IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 29, 2017, accepted February 6, 2018, date of publication March 12, 2018, date of current version April 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2809614

Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks

JAEWON NOH, JEEHYEONG KIM, AND SUNGHYUN CHO, (Member, IEEE)
Department of Computer Science and Engineering, Hanyang University, Ansan, South Korea

Corresponding author: Sunghyun Cho (chopro@hanyang.ac.kr)

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning and the Ministry of Trade, Industry, and Energy South Korea under Grant 20161520302230.

ABSTRACT This paper proposes a secure key exchange scheme for Wi-Fi protected access II pre-shared key (WPA2-PSK)-based public Wi-Fi networks. The existing public Wi-Fi networks have several vulnerabilities, which are caused by eavesdropping stations in the same network. The main problem is that all stations in the same network have the same pre-shared key after the association. The attackers can derive an encryption key by eavesdropping on the four-way handshake procedure. Thus, we apply an elliptic curve public key cryptography concept to the proposed scheme to keep the key safe. In the proposed scheme, only an access point (AP) has its public key and private key pair. The proposed scheme solves the problem by exchanging a secondary key that each user determines or generated in the station during the authentication procedure. In the proposed scheme, the secondary key is encrypted by a station before it is transmitted to the AP. The AP can only decrypt the encrypted authentication message using its private key. By using the secondary key, each user can generate a unique pre-shared key and other following keys, which are derived from the four-way handshake procedure. Therefore, the exchange of the secondary key can defend against attacks from the malicious station in the same network. The safety of the proposed scheme is analyzed by several attack scenarios defined in this paper. Consequently, the proposed scheme provides more security level, 192 bits or 256 bits, compared with the conventional WPA2-PSK-based public Wi-Fi networks.

INDEX TERMS Authentication, elliptic curve cryptography, four-way handshake, security, Wi-Fi, WPA2-PSK.

I. INTRODUCTION

Most of Wi-Fi networks are used in public places or home networks. These Wi-Fi networks use various authentication methods and encryption algorithms. From these options, robustness of the networks is determined. There are two types of the networks in current Wi-Fi system depending on existence of an Authentication Server (AS). One method is called WPA2-PSK (Pre-Shared Key) and the other method is called WPA2-Enterprise. In the WPA2-Enterprise Wi-Fi networks, an AS authenticates users who access the network [1], [2]. On the other hand, an access point (AP) authenticates the users in the WPA2-PSK networks. Most public and small Wi-Fi networks have adopted the WPA2-PSK method. In case of public Wi-Fi networks, they usually reveal their passwords for access; hence, every user can access the network easily. One of the advantages of WPA2 is that it enhances the security level of the access password, called a passphrase, by supporting the use of a longer passphrase and a stronger algorithm compared with previous methods. However, most public Wi-Fi networks discard this advantage by revealing their passphrases. If a malicious station enters a Wi-Fi network, it can sniff all traffic of the other stations using several well-known traffic analysis tools. Furthermore, the malicious station has the same PSK when it exists in the same network. Then the malicious station can acquire other keys from the PSK by using more information about the target. This problem may lead to an invasion of privacy in public Wi-Fi networks. In other words, the existing WPA2-PSK can authenticate users from outside, but it cannot guarantee secure communication in the network. The problem is caused because all user derive their key using same PSK. Thus, we should solve this problem because it has not been completely resolved yet.

In this paper, we propose secure schemes to assure secure individual communications in the vulnerable public Wi-Fi networks. The proposed schemes adopt a public key cryptography in the existing Wi-Fi system. We use an elliptic curve cryptography (ECC) [3], [4] concept in the proposed scheme. Using the ECC concept, we assure that an additional unique key can be safely exchanged between each user and an AP. This additional key is used as a secret key after association. Consequently, each user can communicate securely by using a unique secret key even though all traffic is exposed to an attacker. Our contributions in this paper are as follows.

- The proposed scheme assures that each user exchange their authentication messages. It makes each user derive their unique key in the public Wi-Fi networks.
- We also consider attackers that exist in same network with a target. The proposed method can prevent several attacks such as man-in-the-middle, key recovery and de-authentication attacks from inside.

The rest of the paper is organized as follows. In Section II, we introduce related works about improving security, and discovering vulnerabilities from several attacks in the existing Wi-Fi networks. Section III presents the system models we investigate in this paper. In Section IV, the proposed Wi-Fi access authentication and key exchange schemes are described in detail. In Section V, we present the security and overhead analysis of the proposed scheme from several classical attacks, and finally concluding remarks are presented in Section VI.

II. RELATED WORKS

The Wi-Fi access authentication methods such as wired equivalent privacy (WEP), WPA and WPA2 were defined by IEEE 802.11 and IEEE 802.11i standards. Encryption algorithms such as rivest cipher 4 (RC4), the temporal key integrity protocol (TKIP), and advanced encryption standard counter mode CBC-MAC protocol (AES-CCMP) have been used for the authentication methods [2], [5], [6]. Despite these developments in the Wi-Fi systems, several vulnerabilities which are eavesdropping key exchange procedure and sending malicious messages still remain. Until now, two major types of studies have been conducted for more robust Wi-Fi networks. One includes secure methods to improve security in the existing Wi-Fi networks [7], [8]. The other considers vulnerabilities and attacks followed by the vulnerabilities in the existing Wi-Fi system [9]–[11]. The proposed scheme is related to the latter research. Before presenting the directly related researches, researches that describe possible attacks in the existing Wi-Fi networks are introduced [7], [8]. Agarwal et al. proposed an advanced man-in-the-middle (MITM) attack in WPA2-encrypted Wi-Fi networks in [7]. In this research, a more powerful MITM attack in which a user has trouble noticing the attack. Waliullah et al. studied security attacks in IEEE 802.11 WLAN [8]. They described several attacks that can be possible in the Wi-Fi networks: authentication attack, denial of service attack, man-in-the-middle attack, replay attack, MAC address spoofing and etc.

On the other hand, [9]–[11] are directly related to the proposed idea. Ghanem and Ratnayake proposed a re-authentication protocol to prevent de-authentication following a brute-force attack in a WPA2-PSK-based Wi-Fi system [9]. When a target station is in the Wi-Fi network, an attacker tries a de-authentication attack. Then the target station is disconnected in the network and performs reconnection. The attacker can obtain a pairwise transient key (PTK) by capturing the four-way handshake procedure. The author solved this problem by modifying the re-authentication procedures. The author added re-authentication key in four-way handshake procedure to check the time of the de-authentication. However, this proposed scheme could not solve the vulnerable key problems from MITM and key recovery attacks. In addition, Raju and Nair proposed an approach using a public key concept with a Diffie-Hellman key exchange algorithm for secure hotspot [10]. It used instantaneous session key (ISK) instead of the PSK. It focused on the same vulnerability that we consider in this paper. Although, secure hotspot protocol assured secure key exchange, it may be vulnerable from de-authentication attack. The public key cryptography can be a method to provide higher security than the symmetric key system. However, it requires more computation compared to the existing system. In the previous work, we proposed a key exchange scheme to solve the problems followed by traffic exposure. However, our previous work described only conceptual idea about the public key cryptography and several attack models [11].

In this paper, we consider public key cryptography. Thus, we also found the comparison studies about trade-off in the existing Wi-Fi system depending on public key algorithms. In [12], Sinha et al. performed a comparison study of RSA and ECC algorithms. Their results show that the ECC has less computational overhead than RSA. The ECC also requires much shorter key size, so generating the keys is faster. Through these characteristics, the ECC is efficient for small devices. Although much research has been performed as introduced above, security problems that are caused by MITM attack and key recovery attack in the same WPA2-PSK network have not been solved yet. Thus, in this paper, we performed this research to prevent possible attacks, and to mitigate communication interruption from the attacker.

III. SYSTEM MODEL

A system model of the proposed scheme is described in Fig. 1. In the system model, an AP, stations, and attackers exist in the same network. In the system, the proposed scheme provides secure communication between a station and an AP against an attacker. To use ECC in the proposed scheme, network entities should have an encoder/decoder to convert a point into data. The system model consists of three models: network model, communication model, and attack model. The network model contains the definition and characteristics of entities in the Wi-Fi networks. The communication model describes a communication scenario between the entities. The attack model defines an attacker, the purpose of the attack, and includes assumptions used for the proposed scheme. The proposed scheme cannot be applied directly to current

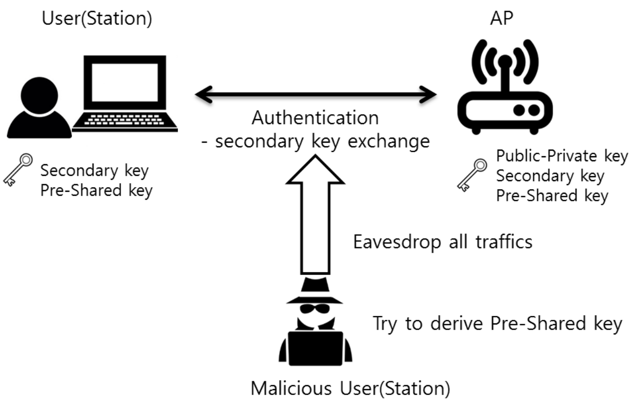


FIGURE 1. System Model in the proposed scheme.

WPA2-PSK based Wi-Fi system. In order to use the proposed scheme, the AP and the station can perform calculation for elliptic curve by installing some software. Also we assume that the proposed scheme utilize reserved fields in the probe response and authentication frame defined in the 802.11 standard without modification of the standard.

A. NETWORK MODEL

1) AP

An AP is connected to many stations in the network, and provides network services to the authenticated station. The AP uses a WPA2-PSK authentication method and AES encryption algorithm in the network. A passphrase for Wi-Fi access is exposed to the public. In the network, the AP should generate a public key and a private key using an elliptic curve. To generate these keys, the AP has to set some parameters, which are described in the following section. We assume that this key pair is hard to obtain from the outside by using a hardware security module (HSM) in the AP [13]. Before an authentication process, the AP transmits ECC parameters and its public key. When the AP authenticates a station, it obtains a secondary. Thus, the AP knows all secondary keys of all stations in its network. The AP also generates a distinct communication key based on the secondary key.

2) STATION

A station is a user device that can access Wi-Fi networks. The station already knows a passphrase for an authentication, because our target system is the public Wi-Fi network. The station has to obtain information about the ECC parameters and a public key of an AP before the authentication. Only the station can randomly generate its secondary key. When the station requests authentication to the AP, the station should encrypt the message with the public key. In the authentication request message, the secondary key is also included.

B. ATTACK AND SECURITY MODEL

All stations perform an access procedure using a passphrase. From this process, a station receives the required information for authentication. After the association, the station performs a four-way handshake procedure. The four-way handshake procedure lets both the station and the AP generate a PTK by exchanging two nonces. In this paper, we assume an attacker is in the same network as a target station as explained above. The attacker just has a malicious purpose compared with a normal station in the public Wi-Fi networks. Any user accessing the network or already existing in the network can be a target. The purpose of an attacker is to obtain a communication key or private information of the target station. The attacker is authenticated in the Wi-Fi network, and has basic information about the network. In our model, the attacker can perform classical attacks such as spoofing, key cracking, denial of service (DoS), etc. Therefore, keeping these data secure from the attacker is the most important issue in the public Wi-Fi networks.

IV. SECURE ACCESS AUTHENTICATION AND 4-WAY HANDSHAKE PROCEDURES

In this paper, we applied public key cryptography. By using elliptic curve cryptography, an AP and a station can exchange secondary key in addition to a passphrase securely. Thus, we define the proposed scheme to SAHS (Secure Authentication and Handshake Scheme). In the SAHS, an AP has a public key and a private key in a finite elliptic curve. As shown in the Fig. 1, users and an attacker exist in the same Wi-Fi network. The attacker attempts ARP spoofing and key recovery attacks. Our research is focused on the way to prevent these attacks from the malicious station. Stations perform authentication and association to be connected to the networks. Then the stations perform a four-way handshake procedure to generate communication key. In this section, we explain preliminary knowledge about ECC first, and describe our proposed scheme.

A. PRELIMINARY KNOWLEDGE FOR ECC

First, an AP generates a public key and a private key based on an elliptic curve. Table 1 shows notation and descriptions for elliptic curve and proposed idea. As described above, an RSA system can be considered in the proposed scheme. A public key and a private key that is generated by the RSA are exponent forms, and 7680-bit keys are used to satisfy 192 bits security level. Compared with RSA, ECC requires only 384 bits for 192 bits security level. In addition, to satisfy 256 bits security level, RSA and ECC have to use 15360-bit key and 512-bit key respectively. Hence, by applying the ECC in the proposed scheme, the proposed scheme mitigates computation costs instead of using RSA. The elliptic curve is defined by

$$y^2 = x^3 + ax + b \tag{1}$$

The ECC has domain parameters (p, a, b, G, n, h). Once the elliptic curve is defined, the AP sets p and determines the base point $G(x_g, y_g)$. A fundamental characteristic is

$$P_{AP} = n_{AP}G \tag{2}$$

It is called elliptic curve logarithm. [3], [4], [14]

In an elliptic curve, when a key n_{AP} and a base point G are given, calculating P_{AP} is easy problem. However, when a

TABLE 1. Notation and descriptions.

Notation	Description
p	k-bit prime number
Z_p	Integers modulo p
$E_p(a, b)$	Finite elliptic curve defined over Z_p
G	Base point in $E_p(a, b)$(Generator)
n_{AP}	Private key of an AP
P_{AP}	Public key of an AP,
$passphrase$	Password for accessing network
$\{*\}_{key}$	Encryption with key
M	Plain Message
$Point_M$	Encoded point on the $E_p(a, b)$ from M
C_M	Encrypted $Point_M$
D_{AA}	Delay from access authentication procedure
D_{Hand}	Delay from four-way handshake procedure
$D_{A_{enc}}$	Asymmetric encryption delay
$D_{A_{dec}}$	Asymmetric decryption delay
$D_{S_{enc}}$	Symmetric encryption delay
$D_{S_{dec}}$	Symmetric decryption delay
D_{gen}	Key generation delay
D_{total}	Total delay of the whole procedure

key P_{AP} and the G are given, deriving the n_{AP} is a difficult problem. There are many points in the elliptic curve field. Finding a point in reverse is a highly time-consuming task. This is one of the properties in the ECC, and it is called the elliptic curve logarithm. An AP reveals its public key P_{AP} to the public after the AP generates an appropriate P_{AP} and n_{AP} pair in the selected elliptic curve. In the ECC, basically an encoder and a decoder are needed to express a message to a point in the elliptic curve. Therefore, each entity has to encrypt and decrypt messages using the points as shown in the following [3], [14]:

$$Enc \rightarrow C_M : \{kG, Point_M + kP_{AP}\} \tag{3}$$

$$Dec \rightarrow Point_M + kP_{AP} - n_{AP}(kG) = Point_M \tag{4}$$

When a station wants to send a message M, the station first encodes the message to a $Point_m$ on the elliptic curve. Then the station generates a random value k, and calculates the $Point_M + kP_{AP}$. Therefore, an encrypted message C_M includes the $Point_M + kP_{AP}$ and the kG which is used to decrypt. When an AP receives the message C_M, the AP can decrypt by using the kG and its private key n_{AP}. The AP calculates a $n_{AP}(kG)$ to remove a kP_{AP} part. Consequently, only the AP can obtain the $Point_M$ using its private key. In this network, other stations cannot derive the original message M even if the stations were eavesdropping the communication. We use this public key cryptographic characteristic in the proposed scheme. Thus, the proposed scheme assures secure exchange between an AP and a station. The proposed access authentication and four-way handshake procedure are described in the following.

B. Wi-Fi ACCESS AUTHENTICATION PROCEDURE

The SAHS can be divided into two parts: probing and requesting authentication for the association and a four-way handshake after the association [15]. Fig. 2 shows the proposed authentication scheme using the public key cryptography before the association. This procedure includes from searching to association between an AP and a station. An access scenario basically consists of three parts that are probing, authentication, and association. Details of the proposed access authentication procedure are given in the following.

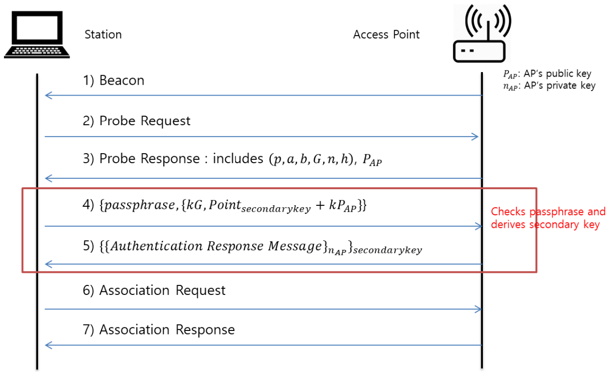

Station
Access Point
P_{AP}: AP's public key
n_{AP}: AP's private key
1) Beacon
2) Probe Request
3) Probe Response : includes (p, a, b, G, n, h), P_{AP}
4) $\{passphrase, \{kG, Point_{secondarykey} + kP_{AP}\}\}$
Checks passphrase and derives secondary key
5) $\{\{Authentication\ Response\ Message\}_{n_{AP}}\}_{secondarykey}$
6) Association Request
7) Association Response

FIGURE 2. Proposed access authentication procedure.

1) Beacon Message
A beacon message is sent by an AP. In the Wi-Fi network, the AP periodically broadcasts this message. The message includes fundamental information such as a timestamp, an interval, a service set identifier (SSID), etc. The information is regarding the corresponding Wi-Fi network. The AP can inform the existence of the network to all stations around the network.

2) Probe Request Message
A station sends a probe request message when it wants to probe the networks surrounding it. Depending on the values of several fields, two cases can exist. If the station just wants to know information about all networks, the specific values are not needed. However, if the station wants to find a specific network, an SSID, a basic service set identifier (BSSID) or a media access control (MAC) address would be included in the message. In the scheme proposed here, we assume the latter case. The station already knows an SSID of the public Wi-Fi network, and tries to access this network.

3) Probe Response Message
The probe response message also includes existing information in the 802.11 standard. However, to perform the proposed method, additional content has to be sent to the station. In the frame of this message, there are some optional fields such as vendor-specific fields. We assume the AP sends basic parameters (p, a, b, G, n, h) and its public key P_{AP}. After the station receives this message, the station can know about the elliptic curve, a used prime, a base point, a public key, etc. These values are used commonly in the network, so these values do not have to be kept secure.

4) Authentication Request Message
In the existing WPA2-PSK Wi-Fi networks, a station requests authentication by sending a passphrase to an AP. Moreover, in this paper, we propose to use an addi-

tional key. We define this additional key as a secondary key. The secondary key is determined by a user of the station. The secondary key should be exchanged between the station and the AP, and this exchange has to be kept safe from the other entities in the network. To assure this secure exchange, the public key P_{AP} is used in encryption. When a message is encrypted with the P_{AP}, this message is only decrypted by the AP using its private key. In this message, the station has to send a secondary key to the AP with encryption. Consequently, the passphrase and the encrypted secondary key are transferred to the AP. This message is described as $\{kG, Point_{secondarykey} + kP_{AP}\}$.

5) Authentication Response Message
Once the AP receives the request message 4, the AP checks whether the passphrase is correct. If the authentication is successful, then the AP decrypts the encrypted part using its private key as shown below. The AP can get $Point_{secondarykey}$ from the decryption, and decode the point to the real message as $Point_{secondarykey} + kP_{AP} - n_{AP}(kG) = Point_{secondarykey}$. The AP that has the secondary key sends an authentication response message with double encryption. The first encryption uses its private key n_{AP}. This makes the station verify that the AP sent the message. The other encryption uses the secondary key. This makes the station verify whether the secondary key was well delivered. Thus, the existing authentication response message is encrypted twice in the proposed scheme to mitigate some problems.

6) Association Message
After the authentication is completed successfully, an association process is performed. From the fourth and fifth message, a secondary is also delivered to the AP. Now, the station and the AP perform an association procedure for the station to obtain complete access authority. These messages are the same as the existing association messages. The request message includes detailed network information, and the response message includes the association identification that the AP assigns.

C. 4-WAY HANDSHAKE PROCEDURE

Four-way handshake is a procedure to generate communication keys. In the existing Wi-Fi systems, there is a key hierarchy as shown in Fig. 3 (see [1], [5], [9]). First, a passphrase, which is used for authentication, is a fundamental key in this hierarchy. Through the four-way handshake procedure, several keys are generated sequentially. Once a station completely accesses the Wi-Fi network, the station generates a PSK using password-based key derivation function 2 (PBKDF2). In this function, basic network information and a passphrase are input parameters. The key becomes a more complex key through this function compared with the passphrase. Then a PMK is generated from the PSK. However, our target system is a WPA2-PSK Wi-Fi network. Thus, PMK is same as PSK because there is no authentication server. Finally, a PTK is derived from the four-way handshake procedure by using a PMK, and two nonces which are exchanged in the procedure. The PTK is the communication encryption key, and it is composed of three parts. These are the key confirmation key (KCK), key encryption key, and temporal key (TK). Among these, a TK is actually used to encrypt the data.

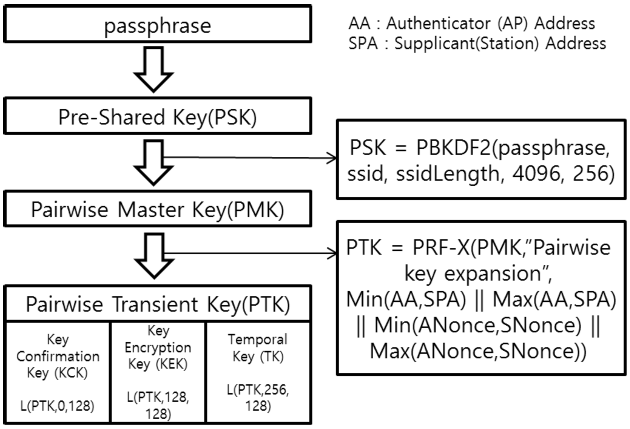

passphrase
AA : Authenticator (AP) Address
SPA : Supplicant(Station) Address
Pre-Shared Key(PSK)
PSK = PBKDF2(passphrase, ssid, ssidLength, 4096, 256)
Pairwise Master Key(PMK)
PTK = PRF-X(PMK,"Pairwise key expansion", Min(AA,SPA) || Max(AA,SPA) || Min(ANonce,SNonce) || Max(ANonce,SNonce))
Pairwise Transient Key(PTK)
Key Confirmation Key (KCK)
L(PTK,0,128)
Key Encryption Key (KEK)
L(PTK,128, 128)
Temporal Key (TK)
L(PTK,256, 128)

FIGURE 3. Existing WPA2-PSK key hierarchy.

In the existing WPA2-PSK network, all entities use the same passphrase. This causes all entities to generate the same PSK and PMK in the network. A PTK is the only unique key for each entity, because they exchange a self-generated nonce with the AP. However, this cannot guarantee that other stations do not know the nonces in the four-way handshake procedure. In fact, an attacker in the same network can eavesdrop on the process just using various sniffing tools. Despite this, an attacker who exists in the network can derive the PTK through several attacks. Thus, in this paper, our goal is that each station generates a secure unique PTK through the SAHS. Fig. 4 shows a modified four-way handshake procedure. As shown in the figure, the most important part is generating a PSK. This is the first step for security, and detailed steps are described below. In the four-way handshake, the extensible authentication protocol over local area networks (EAPOL) is used to deliver an EAP authentication message. The EAPOL has several types such as EAPOL-Packet, EAPOL-Start, EAPOL-Logoff, EAPOL-key, and etc. In the case of the four-way handshake, the EAPOL-key, which is a type of key exchange and negotiation, is used. When the access procedure is completed in the proposed scheme, a station and an AP generate a PSK using a secondary key, not a passphrase. The station and the AP start the four-way handshake procedure after they generate the PSK and the PMK. The proposed four-way handshake procedure is described in more detail in the following.

1) AP → Station (EAPOL-Key Message 1): First, the AP generates a random value defined as an AP nonce (ANonce). Then the AP sends this first message with encryption using the PMK. In the message, the notation P denotes one of key types of the EAPOL. Thus,

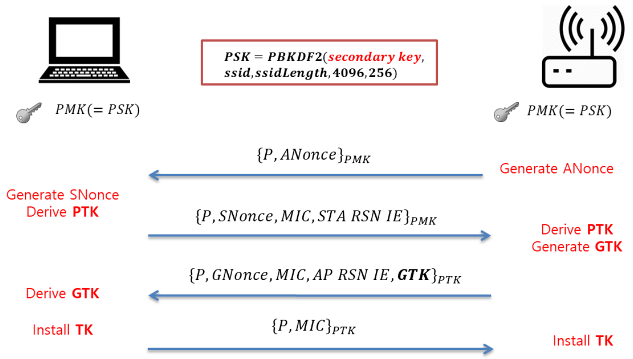


FIGURE 4. Proposed 4-way handshake procedure.

in this case, it shows that this message is for exchanging a one-to-one communication key. This message can also be exposed in the middle of the communication. However, the entities that do not know the PMK will find that it difficult to decrypt the message, because the PMK is followed by a secondary key of the receiver station.

2) Station → AP (EAPOL-Key message 2): Once the station receives EAPOL message 1, the station obtains the ANonce by decrypting the message with its own PMK. Then, the station also generates a random value defined as a station nonce (SNonce). The station derives the PTK using the PMK, the ANonce, and the SNonce. In message 2, the SNonce, message integrity check (MIC) and robust secure network information elements (RSN IE) are included. The MIC is used when the AP checks the integrity of this message. The RSN IE includes the cipher suite such as the authentication method, negotiation information related to the encryption algorithm, etc. Thus, it contains information about the security options that the station selected.
3) AP → Station (EAPOL-Key message 3): After the AP received message 2, it decrypts the message using the PMK first. Through the decryption, the AP can acquire the SNonce and the MIC. The AP checks message integrity using the received MIC. If the MIC is the correct value, the AP also derives the PTK using the same parameters. Now, the AP and the station have the same PTK, and the AP generates a group transient key (GTK) using a group nonce (GNonce). In the existing four-way handshake, the AP only encrypts the GTK field in this message. On the other hand, the AP encrypts the whole message including other parts with the PTK. This message includes the GNonce, MIC of this message, RSN IE of the AP, and the GTK.
4) Station → AP (EAPOL-Key message 4): In this step, the station can check whether both the station and the AP have the same PTK by decrypting the message 3. After the decryption, the station can verify the integrity of the message and obtain the GTK. When the station finishes this verification process, the station finally sends the fourth message. This message only includes a MIC. As described above, a four-way handshake procedure is performed. After the procedure, both the station and the AP install temporal keys for data encryption from the PTK. Consequently, in this paper, the proposed scheme makes each station exchange an additional key with the AP. The proposed scheme used ECC to prevent exposure of the secondary key. Through the proposed scheme also provides secure transmission of the EAPOL message in the four-way handshake.

TABLE 2. Notation and Descriptions for BAN Logic.

Notation	Description
$P \mid\equiv X$	P believes X
$P \triangleleft X$	P sees X, or P holds X
$P \mid\sim X$	P had sent X
$P \mid\Rightarrow X$	P completely controls over X
$P \overset{k}{\leftrightarrow} Q$	P and Q use k as a secret key
$P \mid\not\equiv X$	P cannot believe X
$\frac{Rule1}{Rule2}$	If rule1 is true, then rule2 is true

V. SECURITY AND OVERHEAD ANALYSIS

A. FORMAL VERIFICATION WITH BAN LOGIC

In order to check correctness of the SAHS, we use Burrows, Abadi, and Needham (BAN) logic [16], [17]. The BAN logic is usually used to analyze message exchange protocol such as authentication protocols. We verify correctness of the SAHS using several rules and notations defined in the logic. Also we show that attackers cannot get any critical information in the proposed scheme by adding an opposite notation to the believe notation. Table 2 describes the notations in the BAN logic.

1) IDEALIZATION

Firstly, we have to do idealization that is defined in [16]. Through this step, not important information like clear text which does not contribute to belief of receivers can be removed. Idealized procedure includes a sender, a receiver, and necessary information in a message. We choose three messages in access authentication procedure, and four messages in four-way handshake (see Fig. 3 and Fig. 4). Idealized form of the proposed scheme is described in below.

Idealized form of access authentication

I1. $AP \rightarrow STA_i$: $m_0 = \{(p, a, b, G, n, h), P_{AP}\}$
I2. $STA_i \rightarrow AP$: $m_1 = \{passphrase, E_{P_{AP}}(sk_i)\}$
I3. $AP \rightarrow STA_i$: $m_2 = \{E_{sk_i}(E_{n_{AP}}(response))\}$

Idealized form of four-way handshake

I1. $AP \rightarrow STA_i$: $m_3 = \{E_{PMK_{i-AP}}(ANonce)\}$
I2. $STA_i \rightarrow AP$:
$m_4 = \{E_{PMK_{i-AP}}(SNonce, MIC, RSNIE_{STA_i})\}$
I3. $AP \rightarrow STA_i$:
$m_5 = \{E_{PTK_{i-AP}}(GNonce, MIC, RSNIE_{AP_i}, GTK)\}$
I4. $STA_i \rightarrow AP$: $m_6 = \{E_{PTK_{i-AP}}(MIC)\}$

TABLE 3. Computation time for each operations.

Operations	Algorithm	Times(ms)
Symmetric Encryption(256 bits)	AES-CCMP	100
Symmetric Decryption(256 bits)	AES-CCMP	130
Asymmetric Encryption(384, 512 bits)	ECC	103, 201
Asymmetric Decryption(384, 512 bits)	ECC	140, 299
Key generation(384, 512 bits)		31, 66

2) ASSUMPTIONS

In this part, we define several assumptions for our target system by using symbols described in Table 3. We consider three entities such as a station, an attacker, and an AP. The attacker has one more assumption than the normal station because the attacker can eavesdrop messages between AP and a target station. There are our assumptions and description below.

Assumptions for station

A1. $STA_i \lhd RSNIE_{STA_i}$

A2. $STA_i \mid\equiv (AP, P_{AP}, passphrase)$

A3. $STA_i \mid\Rightarrow sk_i, SNonce$

A4. $STA_i \mid\equiv (SNonce)$

A5. $STA_i \mid\equiv STA_i \xleftrightarrow{PMK_{i-AP}} AP$, after access authentication

Assumptions for attacker

A6. $STA_j \lhd m_{k_{STA_i-TA}}$

Assumptions for AP

A7. $AP \mid\Rightarrow (p, a, b, G, n, h), passphrase, ANonce, GNonce, P_{AP}, n_{AP}$

A8. $AP \lhd P_{AP}, n_{AP}, RSNIE_{AP}$

A9. $AP \mid\equiv STA_i \xleftrightarrow{PMK_{i-AP}} AP$, after access authentication

3) GOALS

Followings are the required goals to assure secure authentication and key exchange.

Goals of access authentication

G1. $STA_i \mid\equiv STA_i \overset{sk_i}{\longleftrightarrow} AP$

G2. $AP \mid\equiv STA_i \overset{sk_i}{\longleftrightarrow} AP$

G3. $STA_j \mid\not\equiv STA_i \overset{sk_i}{\longleftrightarrow} AP$

Goals of four-way handshake

G4. $STA_i \mid\equiv STA_i \xleftrightarrow{PTK_{i-TA}} AP$

G5. $AP \mid\equiv STA_i \xleftrightarrow{PTK_{i-TA}} AP$

G6. $STA_j \mid\not\equiv STA_i \xleftrightarrow{PTK_{i-TA}} AP$

From the defined goals, a normal station STA_i wants to exchange secondary key sk_i to generate PMK_{i-AP}. Thus, to generate PMK_{i-AP} between STA_i and AP securely, G1 and G2 must be satisfied. Through the G1 and G2, we show the correctness of the proposed access authentication scheme. Furthermore, the other stations must not be able to get sk_i from the authentication of STA_i as shown in the G3. Thus, G3 can show safety from eavesdropping. In the same manner, a station and an AP want to install session key TK through the four-way handshake. G4 and G5 mean the station and the AP make common PTK_{i-TA} respectively. G6 means the other stations cannot get the PTK_{i-TA}.

4) VERIFICATION

Followings are goals that are required for secure system and verification processes.

Theorem 1: Station i and AP believe each other with the shared secondary key sk_i to verify G1 and G2.

$$V1: \frac{\dfrac{\dfrac{AP \lhd m_0}{AP \lhd (passphrase, sk_i), AP \mid\equiv STA_i \mid\sim \#(sk_i)}}{AP \mid\equiv STA_i \mid\sim sk_i}}{\dfrac{\dfrac{STA_i \lhd m_1}{STA_i \lhd P_{AP}, STA_i \mid\Rightarrow sk_i}}{STA_i \mid\equiv STA_i \overset{sk_i}{\longleftrightarrow} AP}}$$

$$V2: \frac{\dfrac{\dfrac{AP \lhd m_0}{AP \lhd (passphrase, sk_i), AP \mid\equiv STA_i \mid\sim \#(sk_i)}}{AP \mid\equiv STA_i \mid\sim sk_i}}{\dfrac{TA \mid\equiv STA_i \lhd P_{AP}, STA_i \mid\Rightarrow sk_i}{AP \mid\equiv STA_i \overset{sk_i}{\longleftrightarrow} AP}}$$

Theorem 2: Attacker j cannot believe the secondary key between one station and AP to verify G3.

Assume that the attacker can get the secondary key between one station and AP from eavesdropping. Verification process can be conducted like V3. However, there are contradictions from the A7 and A8.

$$V3: \frac{STA_j \lhd m_0}{\dfrac{STA_j \lhd n_{AP}}{\dfrac{STA_j \mid\equiv STA_i \mid\sim \#(sk_i)}{STA_j \mid\equiv STA_i \overset{sk_i}{\longleftrightarrow} AP}}}$$

The assumption in this verification is contradicted with pre-defined assumptions. The attacker cannot get the secondary key from the access authentication process without a private key of the AP. Thus, we can say the theorem 2 is true.

Theorem 3: Station i and AP believe each other with the PTK to verify G4 and G5.

$$V4: \frac{\dfrac{\dfrac{STA_i \lhd m_2}{STA_i \lhd PMK_{i-AP}, STA_i \mid\equiv AP \mid\sim \#(ANonce)}}{STA_i \mid\equiv AP \mid\equiv ANonce}}{\dfrac{STA_i \lhd m_4}{\dfrac{STA_i \lhd PTK_{i-AP}}{\dfrac{STA_i \lhd PTK_{i-AP}, STA_i \mid\equiv AP \mid\sim GTK}{STA_i \mid\equiv STA_i \xleftrightarrow{PTK_{i-TA}} AP}}}}$$

As same with the theorem 1, A5 assures G4 and G5 after the access authentication. V4 shows that G4 is satisfied. Verifying G5 has similar verification process, so we skip the process.

Theorem 4: Attacker j cannot believe the temporal key PTK between one station and AP to verify G6.

Assume that the attacker can get the PTK between one station and AP by eavesdropping ANonce and SNonce. Similarly, V5 describes verification process. However, there are also sevreal contradictions from the assumption such as A5 and A9.

V5 :

$$\begin{array}{c} STA_j \triangleleft m_2, m_3 \\ \hline STA_j \triangleleft PMK_{i-AP} \\ \hline STA_j \mid\equiv AP \mid\sim \#(ANonce), STA_j \mid\equiv STA_i \mid \#(SNonce) \\ \hline STA_j \triangleleft m_4 \\ \hline STA_j \triangleleft PTK_{i-AP}, STA_j \mid\equiv AP \mid\sim GTK \\ \hline STA_j \mid\equiv STA_i \xleftrightarrow{PTK_{i-TA}} AP \end{array}$$

B. SECURITY ANALYSIS IN CLASSICAL ATTACKS

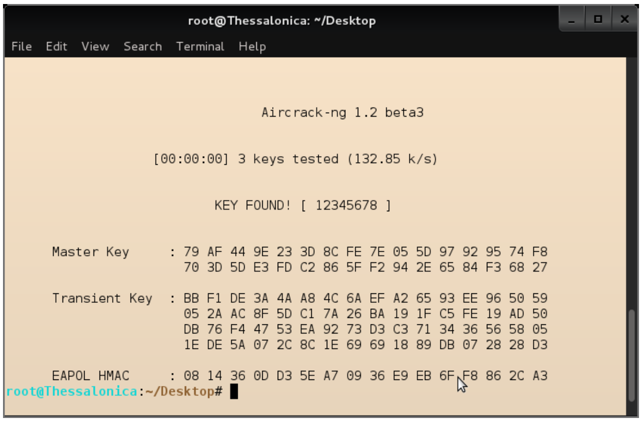
There have been various wireless treats about the IEEE 802.11i and have been analyzed these security issues years ago [14]. In this paper, we choose three classical attacks in WPA2-PSK Wi-Fi networks. The MITM attack, key recovery attack, and de-authentication are well-known attacks in the Wi-Fi networks. Some goals among the attacks seem to be similar, but there are some differences in the approaches. Thus, in the following, we describe each attack and the security of the proposed scheme.

1) MAN-IN-THE-MIDDLE ATTACK

A MITM attack is a common attack method in many other networks. In the Wi-Fi networks, ARP spoofing should be preceded for the MITM attack. An attacker intentionally sends messages using address information. Thus, the receivers send messages to the attacker. Through this attack, the attacker is logically located between the AP and the station. The attacker can eavesdrop on all traffic from the target station or from the AP. Furthermore, the attacker tries to obtain a communication key PTK from the traffic. The communication key is generated by the four-way handshake procedure. Therefore, the attacker makes the target station perform the four-way handshake again. If the target station loses the connection for a short time, the target automatically gets reconnected to the network. Then, the attacker can analyze the message completely. When an attacker obtains parameters such as the ANonce and the SNonce, the attacker can derive the PTK. From the verification, we show that other stations cannot get any information through eavesdropping. The proposed scheme lets each station exchange a sk_i by using asymmetric encryption. In the four-way handshake procedure, the unique PSK makes it difficult for the attacker to know message contents. In short, the proposed scheme mitigates exposure of information from the MITM attack, and prevents additional attacks followed by the MITM.

2) KEY RECOVERY ATTACK

Key recovery attack is caused by eavesdropping traffics. If an attacker acquires several information from the traffics, the attacker can get TK. Fig. 5 shows one of example results of the key recovery attack in the existing WPA2-PSK-based Wi-Fi network. Following is an attack scenario. An attacker based on Kali Linux OS tries to eavesdrop on the network using airodump-ng tool that can capture packets in a wireless network. The attacker waits until the target accesses this Wi-Fi network. When a target connects to the network, the attacker can obtain a pcap file that is a record file including four-way handshake information and traffics between the target and the AP. By using the Aircrack-ng tool, the attacker can obtain keys such as the master key (PMK), transient key (PTK), and EAPOL HMAC (MIC) between the AP and the target as shown in Fig. 5 (see [9]. However, the proposed scheme meets G6 defined in above. The G3 and G6 are goals to verify that attacks through eavesdropping are prevented. The proposed access authentication assures each station generates an unique PMK. Consequently, the attacker cannot get any information from the four-way handshake procedure without the PMK.



```
                         Aircrack-ng 1.2 beta3


               [00:00:00] 3 keys tested (132.85 k/s)


                     KEY FOUND! [ 12345678 ]


    Master Key     : 79 AF 44 9E 23 3D 8C FE 7E 05 5D 97 92 95 74 F8
                     70 3D 5D E3 FD C2 86 5F F2 94 2E 65 84 F3 68 27

    Transient Key  : BB F1 DE 3A 4A A8 4C 6A EF A2 65 93 EE 96 50 59
                     05 2A AC 8F 5D C1 7A 26 BA 19 1F C5 FE 19 AD 50
                     DB 76 F4 47 53 EA 92 73 D3 C3 71 34 36 56 58 05
                     1E DE 5A 07 2C 8C 1E 69 69 18 89 DB 07 28 28 D3

    EAPOL HMAC     : 08 14 36 0D D3 5E A7 09 36 E9 EB 6F F8 86 2C A3
root@Thessalonica:~/Desktop# 
```

FIGURE 5. Key recovery attack.

3) DE-AUTHENTICATION ATTACK

De-authentication attack is one of the DoS attacks. Once an attacker knows a MAC address of a target station, a de-authentication attack is possible [10], [17]. The de-authentication attack is performed to interrupt communication of the target station, and also to make the target station reconnect to the network. In the former case, it causes high delay in transmission or disconnection in the network. In the latter case, it can be used for a prior step to perform a key recovery attack. In the existing networks, it is possible to derive a PTK by eavesdropping on a four-way handshake procedure. After the de-authentication attack, the target station loses its connection and reconnects to the network.

It is hard to prevent DoS attacks, but the proposed scheme contributes to defending against the following attack for cracking the communication key. As explained above, the AP and the target station exchanged the secondary key that the attacker cannot know and made the unique PSK. Thus, both have maintained confidentiality of their keys. To provide higher security from DoS attacks that have the aim of communication interruption, further studies are needed. In the case of a de-authentication attack, several threats may be mitigated by applying encryption in the de-authentication frame. Many DoS attacks can occur in the Wi-Fi system, but our goal is to provide higher key security against the attacker. Thus, several vulnerabilities described in this paper still remain for future work.

TABLE 4. Delay comparison with the existing scheme.

	The WPA2-PSK scheme	The proposed scheme
Access authentication	$D_{AA} =$ No computation delay	$D_{AA} = D_{gen}$ $+3(D_{A_{enc}} + D_{A_{dec}})$ 760, 1566 (ms)
Four-way handshake	$D_{Hand} =$ $4(D_{S_{enc}} + D_{S_{dec}})$ 920 (ms)	$D_{Hand} =$ $4(D_{S_{enc}} + D_{S_{dec}})$ 920 (ms)
Total	920 (ms)	1680, 2486 (ms)

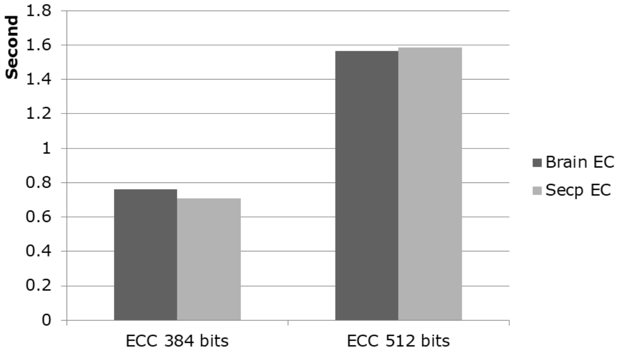


FIGURE 6. Required additional access authentication delay depending on key size and curves.

C. OVERHEADS ANALYSIS

To satisfy the high security level, at least 384-bit keys should be used in ECC [12]. When the proposed scheme is applied to the existing Wi-Fi system, the system may require more computation time and data transmission. M. Arif et al. implemented ECC algorithm and described times for each operation [18]. Also, in the [19], there is simulation result for AES encryption and decryption. Thus, we use the results of the [18], [19] to show overhead more quantitatively. Table 3 describes computation time for each operation, and table 4 shows delay comparison with the existing WPA2-PSK system. In the access authentication procedure, signification and verification using ECC are added compared with the existing system. However, there is no additional overhead in the four-way handshake. The difference is only the key value used for message encryption. As shown in the table 4, we define total delay(D_{total}) that caused by access authentication(D_{AA}), and handshake procedure(D_{Hand}). When the total delay of the existing system is $D_{AA} + D_{Hand}$, the total delay of the proposed scheme requires $D_{gen} + 3(D_{A_{enc}} + D_{A_{dec}})$ additionally(see Fig. 3 and Fig. 4). Fig. 6 shows the total delays for calculating communication key, and it depends on key size and type of elliptic curve. The figure shows the proposed scheme spends 0.76s and 1.56s more (384, 512 bits key respectively). The results show there are a few computational overheads compare with the existing scheme. However, these procedures are performed only once at initial stage. When the station starts data communication after the procedures, encryption delay would be same with the existing scheme. Consequently, the proposed scheme can improve the existing public Wi-Fi system with a few overheads.

VI. CONCLUSION

In this paper, we have proposed secure access authentication and four-way handshake procedures for key agreement by applying the elliptic-curve-based public key cryptography. The proposed scheme can improve the security level of WPA2-PSK-based public Wi-Fi networks compared with existing networks. The existing Wi-Fi systems have vulnerabilities especially from the classical attacks described above. These problems have been solved completely. In the proposed scheme, a station and an AP exchange the messages with encryption using a public key of the AP. From this approach, the station and the AP can exchange a secondary key. Through this secondary key, each station generates a different PSK and a PMK. This can make the four-way handshake procedure safe, and assures that each station generates a unique PTK. Consequently, the public Wi-Fi systems that adopt the proposed scheme assure individual secure communication in the network.

REFERENCES

[1] A. Ghilen, M. Azizi, and R. Bouallegue, "Integration of a quantum protocol for mutual authentication and secret key distribution within 802.11i standard," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. (AICCSA)*, Marrakech, Morocco, Nov. 2015, pp. 1–7.

[2] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*, IEEE Standard 802.11i-2004, 2004.

[3] M. S. Anoop. *Elliptic Curve Cryptography*. Accessed: Feb. 13, 2017. [Online]. Available: http://www.infosecwriters.com/text_resources/pdf/Elliptic_Curve_AnnopMS.pdf

[4] V. Kapoor, V. S. Abraham, and R. Singh, "Elliptic curve cryptography," *ACM Ubiquity*, vol. 9, no. 7, pp. 1–8, May 2008.

[5] *IEEE Standard for Information technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2012, 2012.

[6] A. H. Adnan *et al.*, "A comparative study of WLAN security protocols: WPA, WPA2," in *Proc. Int. Conf. Adv. Elect. Eng. (ICAEE)*, Dhaka, Bangladesh, Dec. 2015, pp. 165–169.

[7] M. Agarwal, S. Biswas, and S. Nandi, "Advanced stealth man-in-the-middle attack in WPA2 encrypted Wi-Fi networks," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 581–584, Apr. 2015.

[8] M. Waliullah, A. B. M. Moniruzzaman, and M. S. Rahman, "An experimental study analysis of security attacks at IEEE 802.11 wireless local area network," *Int. J. Future Generat. Commun. Netw.*, vol. 8, no. 1, pp. 9–18, 2015.

[9] M. C. Ghanem and D. N. Ratnayake, "Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack a novel re-authentication protocol," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, London, U.K., 2016, pp. 1–7.

[10] L. K. Raju and R. Nair, "Secure Hotspot a novel approach to secure public Wi-Fi hotspot," in *Proc. Int. Conf. Control Commun. Comput. India (ICCC)*, Trivandrum, India, Nov. 2015, pp. 642–646.

[11] J. Noh, J. Kim, G. Kwon, and S. Cho, "Secure key exchange scheme for WPA/WPA2-PSK using public key cryptography," in *Proc. IEEE Int. Conf. Consum. Electron.-Asia (ICCE)*, Seoul, South Korea, Oct. 2016, pp. 1–4.

[12] R. Sinha, H. K. Srivastava, and S. Gupta, "Performance based comparison study of RSA and elliptic curve cryptography," *Int. J. Sci. Eng. Res.*, vol. 4, no. 5, pp. 720–725, May 2013.

[13] L. Sustek, "Hardware security module," in *Encyclopedia of Cryptography and Security*. Springer-Verlag, 2011, pp. 535–538.

[14] B. Padma, D. Chandravathi, and R. P. Prapoorna, "Encoding and decoding of a message in the implementation of Elliptic Curve cryptography using Koblitz's method," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 5, pp. 1904–1907, Aug. 2010.

[15] J. C. Mitchell and C. He, "Security analysis and improvements for IEEE 802.11i," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, 2005, pp. 90–110.

[16] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[17] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[18] M. Arif, A. Habib, I. Rufat, and S. Azer, "Study and implementation of elliptic curve encryption algorithm for azerbaijan E-ID card," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 5, pp. 3708–3713, May 2015.

[19] C. Sivakumar and A. Velmurugan, "High speed VLSI design CCMP AES cipher for WLAN (IEEE 802.11i)," in *Proc. Int. Conf. Signal Process., Commun. Netw. (ICSCN)*, Chennai, India, 2007, pp. 398–403.

JAEWON NOH received the B.E. degree in computer science and engineering from Hanyang University, South Korea, in 2015, where he is currently pursuing the M.S./Ph.D. degree in computer science and engineering. His research interests include security for wireless communication, wireless communication, and vehicular communication systems.

JEEHYEONG KIM received the B.E. degree in computer science and engineering from Hanyang University, South Korea, in 2015, where he is currently pursuing the M.S./Ph.D. degree. His research interests include interference management for cellular communications, military communications using satellites, IoT security, and applied deep learning to wireless communications.

SUNGHYUN CHO received the B.S., M.S., and Ph.D. degrees in computer science and engineering from Hanyang University, South Korea, in 1995, 1997, and 2001, respectively. From 2001 to 2006, he was with the Telecommunication Research and Development Center, Samsung Advanced Institute of Technology, Samsung Electronics, where he has been engaged in the design and standardization of MAC and network layers of WiBro/WiMAX and 4G-LTE systems. From 2006 to 2008, he was a Post-Doctoral Visiting Scholar with the Department of Electrical Engineering, Stanford University. He is currently a Professor with the Department of Computer Science and Engineering, Hanyang University. His primary research interests are 5G mobile communications, software defined networks, and vehicular communication systems. He is a member of the board of directors of the Institute of Electronics and Information Engineers and the Korean Institute of Communication Sciences.