ENTHUSIASTIC
INTERNATIONAL JOURNAL OF APPLIED STATISTICS AND DATA SCIENCE
Volume 3, Issue 1, April 2023, pp. 1-15

Key Agreement Scheme Based on Smart Cards

Graygorry Brayone Ekal [a,1,*], Eddie Shahril Ismail [a,2], Abdul Rahman Farhan bin Sabdin [a,3]

[a] Department of Mathematical Sciences, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia
[1] graygorrybrayone@gmail.com*; [2] esbi@ukm.edu.my; [3] a168637@siswa.ukm.edu.my
* Corresponding author

ARTICLE INFO

Keywords
Cryptography
Key agreement
Smart card
Global mobility network
Roaming

ABSTRACT

An efficient roaming service over wireless networks is essential for mobile users. It allows mobile users to seamlessly access the services provided by the home agent without losing connectivity when they visit a foreign network. This handover communication happens with the help of a foreign agent. In most cases, the communication between the mobile user and the foreign agent occurs over an unsecured channel. Therefore, researchers have proposed various authentication schemes to protect data transmitted over this unsecured channel. Most of the proposed schemes are focused on key agreement schemes. However, the key agreement schemes researchers have submitted are primarily high in computational and communication costs. Therefore, this research proposed an authenticated key agreement scheme based on passwords and smart cards with lower computational and communication costs without compromising the scheme's security. This criterion was achieved due to using lower-cost operations and functions in the scheme. Moreover, the scheme's development is based on the result of analyzing and improving other schemes proposed by other researchers.

1. Introduction

Nowadays, wireless communication has become essential in various aspects of our life. For instance, transferring money from one person to another can be done anywhere through online banking without going to the bank. Furthermore, users can enjoy online shopping and communicate with each other wherever they are around the world, anytime they want. The ability of users to present at any place and still can access these services is facilitated by the global mobility network through roaming service [1]. In the global mobility network, there are three entities involved, namely "mobile user", "home agent", and "foreign agent" [2].

Moreover, the terms home network and foreign network are used throughout this paper. A home network is a network that is the permanent home of the mobile user. Meanwhile, a foreign network is a network to which the mobile user moves outside their home network coverage area. Next, a mobile user is a person from a home network who uses devices such as a mobile phone, laptop, or tablet. Next, home and foreign agents are routers at home and foreign networks, respectively [3]. The mobile user needs to register themselves at the home agent via a secured channel before they get their desired services. However, when the mobile user visits a foreign network, they must send a request to the foreign agent to use the services provided by the home agent.

Wireless signals are open and public; thus, the data transmission between the mobile user, the home agent, and the foreign agent is vulnerable to attacks from unauthorized parties. Hence, it is crucial to employ proper security protocols, which as roaming authentication, to resist attacks or overcome other protocol weaknesses [1]. If the mobile user is in their registered network, the home agent can verify the mobile user's authenticity. On the other hand, if the mobile user is in a foreign network, the foreign agent cannot directly authenticate the mobile user because it does not have the credentials of the mobile user. Therefore, through roaming authentication, the foreign agent is able to confirm the legitimacy of the mobile user with help from the home agent. A session key will be agreed upon between the foreign agent and the mobile user and will be used to secure the communication channel.

Apart from that, mobile devices are typically constrained in terms of computational power, battery lifetime, and communications (i.e., network bandwidth and mobility) [4], [5]. These weaknesses will affect the efficiency and effectiveness of the authentication prosses between the home agent, foreign agent, and mobile user. A secure and efficient key agreement scheme based on a smart card between the mobile user and a foreign agent was proposed to overcome the mobile device's limitations and security issues during roaming. The smart card is a subscriber identity module (SIM) that is directly integrated into the mobile device [6]; hence only the mobile user who possesses the smart card can pass the verification from the foreign agent and home agent. Smart card-based authentication is used because of its simplicity, portability, and cryptographic capabilities [2], [7].

The remainder of the paper is organized as follows. In Section 2, other researchers' works are first observed and analyzed before relating the findings to this research's scheme. Then, in Section 3, an overview of the mathematical concepts that are used to develop the key agreement scheme is explained. Section 4 presents the proposed scheme in detail. Next, Section 5 discusses the safety of the scheme. In addition, Section 6 shows the proposed scheme's performance and efficiency. Finally, conclusions regarding the findings are presented in Section 7.

2. Related Works

Over the past years, various researchers have proposed many smart card-based key agreement schemes for roaming services. Lamport [8] developed the first password authentication technique in 1981, which employed a safe hash function to generate one-time passwords for validating user identification. Furthermore, Aziz and Diffie [9] established a security-protecting authentication system for wireless networks using a random nonce and a user's certificate in 1994. Moreover, Park [10] introduced a certificate-based session key exchange mechanism for wireless mobile systems in 1997. Several years later, Zhu and Ma [11] introduced a novel authentication mechanism for wireless networks utilizing a smart card to improve security protocol. In their proposed scheme, mobile users are only required to conduct symmetric encryptions and decryptions, reducing the computational burden. However, it was pointed out by Lee *et al*. [12] that Zhu and Ma's scheme cannot accomplish full backward secrecy and mutual authentication, so they offered an upgrade to address the shortcomings of the scheme. Unfortunately, Lee *et al.*'s proposed authentication scheme was found by Xu *et al*. [13] to have several security flaws, namely non-anonymity, unequal key agreement, and the inapplicable security design. Therefore, a new authentication scheme for wireless networks that included anonymity was developed by Xu *et al.*

On the other hand, Karuppiah and Saravanan [14] devised an improved authentication scheme for roaming services by utilizing the one-way hash function, Diffie-Hellman problem, and discrete logarithm problem. This improved authentication scheme was developed in order to remedy the weaknesses the Rhee *et al*.'s scheme [15]. In 2017, Guo and Sun [16] developed a novel password-

p-ISSN 2798-253X
e-ISSN 2798-3153

based authentication scheme with a smart card. Their scheme only uses a hash function and exclusive-OR operations to encrypt and decrypt data exchanged between the mobile user, foreign agent, and home agent. Hence, they claim that their scheme is more efficient because of the absence of asymmetric and symmetric encryption/decryption while maintaining the scheme's security. Moreover, in 2018, Xu *et al*. [17] proposed a new efficient mutual authentication and key agreement scheme with smart card-based by implementing a low-cost cryptographic primitive, the Exclusive-OR operation. Furthermore, Pan *et al*. [18] proposed an enhanced secure smart card-based Password Authentication Scheme by implementing a biometric-based password authentication.

The authentication scheme in this paper is inspired by the authentication scheme developed by Guo and Sun [16]. Similar to the approaches by Guo and Sun, a low-cost cryptographic primitive, the exclusive-OR operation, and a one-way hash function was used to maintain the scheme's security. Moreover, the efficiency of Guo and Sun's scheme would be improved by reducing the number of operations and calculations involved without compromising the scheme's security.

3. The Proposed Method

This section will briefly introduce the cryptographic primitives (Exclusive-OR), and a function (hash function) used to develop the key agreement scheme. The Exclusive-OR operation is a tool to encrypt and decrypt every message transmitted between the mobile user, home agent, and foreign agent. Meanwhile, the one-way hash function is used for data integrity to ensure whether the message received is valid [19].

3.1. Exclusive-OR

Exclusive-OR (XOR) is a simple bitwise operation, denoted as $\oplus$ and operates on binary data. The idea behind this operator is that if two input bits are the same and XOR'ed, the output bit will be "0". However, if two input bits differ, the output bit will be "1". Furthermore, in cryptography, XOR operates on binary data such as one message bit and one key stream bit to generate one ciphertext bit [20]. Four important properties of the XOR operator are useful in cryptography. Given three inputs (in binary form), say A, B, and C. Then these following statements are true.

1) XOR operation is commutative;
   $A \oplus B = B \oplus A$

2) XOR operation is associative;
   $A \oplus (B \oplus C) = (A \oplus B) \oplus C$

3) There exists an identity element in XOR'ing which is "0".
   $A \oplus 0 = A$

4) There exists an inverse for an element that is itself.
   $A \oplus A = 0$

The XOR encryption and decryption processes are given as follows [17]:

- Encryption process: *plaintext* $\oplus$ *key* = *ciphertext*
- Decryption process: *ciphertext* $\oplus$ *key* = *plaintext*

3.2. Hash Function

Definition 1 (See [18]). *A hash function is a function* $h: x \rightarrow y$ *that maps binary strings of arbitrary to binary strings of some fixed length, called hash-values. Note that* x *is input in binary form, while* y *is an output in binary form.*

p-ISSN 2798-253X
e-ISSN 2798-3153

In order to be useful in cryptography, a hash function must be designed so that any two different inputs, say x_1 and x_2, cannot have the same hash value, say $h(x_1) = h(x_2)$. Furthermore, a hash function must be a one-way function meaning that it is easy to compute $h(x) = y$ for a given x, but difficult to compute $h^{-1}(y) = x$ for a given y [14].

4. Proposed Scheme

This section presents the key agreement scheme for wireless roaming service based on smart cards. The proposed scheme will consist of three phases, namely the registration phase, login and authentication phase, and update password phase. The entities involved in this authentication process are mobile users, home agents, and foreign agents. Firstly, a mobile user who intends to roam to the foreign network must register with the home agent. A set of secret parameters saved on a smart card will be provided to the mobile user by the home agent. Then, the mobile user can use the smart card to log in to the home agent with the assistance of the foreign agent. After verifying that the mobile user is permitted, the home agent creates a session key between the mobile user and the foreign agent. In the update password phase, mobile use can change their password freely. The notations that are used throughout this section are listed in Table 1.

Table 1. Notations

Notations	Descriptions
$A, B, C, D, E, F, G, H, I, J, K, L$	Parameter
AA	The home agent where the PM registered
AL	The foreign agent of a foreign network where the PM visits
ID_{AA}	The identity of the home agent
ID_{AL}	The identity of the foreign agent
ID_{PM}	The identity of the mobile user
$KP = [S, R, \dots]$	Smart card containing the parameter, say $S, R, \dots$
N_i	The i-th nonce (a number that can only be used once [21])
PW_{PM}	A password of mobile user
PM	A mobile user
KS	Session key
$h(\cdot)$	Hash function
$h_k\ (\cdot)$	Keyed hash function
$\oplus$	A XOR operation
$\Vert$	A concatenation operator
$\{\alpha, \beta, \dots\}$	A message that contains parameters say $\alpha, \beta, \dots$

4.1. Registration Phase

Before a mobile user visits a foreign network, they must register with their home agents via a secure channel. In this phase, only two entities are involved: the mobile user and the home agent. The overview of the whole process of this phase is depicted in Table 2. The details are described as follows:

Step 1 : $PM \rightarrow AA : \{ ID_{PM} ,\ A\}$

- PM will randomly pick a secrete number b
- Then he/she freely chooses his/her password PW_{PM}

- After that, PM will compute a parameter A such that $A = h(PW_{PM} \| b)$
- PM then sends A, and its ID_{PM} to AA

Step 2 : $AA \rightarrow PM$: $KP = [\ C, D, h(.), x\ ]$

- AA received A dan ID_{PM} from PM.
- AA randomly generates a number x and calculates the following parameters:

  $B = h(ID_{AA} \| h_k(x))$
  $C = h(A \parallel ID_{PM}) \oplus B$
  $D = h(B)$
- AA the stores $C, D, h(.), x$ into the smart card, KP, and send KP to PM

Step 3 : $KP = [\ C, D, h(.), x, b\ ]$

- PM received KP from AA
- PM stores b into KP

Table 2. Registration Phase

$\boldsymbol{PM}$		$\boldsymbol{AA}$
Choose a secrete number b and PW_{PM}, Calculate A: $A = h(PW_{PM} \| b)$ $\{A, ID_{PM}\}$ Step 1	$\longrightarrow$	
		Generates x, Calculate: $B = h(ID_{AA} \| h_k(x))$ $C = h(A \parallel ID_{PM}) \oplus B$ $D = h(B)$ Stores $C, D, h(.), x$ into KP KP=[$C, D, h(.), x$]
Stores b into KP $KP = [C, D, h(.), x, b]$ Step 3	$\xleftarrow{KP}$	Step 2

4.2. Login and Authentication Phase

When the mobile user visits a foreign network, they will undergo a login and authentication phase before they gain access to the services provided by their home network. In the login phase, PM inserts their smart card, KP into their mobile device. Then, PM enters their password and identity, which is PW_{PM} and ID_{PM}, respectively. To ensure the PM is the owner of the KP, the KP will perform an authentication procedure. If the PM is the valid owner of that KP, then only the AL can proceed to validate whether the PM is the registered user of the AA or not. In this phase, it is assumed that AL and AA already agreed with $h_k(ID_{AL} \parallel w)$ and w. Finally, if PM is verified to be the registered user under the AA, then AA will generate a session key, KS, to be used in the communication between PM dan AL. The detailed process of the login and authentication phase will be depicted in Table 3 and explained as follows:

Step 1 : Verify the owner of the KP

- PM inserts their ID_{PM} and PW_{PM}
- KP then calculate the following parameters:

  $A = h(PW_{PM} \| b)$
  $B = h(A \parallel ID_{PM}) \oplus C$
- KP checks $h(B) \stackrel{?}{=} D$

p-ISSN 2798-253X
e-ISSN 2798-3153

(If equal, then the PM is the real owner of KP, and vice versa)

Step 2 : $PM \rightarrow AL: \{E, F, x\}$
- PM generates a nonce, N_1.
- Then, PM computes E and F using the calculated value B as follows:
  $E = N_1 \oplus B$
  $F = h(E \parallel B)$
- PM sends E, F, x to AL. The value x is obtained from KP.

Step 3 : $AL \rightarrow AA: \{E, G, H, w, x\}$
- AL receives E, G, H, w, x from PM.
- AL also generates a random nonce, N_2.
- AL then computes G and H as follows:
  $G = N_2 \oplus h_k(ID_{AL} \parallel w)$
  $H = F \oplus h(G \parallel h_k(ID_{AL} \parallel w))$
- After that, AL sends E, G, H, w, x to AA.

Step 4 : AA checks the authenticity of the message E, G
- AA receives E, G, H, w, x from AL.
- AA uses the received E, G, x, w to calculate:
  $h(E \parallel h(ID_{AA} \parallel h_k(x))) \oplus h(G \parallel h_k(ID_{AL} \parallel w))$
- AA verifies whether E, G are valid messages sent by AL or not through the following comparison:
  $h\left(E \parallel h\left(ID_{AA} \parallel h_k(x)\right)\right) \oplus h\left(G \parallel h_k(ID_{AL} \parallel w)\right) \stackrel{?}{=} H$

Step 5 : The development of the session key, KS
- AA uses the received x, w, k to extract the nonces, N_1 and N_2 from E and G, respectively, by performing the following calculation:
  $N_1 = E \oplus h(ID_{AA} \parallel h_k(x))$
  $N_2 = G \oplus h_k(ID_{AL} \parallel w)$
- The session key KS is created by using the extracted nonces, N_1 and N_2 as follows:
  $KS = h(N_1 \oplus h_k(x) \parallel N_2)$
- This session key is stored inside the parameter I:
  $I = KS \oplus N_2$

Step 6 : $AA \rightarrow AL: \{I, J, K, L\}$
- AA also computes J, K, L:
  $J = h(I \parallel h_k(ID_{AL} \parallel w))$
  $K = N_1 \oplus N_2$
  $L = h(K \parallel N_2)$
- I, J, K, L are then sent to AL.

Step 7 : AL checks the validity of the parameters I, K, and derives the session key, KS, from I.
- AL receives I, J, K, L from AA.
- AL calculate the following value by using $h_k(ID_{AL} \parallel w)$:
  $h\left(I \parallel h_k(ID_{AL} \parallel w)\right)$
- Then, the validity of I will be verified by calculating the following equation:
  $h\left(I \parallel h_k(ID_{AL} \parallel w)\right) \stackrel{?}{=} J$

p-ISSN 2798-253X
e-ISSN 2798-3153

- If I is valid, then AL can extract the session key, KS, from I by using its N_2:
  $KS = I \oplus N_2$
- After that, AL uses its N_2 to calculate the following value:
  $h(K \parallel N_2)$
- Then, AL checks whether K is valid or not using L:
  $h(K \parallel N_2) \stackrel{?}{=} L$

Step 8 : $AL \rightarrow PM: \{M, N\}$

- If K is valid, then AL will extract N_1 from K by using its N_2:
  $N_1 = K \oplus N_2$.
- Then, AL sores the session key, KS, into the parameter M:
  $M = KS \oplus N_1$.
- AL also computes the parameter N
  $N = h(M \parallel N_1)$
- and send M, N to PM

Step 9 : PM gets the session key, KS

- PM receives M, N from AL
- PM then uses his/her N_1 to calculate:
  $h(M \parallel N_1)$
- PM determines whether M is valid or not sent from AL:
  $h(M \parallel N_1) \stackrel{?}{=} N$
- If M is valid, then PM uses his/her N_1 to extract the session key, KS from M:
  $KS = M \oplus N_1 = h(N_1 \oplus h_k(x) \parallel N_2)$

Hereafter, the session key, $KS = h(N_1 \oplus h_k(x) \parallel N_2)$ will be used by the mobile user PM and the foreign agent AL, to secure their communication.

Table 3. Login and Registration Phase

$\boldsymbol{PM}$	$\boldsymbol{AL}$	$\boldsymbol{AA}$
Enters ID_{PM} , PW_{PM} Calculates: $A = h(PW_{PM} \parallel b)$ $B = h(A \parallel ID_{PM}) \oplus C$ Checks: $h(B) \stackrel{?}{=} D$ Generates N_1 Computes: $E = N_1 \oplus B$ $F = h(E \parallel B)$ $\{E, F, x\}$		
Step 1 & 2	Generates N_2 Calculates: $G = N_2 \oplus h_k(ID_{AL} \parallel w)$ $H = F \oplus h(G \parallel h_k(ID_{AL} \parallel w))$ $\{E, G, H, w, x\}$	
	Step 3	Checks: $h\left(E \parallel h(ID_{AA} \parallel h_k(x))\right)$ $\oplus h(G \parallel h_k(ID_{AL} \parallel w)) \stackrel{?}{=} H$ Calculates: $N_1 = E \oplus h(ID_{AA} \parallel h_k(x))$ $N_2 = G \oplus h_k(ID_{AL} \parallel w)$ Generates session key:

p-ISSN 2798-253X
e-ISSN 2798-3153

$KS = h(N_1 \oplus h_k(x) \parallel N_2)$
Calculates:
$I = KS \oplus N_2$
$J = h(I \parallel h_k(ID_{AL} \parallel w))$
$K = N_1 \oplus N_2$
$L = h(K \parallel N_2)$
$\{I, J, K, L\}$

Steps 4, 5, & 6

Checks & derives session key:
$h\big(I \parallel h_k(ID_{AL} \parallel w)\big) \stackrel{?}{=} J$
$KS = I \oplus N_2$
$\quad = h(N_1 \oplus h_k(x) \parallel N_2)$
Checks:
$h(K \parallel N_2) \stackrel{?}{=} L$
Calculates:
$N_1 = K \oplus N_2$
$M = KS \oplus N_1$
$N = h(M \parallel N_1)$
$\{M, N\}$

Step 7 & 8

Checks:
$h(M \parallel N_1) \stackrel{?}{=} N$
Derives Session key:
$KS = M \oplus N_1$
$\quad = h(N_1 \oplus h_k(x) \parallel N_2)$

Step 9

4.3. Update Password Phase

In this phase, mobile user, PM can freely update or change their desired password, hence the authentication scheme is user-friendly. The mobile user inserts their smart card KP into their mobile device. After that, the mobile user enters their old password PW_{PM} as well as their identity ID_{PM}. Then, smart card KP determines whether the PM is a valid owner or not. Finally, the old C will be replaced with the new one i.e C'. The details is explained as follows and depicted in Table 4.

Step 1 : Checks whether PM is the valid owner of KP or not.

- PM enters their old password PW_{PM}, and ID_{PM}.
- KP calculates A by using b stored inside it:

  $A = h(PW_{PM} \parallel b)$

- Then, KP calculates B by using A and C stored inside it:

  $B = h(A \parallel ID_{PM}) \oplus C$

- KP determines whether B valid or not using the following equation:

  $h(B) \stackrel{?}{=} D$

- If the equation hold, then PM is the owner of KP.

Step 2 : Changing the old password to new password, PW'_{PM}

- PM can enter the new password, PW'_{PM}.
- KP calculates:

  $A' = h(PW'_{PM} \parallel b)$

- Then, KP computes the new C and stores it into the parameter C':

p-ISSN 2798-253X
e-ISSN 2798-3153

$$C' = h(A' \parallel ID_{PM}) \oplus h(A \parallel ID_{PM}) \oplus C$$

- KP deletes the old C and stores C'.
- Therefore, the smart card KP now has these parameters stored inside it; $C', D, h(.), x, b$

Table 4. Update Password Phase

$\boldsymbol{PM}$	$\boldsymbol{KP}$
Enters: PW_{PM} ID_{PM} Step 1	
	Computes: $A = h(PW_{PM} \parallel b)$ $B = h(A \parallel ID_{PM}) \oplus C$ Checks: $h(B) \stackrel{?}{=} D$ Step 1
Enters: PW'_{PM} Step 2	Calculates: $A' = h(PW'_{PM} \parallel b)$ Calculates: $C' = h(A' \parallel ID_{PM}) \oplus h(A \parallel ID_{PM}) \oplus C$ Stores C' into KP. $KP = [C', D, h(.), x, b]$ Step 2
$KP = [C', D, h(.), x, b]$ Step 2	

5. Security Analysis

Attack scenarios was employed to demonstrate that the proposed scheme was capable of withstanding possible threats. Assume that Eve, the attacker, can intercept and eavesdrop on the messages transmitted over public communication between the user, the foreign agent, and the home agent. The security assessments are shown in the sections to come.

5.1. Smart Card Loss Attack

Assume that Eve stole or found the lost smart card, and she has the ability to extract the secret parameters stored inside the smart card. Notice that the parameters that are stored in the smart card, KP, are $C, D, h(.), x, b$. Recall that the parameters C and D are:

$$A = h(PW_{PM} \| b)$$

$$B = h(ID_{AA} \| h_k(x))$$

$$C = h(A \parallel ID_{PM}) \oplus B$$

$$D = h(B)$$

There are three scenarios where Eve can utilize the parameters $C, D, h(.), x, b$ for her benefit:

1. Use $C, D, h(.)$ to bypass step 1 in the login and authentication phase. In step 1, KP needs to verify the smart card owner. Eve can be verified if the equation $h(B) = D$ hold. Thus, Eve must get the parameter B. Observe that Eve can extract B from C that is being stored inside KP. To decrypt C, Eve needs $h(A \parallel ID_{PM})$. However, Eve does not have any information about ID_{PM} and A because only the real owner of the KP knows the valid ID_{PM} and PW_{PM} to compute A. Therefore, Eve failed to pass through step 1 in the login and authentication phase. Hence, the login and authentication phase failed to proceed.

p-ISSN 2798-253X
e-ISSN 2798-3153

2. Assume that Eve uses $h(.)$ and b to change passwords in the update password phase. In this phase, KP will determine whether the equation $h(B) = D$ satisfied or not before Eve can proceed to change the old password. However, Eve does not have a valid B because she does not have ID_{PM} and PW_{PM}. Hence, Eve failed to change the actual user's password.
3. Assume that Eve tries to decrypt D to get B. Nevertheless, Eve cannot decrypt $D = h(B)$ because it is hard or almost impossible to decrypt a hash function (the often-used hash function in the real world is SHA-256). Eve may try to find B' such that $h(B') = D$, but she might not be able to find one because a hash function is a collision-free function. Also, if Eve tries to guess B where $B = h(ID_{AA} \| h_k(x))$ such that $h(B) = D$, she will fail since she does not have the secret key k (only known by AA).

Therefore, the proposed key agreement scheme can resist a smart card loss case.

5.2. Replay Attack

A replay attack occurs when Eve sends back stolen messages to the actual mobile user to get information about the session key. There are two scenarios that allow Eve to steal the transmitted messages between the mobile user, foreign agent, and home agent.

1. Assume that Eve stole $\{E, F, x\}$ in step 2, login and authentication phase. Eve sends $\{E, F, x\}$ back to the AA to get the session key used by the PM and AL. When the AA sends back $\{I, J, K, L\}$ to AL, and AL sends back $\{M, N\}$ to Eve, Eve will fail to decrypt M such that $M = KS \oplus N_1$ to get the session key KS. This is because Eve does not have N_1. If Eve wants the value of N_1, then she needs to decrypt E where $E = N_1 \oplus B$. However, Eve will fail again because she does not have B. Thus, Eve cannot generate a session key used by PM and AL.

2. Assume that Eve stole $\{E, G, H, w, x\}$ in step 3, login and authentication phase. Then, Eve sends back this message to AA. When AA sends back $\{I, J, K, L\}$ to Eve, Eve will fail to decrypt I where $I = KS \oplus N_2$ to get the session key KS because Eve does not have N_2. Moreover, Eve will fail to decrypt K where $K = N_1 \oplus N_2$ to get N_1 or N_2 since Eve does not have either one of them.

Therefore, based on the analysis above, the proposed key agreement scheme can resist a replay attack.

5.3. Man-in-the-Middle Attack

In a man-in-the-middle attack, Eve acts as a middleman between the mobile user PM and foreign agent AL, or between foreign agent AL and home agent AA. Eve steals and modifies the message transmitted between the entities. There are two situations where this attack can occur.

1. Assume that Eve acts as a middleman between PM and AL, and steals the messages $\{E, F, x\}$ where $E = N_1 \oplus B$, $F = h(E \parallel B)$ in step 2, login and authentication phase. Eve then modifies the message $\{E', F', x'\}$ and forwards it to AL. Note that F' here not $F' = h(E' \parallel B)$. This is because Eve does not have the valid parameter of B where $B = h(ID_{AA} \parallel h_k(x))$ such that Eve can generate $F' = h(E' \parallel B)$. After that, AL sends back the message $\{E', G, H', w, x'\}$ where $G = N_2 \oplus h_k(ID_{AL} \parallel w)$, $H' = F' \oplus h(G \parallel h_k(ID_{AL} \parallel w))$ to AA. However, as soon as the AA takes the parameter E', x', G alongside with $h_k(.)$, ID_{AA} and $h_k(ID_{AL} \parallel w)$ that stored in AA then computes $h(E' \parallel h(ID_{AA} \parallel h_k(x'))) \oplus h(G \parallel h_k(ID_{AL} \parallel w))$, AA will get this inequality; $h(E' \parallel h(ID_{AA} \parallel h_k(x'))) \oplus h(G \parallel h_k(ID_{AL} \parallel w)) \neq H'$. Note that H' here is $H' = F' \oplus h(G \parallel h_k(ID_{AL} \parallel w))$ and F' not equal to $h(E' \parallel h(ID_{AA} \parallel h_k(x'))$. This is because Eve does not have the secret key k that can allow her to alter F' into $F' = h(E' \parallel h(ID_{AA} \parallel h_k(x'))$. Thus, AA will immediately terminate this session.

2. Assume that Eve acts as a middleman between AL and AA and steals the message $\{E, G, H, w, x\}$ in step 3, login and authentication phase. Eve then modifies $\{E, G, H, w, x\}$ into $\{E', G', H', w', x'\}$ and forwards $\{E', G', H', w', x'\}$ to the AA. The AA takes E', G', w', x' and computes $h(E' \parallel$

$h(ID_{AA} \parallel h_k(x')))\oplus h(G' \parallel h_k(ID_{AL} \parallel w'))$. However, AA will find that the equation is not equal to H' because H' does not contain the valid $h_k(ID_{AA} \parallel h_k(x'))$ and $h_k(ID_{AL} \parallel w')$. This is because Eve does not have the secret key k to generate the correct $h_k(ID_{AA} \parallel h_k(x'))$ and $h_k(ID_{AL} \parallel w')$ which are necessary to modify E', G', and H'. Therefore, AA will immediately terminate this session.

Hence through the analysis above, the key agreement scheme secured against a Man-in-the-middle attack.

5.4. Impersonation Attack

There are three scenarios that can occur. Firstly, Eve might impersonate the mobile user PM. Secondly, Eve can impersonate the foreign agent AL. Thirdly, Eve can impersonate the home agent AA. The detail of each situation is as follows:

1. Assume that Eve impersonates the mobile user PM. Therefore, Eve needs a valid the PM's password PW_{PM} and his/her identity ID_{PM}. Moreover, Eve needs the PM's smart card KP to allow her to log in to AL. In addition, the parameters stored inside KP are required to allow Eve to pass through the authentication phase. With these limitations, Eve cannot successfully log in to AL because she does not have the correct PW_{PM} and ID_{PM}. Besides that, Eve does not have KP. If Eve steals the PM's smart card KP, Eve still not be able to pass through the authentication process because the scheme can resist smart card loss (see section 5.1)
2. Next, assume that Eve impersonates AL. However, every AL have its unique w. Also, AA computes $h_k(ID_{AL} \parallel w)$ by using its secrete key k distributes $h_k(ID_{AL} \parallel w)$ to each AL, specifically. This process is assumed to have occurred before the login and authentication phase. Therefore, if Eve wants to impersonate AL, Eve will receive $\{E, F, x\}$ from PM in step 2, login and authentication phase. Then, Eve will generate her nonce N_2' and w' to calculate $G' = N_2'\oplus h_k(ID_{AL} \parallel w')$ and $H' = F\oplus h(G \parallel h_k(ID_{AL} \parallel w'))$. However, when AA checks the equation $h(E' \parallel h(ID_{AA} \parallel h_k(x')))\oplus h(G' \parallel h_k(ID_{AL} \parallel w'))$, AA will detect that this equation is not equal to H'. This is because Eve does not have the secret key k to generate $h_k(ID_{AL} \parallel w')$.
3. Assume that Eve impersonates AA. Eve will receive $\{E, G, H, w, x\}$ from AL in step 3, login and authentication phase. However, Eve is not able to extract N_1 and N_2 from the parameter $E = N_1\oplus h(ID_{PM} \parallel h_k(x))$ and $G = N_2\oplus h_k(ID_{AL} \parallel w)$, respectively. This is because Eve does not have the secrete key k to compute $h(ID_{PM} \parallel h_k(x))$ and $h_k(ID_{AL} \parallel w)$. If Eve wants to send a fake $\{I', J', K', L'\}$ which initially are $I = KS\oplus N_2$, $J = h(I \parallel h_k(ID_{AL} \parallel w))$, $K = N_1\oplus N_2$, and $K = N_1\oplus N_2$ to AL, Then the equation $h\big(I \parallel h_k(ID_{AL} \parallel w)\big)$ no longer equal to J since J' does not contain the valid $h_k(ID_{AL} \parallel w)$. Thus, AL will immediately terminate this session, and the session key KS cannot be derived from I'.

Hence, the proposed key agreement scheme is secure against impersonation attacks.

5.5. Perfect Forward Secrecy

In the login and authentication phase, the generated session key $KS = h(N_1\oplus h_k(x) \parallel N_2)$ is contains with the nonces N_1 and N_2. In every new round, PM and AL will always change the nonces N_1 and N_2. Therefore, the session key $KS = h(N_1\oplus h_k(x) \parallel N_2)$ will also change depending on the new N_1 and N_2. Hence, even though Eve successfully obtained the session key $KS = h(N_1\oplus h_k(x) \parallel N_2)$ in one session, she only can use it in that session. Thus, Eve cannot decrypt the previous messages shared between PM and AL. In conclusion, the proposed key agreement scheme can resist various attacks from unauthorized parties.

6. Discussions

In this section, the performance and efficiency of the key agreement scheme are analyzed. The scheme was proven to satisfy the important requirements for a secure and efficient key agreement

p-ISSN 2798-253X
e-ISSN 2798-3153

scheme, namely mutual authentication, user-friendly, anonymity, and low computational cost. The proof for each requirement below is presented below.

6.1. Mutual Authentication

In the login and authentication phase, the mobile user PM first sends $\{E, F, x\}$ where $E = N_1 \oplus B$ and $F = h(E \parallel B)$ to the foreign agent AL whenever they want to communicate with the home agent AA. AL then receives the message $\{E, F, x\}$ from PM. After that, AL computes $G = N_2 \oplus h_k(ID_{AL} \parallel w)$ and uses E and F to calculate $H = F \oplus h(G \parallel h_k(ID_{AL} \parallel w))$. Note that the parameter H contains E, F, and G. Thus, if AA checks the validity of H, AA will also check the validity of E, F, G as well. Hence, AA can check that the PM is a valid user. Furthermore, AA sends $\{I, J, K, L\}$ to AL where $I = KS \oplus N_2$, $J = h(I \parallel h_k(ID_{AL} \parallel w))$, $K = N_1 \oplus N_2$ and $L = h(K \parallel N_2)$. Then, AL uses the received I and its $h_k(ID_{AL} \parallel w)$ to computes $h\big(I \parallel h_k(ID_{AL} \parallel w)\big)$ to verify J. Therefore, AL is able to make sure that the AA is a valid home agent. This is because if $h\big(I \parallel h_k(ID_{AL} \parallel w)\big) \neq J$, then AA is not an authorized home agent because only AA knows $h_k(ID_{AL} \parallel w)$ to calculate the correct J. Apart from that, AL also can verify L by determining whether $h(K \parallel N_2) = L$ or not. If the equality holds, then AL can proceed to decrypt K by using its N_2 to obtain N_1. In this situation, AL sure that N_1 is valid. Moreover, AL uses the N_1 to encrypt KS such that $M = KS \oplus N_1$. AL also calculates $N = h(M \parallel N_1)$ then sends $\{M, N\}$ to PM. PM will use his/her N_1 and the received M to compute and determine whether $h(M \parallel N_1) = N$. If it is equal, then PM is sure that AL is a valid foreign agent because only AL who knows the correct N_1 which is used to generate $N = h(M \parallel N_1)$. Therefore, PM can authenticate AA because the actual N_1 received by AL is from AA. Hence, through the scenarios above, PM, AL, and AA can authenticate each other.

6.2. User-Friendly

In this section, the performance and efficiency of the key agreement scheme is analyzed. It is proven that the scheme satisfied the important requirements for a secure and efficient key agreement scheme, namely mutual authentication, user-friendly, anonymity, and low computational cost. The proof for each requirement below is presented below.

6.3. Anonymity

The proposed key agreement scheme satisfied the anonymity property. Observe the message sent in step 2, the login and authentication phase. In step 2, the message sent is $\{E, F, x\}$ where $E = N_1 \oplus B = N_1 \oplus h\big(ID_{AA} \parallel h_k(x)\big)$ and $F = h(E \parallel B) = h(E \parallel h\big(ID_{AA} \parallel h_k(x)\big)$. It can be seen that no user's identity is involved in the message. Suppose an unauthorized party somehow obtained the smart card and is able to access all the parameters stored inside it. In that case, he/she cannot extract the user's identity stored in parameter C because he/she does not have the password PW_{PM}. In addition, C is encrypted by a secure hash function. Therefore, no user identity can be extracted or exposed to an unauthorized party; hence user anonymity is achieved.

6.4. Low Computational Cost

Computational cost is an important aspect in the development of a key agreement scheme. This is because mobile devices such as mobile phones, smart watches, smart cards, Ipad, etc., do not have the capability to handle complex and tedious calculations due to limited computational power. Besides that, a tedious and complex calculation requires a large battery capacity and can exhaust the mobile device's sensors. Therefore, a key agreement scheme based only on low-cost cryptographic primitive, namely XOR operations, keyed one-way hash function, and one-way hash function to reduce the computational tediousness and complexity is proposed. The number of operations involved in the scheme with the scheme proposed by Cheng Guo dan Chin-Yu Sun [16] are compared. The notations involved are listed in Table 5.

Table 5. Notations

Notations	Descriptions
H	Hash function
X	XOR operation
AA	Home agent
AL	Foreign agent
PM	Mobile user

The comparison of the number of operations involved in the proposed key agreement scheme with the scheme proposed by Cheng Guo dan Chin-Yu Sun is given in Table 6 below.

Table 6. Comparison of the Number of Operations

Operations	Entities	Our scheme	Cheng Guo & Chin-Yu Sun's scheme
H	PM	12	12
	AA	18	25
	AL	7	9
X	PM	6	18
	AA	7	13
	AL	5	7

Based on Table 6, the mobile user only needed to execute six XOR operations compared to 18 XOR operations in Cheng-Guo and Chin-Yu Sun's scheme. Moreover, the home and foreign agents are only required to perform fewer hash functions and XOR operations than Cheng-Guo and Chin-Yu Sun's scheme. Therefore, the decrement in the number of operations required to be done by each entity will reduce the tediousness and complexity of the calculations involved in the proposed scheme. This will save the mobile device's battery consumption, computational power, and sensor.

7. Conclusion

This work presents an improved key agreement scheme from the previous scheme [16] of wireless network authentication. Based on the results in Section 6, the proposed authentication scheme can withstand the most well-known attacks, such as replay attacks, man-in-the-middle attacks, and impersonation attacks, and achieve absolute forward secrecy simultaneously. Moreover, an attacker would still be unable to utilize the parameters stored in the smart card even though they gain access to the smart card because the proposed scheme is an anti-smart card loss attack. Furthermore, the scheme is easy to use, cryptographically secure, and has a minimal computational cost. In addition, neither asymmetric nor symmetric encryption or decryption methods are used. Instead, a low-cost cryptographic primitive is used. Therefore, the authentication scheme is more efficient as well as cryptographically secure.

Based on the results presented in Table 6, Section 6.4 shows that the scheme still requires the mobile user to compute the same number of the hash function as in the Cheng-Guo and Chin-Yu Sun's scheme. Hence, there is still improvement that can be made in the proposed scheme in further study.

References

[1] H. Arshad and A. Rasoolzadegan, "A Secure Authentication and Key Agreement Scheme for Roaming Service with User Anonymity," *International Journal of Communication Systems*, vol. 30, no.18, pp. 1–18, 2017, doi: https://doi.org/10.1002/dac.3361.

[2] A. Ostad-Sharif, A. Babamohammadi, D. Abbasinezhad-Mood, and M. Nikooghadam, "Efficient Privacy-Preserving Authentication Scheme for Roaming Consumer in Global Mobility Networks," *International Journal of Communication Systems*, vol. 32, no. 5, pp. 1–27, 2019, doi: https://doi.org/10.1002/dac.3904.

[3] B.A. Forouzan, *TCP/IP Protocol Suite*, 4th ed. NY, USA: McGraw-Hill Higher Education, 2010.

[4] Y.S. Patel, M. Reddy, and R. Misra, "Energy and Cost Trade-Off for Computational Tasks Offloading in Mobile Multi-Tenant Clouds," *Cluster Computing*, vol. 24, no. 3, pp. 1793–1824, 2021, doi: https://doi.org/10.1007/s10586-020-03226-8.

[5] S.U.R. Malik, H. Akram, S.S. Gill, H. Pervaiz, and H. Malik, "EFFORT: Energy Efficient Framework for Offload Communication in Mobile Cloud Computing," *Software: Practice and Experience*, vol. 51, no. 9, pp. 1896–1909, 2021, doi: https://doi.org/10.1002/spe.2850.

[6] L.D. Tsobdjou, S. Pierre, and A. Quintero, "A New Mutual Authentication and Key Agreement Protocol for Mobile Client - Server Environment," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1275–1286, 2021, doi: 10.1109/TNSM.2021.3071087.

[7] D. Wang, P. Wang, and J. Liu, "Improved Privacy-Preserving Authentication Scheme for Roaming Service in Mobile Networks," *IEEE Wireless Communications and Networking Conference*, 2016, pp. 3136–3141, doi: 10.1109/WCNC.2014.6953015.

[8] L. Lamport, "Password Authentication with Insecure Communication," *Communication of the ACM*, vol. 24, no. 11, 1981, pp. 770–772, doi: https://doi.org/10.1145/358790.358797.

[9] A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks," *IEEE Personal Communications*, vol. 1, no. 1, pp. 25–31, 1994, doi: 10.1109/98.295357.

[10] C.-S. Park, "On Certificate-Based Security Protocols for Wireless Mobile Communication Systems," *IEEE Network*, vol. 11, no. 5, pp. 50–55, 1997, doi: 10.1109/65.620522.

[11] J. Zhu and J. Ma, "A New Authentication Scheme with Anonymity for Wireless Environments," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 231–235, 2004, doi: 10.1109/TCE.2004.1277867.

[12] C.-C. Lee, M.-S. Hwang, and I.-E. Liao, "Security Enhancement on a New Authentication Scheme with Anonymity for Wireless Environments," IEEE Transactions on Industrial Electronics, vol. 53, no. 5, pp. 1683–1687, 2006, doi: 10.1109/TIE.2006.881998.

[13] J. Xu and D. Feng, "Security Flaws in Authentication Protocols with Anonymity for Wireless Environments," *ETRI Journal*, vol. 31, no. 4, pp. 460–462, 2009, doi: https://doi.org/10.4218/etrij.09.0209.0026

[14] M. Karuppiah and R. Saravanan, "A Secure Authentication Scheme with User Anonymity for Roaming Service in Global Mobility Networks," *Wireless Personal Communications*, vol. 84, no. 3, pp. 2055–2078, 2015, doi: https://doi.org/10.1007/s11277-015-2524-x.

[15] M. Kang, H.S. Rhee, and J.-Y. Choi, "Improved User Authentication Scheme with User Anonymity for Wireless Communications," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 94, no. 2, pp. 860–864, 2011, doi: https://doi.org/10.1587/transfun.E94.A.860

[16] C. Guo and C. Y. Sun, "Lightweight Authenticated Key Agreement Scheme with Smart Cards for Wireless Mobile Networks," *Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering*, 2017, pp. 961–967, doi: 10.18178/wcse.2017.06.167.

[17] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li, "A Novel Efficient MAKA Protocol with Desynchronization for Anonymous Roaming Service in Global Mobility Networks," *Journal of Network and Computer Applications*, vol. 107, pp. 83–92, 2018, doi: https://doi.org/10.1016/j.jnca.2018.02.003.

[18] H.-T. Pan, H.-W. Yang, and M.-S. Hwang, "An Enhanced Secure Smart Card-Based Password Authentication Scheme," *International Journal of Network Security*, vol. 22, no. 2, , pp. 358–363, 2020, doi: https://doi.org/10.1016/j.csi.2008.09.006.

[19] S. Dichenko and O. Finko, "Two-Dimensional Control and Assurance of Data Integrity in Information Systems Based on Residue Number System Codes and Cryptographic Hash Functions", 2018, *arXiv:1809.03251*.

[20] F. Huo and G. Gong, "XOR Encryption Versus Phase Encryption, an in-Depth Analysis," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 4, pp. 903–911, 2015, doi: 10.1109/TEMC.2015.2390229.

[21] T.C.M. Dönmez and E. Nigussie, "Security of LoRaWAN v1.1 in Backward Compatibility Scenarios," *Procedia Computer Science*, vol. 134, pp. 51–58, 2018, doi: https://doi.org/10.1016/j.procs.2018.07.143.