comput. Appl.* **2018**, *107*, 83–92. [CrossRef]

27. Gope, P.; Hwang, T. An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *J. Netw. Comput. Appl.* **2015**, *62*, 1–8. [CrossRef]
28. Ostad-Sharif, A.; Babamohammadi, A.; Abbasinezhad-Mood, D.; Nikooghadam, M. Efficient privacy-preserving authentication scheme for roaming consumer in global mobility networks. *Int. J. Commun. Syst.* **2019**, *32*, e3904. [CrossRef]
29. Arshad, H.; Rasoolzadegan, A. A secure authentication and key agreement scheme for roaming service with user anonymity. *Int. J. Commun. Syst.* **2017**, *30*, e3361. [CrossRef]
30. Chen, R.; Peng, D. An anonymous authentication scheme with the enhanced security for wireless communications. *Wirel. Pers. Commun.* **2017**, *97*, 2665–2682. [CrossRef]
31. Xie, Q.; Hu, B.; Tan, X.; Wong, D.S. Chaotic maps-based strong anonymous authentication scheme for roaming services in global mobility networks. *Wirel. Pers. Commun.* **2017**, *96*, 5881–5896. [CrossRef]
32. Wei, F.; Vijayakumar, P.; Jiang, Q.; Zhang, R. A mobile intelligent terminal based anonymous authenticated key exchange protocol for roaming service in global mobility networks. *IEEE Trans. Sustain. Comput.* **2018**, *5*, 268–278. [CrossRef]
33. Wang, D.; Wang, P.; Liu, J. Improved privacy-preserving authentication scheme for roaming service in mobile networks. In Proceedings of the 2014 IEEE wireless communications and networking conference (WCNC), Istanbul, Turkey, 6–9 April 2014; pp. 3136–3141.
34. Li, H.; Yang, Y.; Pang, L. An efficient authentication protocol with user anonymity for mobile networks. In Proceedings of the 2013 IEEE wireless communications and networking conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 1842–1847.
35. Shin, S.; Yeh, H.; Kim, K. An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks. *Peer-to-Peer Netw. Appl.* **2015**, *8*, 674–683. [CrossRef]
36. Farash, M.S.; Chaudhry, S.A.; Heydari, M.; Sajad Sadough, S.M.; Kumari, S.; Khan, M.K. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *Int. J. Commun. Syst.* **2017**, *30*, e3019. [CrossRef]
37. Karuppiah, M.; Kumari, S.; Das, A.K.; Li, X.; Wu, F.; Basu, S. A secure lightweight authentication scheme with user anonymity for roaming service in ubiquitous networks. *Secur. Commun. Netw.* **2016**, *9*, 4192–4209. [CrossRef]
38. He, D.; Ma, M.; Zhang, Y.; Chen, C.; Bu, J. A strong user authentication scheme with smart cards for wireless communications. *Comput. Commun.* **2010**, *34*, 367–374. [CrossRef]
39. Odelu, V.; Banerjee, S.; Das, A.K.; Chattopadhyay, S.; Kumari, S.; Li, X.; Goswami, A. A secure anonymity preserving authentication scheme for roaming service in global mobility networks. *Wirel. Pers. Commun.* **2017**, *96*, 2351–2387. [CrossRef]
40. Zhao, D.; Peng, H.; Li, L.; Yang, Y. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wirel. Pers. Commun.* **2014**, *78*, 247–269. [CrossRef]
41. Wu, F.; Li, X.; Xu, L.; Kumari, S.; Sangaiah, A.K. A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion. *Comput. Electr. Eng.* **2018**, *68*, 107–118. [CrossRef]
42. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Park, Y.; Tanwar, S. Design of an anonymity-preserving group formation based authentication protocol in global mobility networks. *IEEE Access* **2018**, *6*, 20673–20693. [CrossRef]
43. Karuppiah, M.; Saravanan, R. A secure authentication scheme with user anonymity for roaming service in global mobility networks. *Wirel. Pers. Commun.* **2015**, *84*, 2055–2078. [CrossRef]
44. Lu, Y.; Xu, G.; Li, L.; Yang, Y. Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks. *IEEE Syst. J.* **2019**, *13*, 1454–1465. [CrossRef]
45. Gope, P.; Hwang, T. Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. *IEEE Syst. J.* **2016**, *10*, 1370–1379. [CrossRef]
46. Aghili, S.F.; Mala, H.; Shojafar, M.; Conti, M. Pakit: Proactive authentication and key agreement protocol for internet of things. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April–2 May 2019; pp. 348–353.
47. Wan, Z.; Xu, Z.; Liu, S.; Ni, W.; Ye, S. An internet of things roaming authentication protocol based on heterogeneous fusion mechanism. *IEEE Access* **2020**, *8*, 17663–17672. [CrossRef]
48. Ghahramani, M.; Javidan, R.; Shojafar, M. A secure biometric-based authentication protocol for global mobility networks in smart cities. *J. Supercomput.* **2020**, *76*, 8729–8755. [CrossRef]
49. Jiang, Q.; Ma, J.; Li, G.; Yang, L. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wirel. Pers. Commun.* **2013**, *68*, 1477–1491. [CrossRef]
50. Neil, K. Ëlliptc Curve Cryptosystem. *Math. Comput.* **1987**, *48*, 203–209.
51. Rogaway, P.; Shrimpton, T. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International Workshop on Fast Software Encryption*; Springer: Berlin, Germany, 2004; pp. 371–388.
52. Bhattacharjee, K.; Maity, K.; Das, S. A search for good pseudo-random number generators: Survey and empirical studies. *arXiv* **2018**, arXiv:1811.04035.
53. Dodis, Y.; Ostrovsky, R.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.* **2008**, *38*, 97–139. [CrossRef]
54. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]

55. Wu, F.; Xu, L.; Kumari, S.; Li, X.; Das, A.K.; Khan, M.K.; Karuppiah, M.; Baliyan, R. A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. *Secur. Commun. Netw.* **2016**, *9*, 3527–3542. [CrossRef]
56. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In *Annual International Cryptology Conference*; Springer: Berlin, Germany, 1999; pp. 388–397.
57. Nikooghadam, M.; Amintoosi, H.; Kumari, S. A provably secure ECC-based roaming authentication scheme for global mobility networks. *J. Inf. Secur. Appl.* **2020**, *54*, 102588. [CrossRef]
58. Li, X.; Sangaiah, A.K.; Kumari, S.; Wu, F.; Shen, J.; Khan, M.K. An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city. *Pers. Ubiquitous Comput.* **2017**, *21*, 791–805. [CrossRef]