BIOSCIENCES BIOTECHNOLOGY RESEARCH ASIA, August 2014. Vol. **11**(2), 649-656

Providing A Forward Secure Authentication and Key Agreement Protocol for UMTS

Emad Aminmoghaddam*

Department of Mathematics and Cryptography, Imam Hossein University, Tehran, Iran.

doi: http://dx.doi.org/10.13005/bbra/1318

(Received: 10 June 2014; accepted: 19 July 2014)

Access to the wireless and radio connections is different from wired networks regarding to the vulnerability of wireless networks. Universal Mobile Telecommunication System (UMTS) as one of the third-generation cellular telecommunication systems is capable of adjustment to the Global system for Mobile Communications (GSM) and has resolved some of its drawbacks too. Furthermore, UMTS has provided an authentication and key agreement protocol (AKA) namely UMTS AKA that has some disadvantages like as bandwidth usage, huge memory to store data, lack of User Identification security, and synchronization problem. In this paper we investigate an authentication and key agreement protocol named IAP AKA that has resolved a number of problems associated with the security shortcomings of the UMTS AKA protocol. Then, we will represent a new protocol that has applied new procedures for the secrecy of User Identification by preventing general access to user identity. In addition, Elliptic Curve Cryptography is used to strength our protocol security. Finally, the most interesting property of our proposed protocol is Forward Secrecy which is necessary for user conversations confidentiality.

Key words: Wireless Networks, Cellular Telecommunication System, Authentication and Key Agreement Protocol, User Identity confidentiality, Forward Secrecy.

Wireless and mobile telecommunication systems especially, Universal Mobile Telecommunication System (UMTS) have been dramatically increased during recent years. UMTS is one of the third-generation mobile telecommunication standards which is currently entered to the global markets and uses the Global system for Mobile Communications (GSM) framework that has many disadvantages (Harn & Lin, 1995; Lee, Hwang, & Yang, 1999). It uses the UMTS AKA protocol for the authentication of mobile stations (MS) (Niemi & Nyberg, 2003) that is utilized to eliminate the GSM security problems and confront the recognized attacks.

* To whom all correspondence should be addressed.
Tel.: +(98)-912-8065796;
E-mail: emadam@gmail.com

UMTS Network Security Architecture

The cellular third-generation telecommunication network UMTS has different parts (Third Generation Partnership Project & Technical Specification Group SA, 2002) that the network components recognizing will help us to plan a security configuration. With regard to the proposed standard characteristics by ETSI (European Telecommunication Standard Institute) about the third-generation security (Third Generation Partnership Project & Technical Specification Group SA;3G Security, 2001), the security architecture is formed with a set of features and security mechanisms. The security feature is a part of service capabilities that states one or

more security needs. The security mechanism is a process to use a security feature. Figure 1 shows the placement of security features in five sets each of them is faced specific threats and used for specific security purposes. In this figure, mobile equipment (ME) is a cell phone that along with User Services Identity Module (USIM) provides an access to a third-generation cellular telecommunication network. Access network (AN),. Now, we explain five groups of security structure available in the UMTS architecture (Figure 1).

1. Network Access Security (1): To provide the secure access to the third-generation services (3G) and to prevent the attack to the radio interface link.
2. Network Domain Security (2): To allow the nods of network operator, to exchange the signaling information securely and to prevent the attack to the wired network.
3. User Domain Security (3): To secure accessing to the mobile stations
4. Application Domain Security (4): Application programs available at the user domain that enables a server to exchange information securely.
5. Visibility and Configurability of Security (5): To inform the user of the current active or inactive security features or enables the user to determine that a service is dependent on which security feature.

The security feature of the network accessing is divided to several subgroups that are authentication, secrecy and integrity of the information, authentication and key agreement protocol, a security mechanism for performing the kind of the features set which are responsible for the service of authentication and key agreement. These features are:

1) User Authentication: this feature means that the serving network (SN) endorses the user identification.
2) Network Authentication: this feature means the user confirms the serving network is authorized to provide services instead of the home network of the user and guarantees the currency of the authentication too.
3) Encryption key agreement: this characteristic means that MS and SN are capable of making an agreement on the Cipher Key (CK) will be used later.
4) Integrity key agreement: this characteristic means that MS and SN are capable of making an agreement on the Integrity Key (IK) will be used later.

Table 1. The comparison of the key agreement protocols in UMTS network

Characteristics/Protocol	UMTS AKA	IAP-AKA	Proposed protocol
Using Authentication Vectors	√	×	×
The synchronization between MS and HN	√	√	√
Bandwidth consumption	√	×	×
Data storage in SN	√	×	×
Mutual authentication between MS and HN	×	√	√
Mutual authentication between MS and SN	√	√	√
Disclosure effect of the short-term keys	√	×	√
Forward secrecy	×	×	√
False SN attack resistance	×	√	√
Confidentiality of the user ID	×	√	√

IAP AKA protocol

Analysis of the proposed protocol by ETSI (Niemi & Nyberg, 2003), UMTS AKA, highlighted the shortcomings. Therefore, some other protocols were proposed to remove disadvantages like AP AKA protocol (Adaptive authentication and key agreement Protocol) (Zhang & Fang, 2005) and E-UMTSAKA protocol (Extension of UMTS AKA) (J.AL-Saraireh & S.Yousef, 2006). But those protocols had some other weak points. In this regard, Shalmany and Rahbar (Shalmany & Rahbar, 2008) proposed a protocol (IAP AKA (Improved AP-AKA)) that was a combination of the mentioned protocols.

Before performing the protocol, every MS user shares one secret key and specific encryption algorithms with its related HN that these algorithms include message authentication code's f_1, f_2 and key generation's functions f_3, f_4. The key K, is named master key that is common between USIM and AuC and never has been transmitted between these two places. The length of this constantly hidden key is 128 bits. Also, the channel between the HN and SN is supposed as a secure cannel. $RAND_1$, $RAND_2$, $RAND_3$ are random numbers and ID_{SN} and ID_{HN} are the identifier of the SN and HN, respectively. AMF (Authentication and key Management Field) is the field of the authentication and key management that is used to define the options related to operator during authentication; for instance, using of several authentication algorithms or defining a limitation for the usage of a key. Count is a counter with initial value of zero. When MS is sending an authentication request to the SN, the value of this counter increases one unite.

The IAP AKA protocol operation, as seen in figure 2, is as follows:

1) SN creates a random number ($RAND_1$) and sends to the MS.
2) MS calculates $U_{MS}=f_1(K, RAND_1, ID_{SN})$ and sends it with a random number ($RAND_2$) to the SN.
3) SN sends the values of $RAND_1$, $RAND_2$, U_{MS}, IMSI (International Mobile Subscriber Identity) to HN (Home Network). IMSI is a fifteen-digit number that is saved in SIM (Subscriber Identity Module) and is ascribed by the network operator to the user. IMSI allows the operator to assign a phone number to the subscriber. This number includes an ID corresponding to a country that provides a global function. IMSI is mostly bookkeeping and to preclude its replication, try to send as less as possible.
4) HN calculates the value of $U_{MS}=f_1(K, RAND_1, ID_{SN})$ and compares it to U_{MS}. If these two values are not identical, the authentication process will be impeded because this inequality shows that MS has not K integer value or ID_{SN} was not correct and a fraudulent-SN had intent of attacking. If these two values are identical, HN will calculate the following values:

$$U_{HN} = f_1(K, RAND_2 \| ID_{HN} \| AMF) \quad (13)$$

$$AUTH_{HN} = U_{HN}\ RAND_2 \| AMF \quad (14)$$

Then, the $AUTH_{HN}$ is sent to the SN.
5) SN creates the random number of $RAND_3$ and calculates the following values:

$$U_{SN} = f_1(U_{HN} \| ID_{SN} \| RAND_3 \| AMF) \quad (15)$$

$$AUTH_{SN} = U_{SN} \| RAND_3 \| AMF \quad (16)$$

Then SN adds one unit to the value of Count and sends $AUTH_{SN}$ and $RAND_3$ to the MS. When the value of Count received from SN is more than the amount of its counter, MS will substantiate the Count accuracy and calculate U_{SN} from $AUTH_{SN}$. MS has the values of K, ID_{HN}, ID_{SN}, $RAND_2$, $RAND_3$, AMF, therefore it can calculate $U_{HN} = f_1(K, RAND_2 \| ID_{HN} \| AMF)$. Then it calculates $U_{SN} = f_1(U_{HN} \| ID_{SN} \| RAND_3 \| AMF)$. In

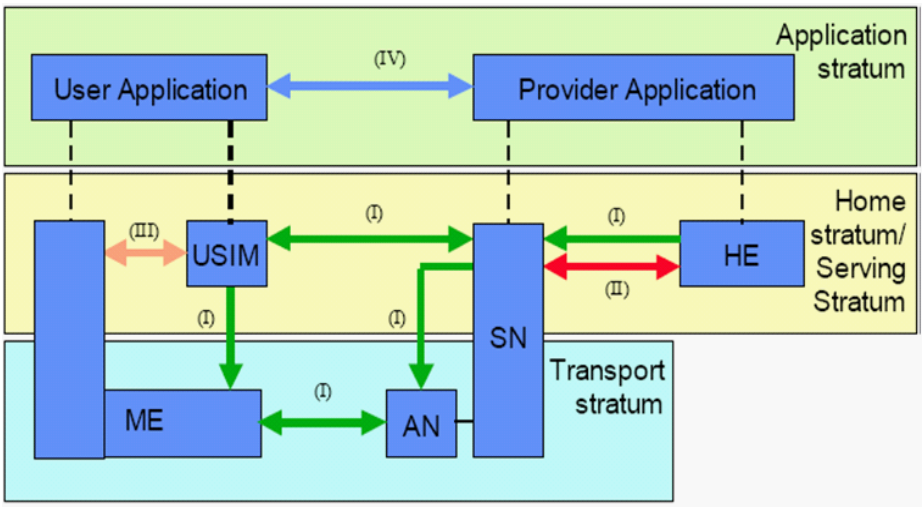

Fig.1. Security architecture in UMTS network

the next step, it compares these values with received value of $AUTH_{SN}$ from SN. If they are equal, MS calculates the authentication of the SN and HN. At the final step, MS calculates the value of RES = f_2 ($RAND_3$) and sends it to SN.

SN calculates the value of the f_2($RAND_3$) and compares it with RES. If these two values are equal, the authentication process ends successfully and SN and MS calculate the value of encryption key CK = f_3 ($RAND_3$) and integrity key IK = f_4 ($RAND_3$).

The proposed authentication and key agreement protocol

Some protocols do not use the ID_{SN} identifier during the authentication process and emphasize on the SN identification, so it can increase the possible false base station attacks. Actually, the commercial kinds of these false base stations exist that are called IMSI catcher too (Fox, 2002) and has all features of an authorized base station. These false base stations are capable of introducing themselves as an authorized base station and connect to MS. On the other hand, they are able to contact with HN as an MS. IAP AKA protocol is a resistant one to the attack of a false SN or false base station due to use of ID_{SN} in the first step and send it to HN in the next step. Nevertheless, this protocol has some drawbacks inferring as follow. Authentication Vector (AV) is not used in IAP AKA protocol unlike UMTS AKA (Niemi & Nyberg, 2003). But in E-UMTS AKA protocol despite AV elimination from the protocol, there is a temporary common key between MS and SN being calculated from a private long-term key named K. then, MS is able to calculate the key

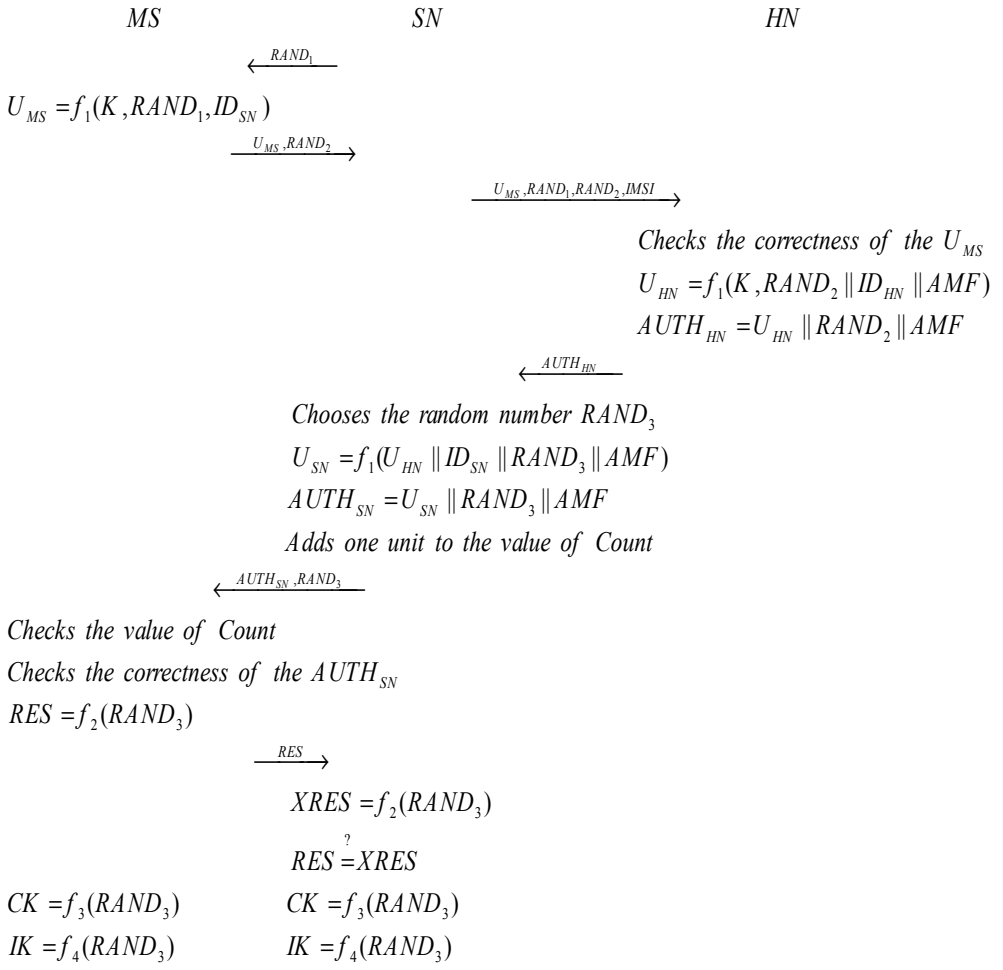

Fig. 2. The authentication and key agreement protocol of IAP- AKA

but SN does not. Therefore, HN calculates this temporary key and makes it accessible for SN. Now SN should calculate the information related to the user authentication by use of this temporary key because of no existence of authentication. While in IAP AKA protocol (Shalmany & Rahbar, 2008) there is no common key between MS and SN causing many problems.

1) During the fifth step when the (AUTHSN, RAND3) message is sent on a public channel, attacker can calculate the RES = f_2 ($RAND_3$) with user impersonation and also can send it to SN because it has an access not only to the $RAND_3$ but also to the f_2 algorithm that is available at the USIM for every user. It is necessary to remind that the encryption algorithms in the UMTS are based on TS33.105 standard (Third Generation Partnership Project & Technical Specification Group SA;3G Security, 2004). As a result, the key, K, is used to calculate f_1, f_2, f_3, and f_4 functions because these algorithms are public and their security depends on the key that is used for them.

Fig. 3. The proposed authentication and key agreement protocol

However, IAP AKA has no key for the considered functions.

2) The CK and IK calculation is possible for the attacker because it has access to the $RAND_3$: f_3, f_4 are the key production functions that in IAP AKA unlike other protocols, no key is used.

In the proposed protocol two one-way hash functions, f_1 and f_2, and four key generation functions (g_1, g_2, g_3, g_4) are used. The first phrase in the parenthesis of the function f is the key of this function and other sentences are phrases that the function f is applied on them.

This protocol assumes that HN saves the former and current IMSI and TID_{MS} of every customer in its database. TID_{MS} is the temporary customer ID which is formed from IMSI and MS received it from HN. HN and MS have a counter, COUNT. Also in this protocol we assume that the G is a group of elliptic curve from first order q, p is a random member of G, and a, b are two random members of Z_q. Also we assume that the discrete logarithm of the elliptic curve (Hankerson, Vanstone, & Menezes, 2004) in Z_q is a hard problem. As seen in figure 3 the steps of the protocol are as follow:

1) First SN generates the random number of $RAND_1$ and sends to the MS.
2) MS calculates $MAC_{TIDMS} = f_1 (K, CTID_{MS} || RAND_1 || RAND_2)$ and $U_{MS} = RAND_2 || MAC_{TIDMS}$ and sends U_{MS} and $cTID_{MS}$ to the SN. Also when the protocol is running for the first time, MS sends its permanent ID (IMSI) because it has no temporary ID.
3) SN sends the values of $RAND_1$, $cTID_{MS}$, and U_{MS} to the HN.
4) HN firstly searches its own dataset for MS authentication. In this database for every user, former and current TID_{MS} and IMSI as well as the key K is associated with that IMSI are saved. The former TID_{MS} is saved for solving the synchronization problem in TID_{MS}. HN obtains the key K related to the MS after finding the $cTID_{MS}$ in its database. Then it calculates the value of $MAC_{TIDMS} = f_1 (K, CTID_{MS} || RAND_1 || RAND_2)$ and compares it to received value for MS. If these two values are not identical, the authentication process will be impeded. But if two values are identical, HN chooses the random number of $RAND_3$ and calculates the following values:

$nTID_{MS} = f_1 (K, cTID_{MS})$ (17)

$AK = g_1 (K, RAND_3)$ (18)

$K_{TEMP} = g_2 (K, RAND_2)$ (19)

$U_{HN} = f_2 (K, RAND_2 || ID_{HN} || AMF)$ (20)

$AUTH_{HN} = (AK \oplus nTID_{MS} || U_{HN} || RAND_2 || AMF)$ (21)

Where $nTID_{MS}$ is the new ID for the user and will be used in the next step of running protocol. AK is an anonymity key and its duty is protecting the secrecy of the temporary ID. Finally, HN sends the $AUTH_{HN}$ and K_{TEMP} values to the SN.

1) SN chooses the random number of $RAND_4$ and $b \in Zq$. Then, SN calculates the bP that the P is a point on the elliptic curve. Then, SN calculates the following values:

$U_{SN} = f_2 (K_{TEMP}, U_{HN} || ID_{SN} || RAND_4 || bP)$ (22)

$AUTH_{HN} = (AK \oplus nTID_{MS}) || U_{SN} || RAND_3 || RAND_4 || AMF)$ (23)

Then, SN adds one unit into the value of the Count and sends $AUTH_{HN}$, bP, and $RAND_4$ to the MS.

2) MS evaluates the correctness of the Count then calculates the U_{SN} from $AUTH_{SN}$. MS has the values of K, ID_{HN}, $RAND_2$, and AMF, therefore it can calculate the value of $U_{HN} = f_2 (K, RAND_2|| ID_{HN} || AMF)$. Then it calculates $KTEMP = g_2 (K, RAND_2)$ and $U_{SN} = f_2 (K_{TEMP}, U_{HN} || ID_{SN} || RAND_4 || bP)$. After that it compares these values with the value of the received U_{SN} from SN and if two values are identical, the authentication of SN and HN will be performed by the MS. Then, MS does the following calculations to attain the temporary ID that is needed in the next step of the running protocol:

$AK = g_1 (K, RAND_3)$ (24)

$nTID_{MS} = AK \oplus (AK \oplus nTID_{MS})$ (25)

1) Now, MS chooses the random number of $a \in Zq$ and calculates the aP. Finally, it calculates the value of the $RES = f_2 (K_{TEMP}, RAND_4 || aP)$ and sends it to the SN.
2) SN calculates the value of $f_2 (K_{TEMP}, RAND_4 || aP)$ and compares it with the value of the RES received from MS. If these two values are identical, the authentication process ends

successfully and SN and MS calculates the cipher key $CK = g_3(K_{TEMP}, abP)$ and integrity key $IK = g_4(K_{TEMP}, abP)$.

Proposed Security Analysis

Now we investigate the operation of the authentication and proposed key agreement protocol.

1) The attack of the false SN: in this protocol because of ID_{SN} using in U_{MS} and sending it to HN that makes it possible for HN to authenticate the SN, the attacker cannot introduce itself as a real SN and connect to MS. Therefore, this protocol is resistant to the false SN attack.
2) Reply attack: in this attack, the attacker saves the exchanged information related to the previous meeting. The attacker tries to impersonate one of the parties to send the information again. According to the random numbers available in this protocol, there is no possibility for the attacker to plan an attack. For example, U_{MS} is calculated in every stage from a new RAND1 which is sent by SN. Therefore, the attacker cannot send it again and the proposed protocol is resistant to this attack.
3) Effect of short-term key disclosure: if K_{TEMP} as a temporary and short-term key is compromised, the attacker cannot calculate CK and IK. In order to calculate the session key, attacker should calculate abP. Calculation of abP with aP and bP is difficult regarding to the computational Diffie-Hellman problem (CDP) on elliptic curve. Therefore, the attacker cannot calculate CK and IK.
4) Forward secrecy: this feature (Park, Boyd, & Moon, 2000) states that the attacker should not be able to attack the security of the former exchanged information if the private long-term keys for one or some user are disclosed. In this protocol, the attacker can calculate K_{TEMP} using the long-term private key K.But according to computational Diffie-Hellman problem on elliptic curve, calculation of abP with available values of aP and bP is difficult. Therefore, attacker cannot calculate IK and CK keys. As a result, the proposed protocol has the propertyof forward secrecy.
5) The confidentiality of the user ID: as mentioned earlier, one of the available properties in the security feature for network accessing is the confidentiality of the user ID. In some of the former protocols, IMSI was sent as a plaintext that was in discrepancy with the confidentiality of the user ID. In the proposed protocol, the temporary user ID (TID_{MS}) is sent instead of IMSI that prevents from its disclosure to the attacker. A main character that the proposed protocol has in comparison with other protocols is the usage of the anonymity key (AK). In this protocol, SN has no access to the temporary user ID and only knows the phrase ($nTID_{MS} \otimes AK$). Because of the AK calculation of being possible only through HN and MS, SN has no access to temporary user ID and this condition will increase the confidentiality of the user ID.
6) Using the public key operations: MS has limitation in battery and computational operation, so none of the former protocols have used the public key; but in this protocol each of the MS and SN run two elliptic curve processes during each running of the protocol. With a rapid technology development, nowadays some solutions completely based on the public key for UMTS have been proposed (Kambourakis, Rouskas, & Gritzalis, 2004; USECA Project, 1999). Because of using long-term keys in this protocol, there is no need to use the attestation and two elliptic curve processes during each authentication do not have many calculations for MS.

In this section, our proposed protocol is compared with the previous protocols (Table 1). UMTS AKA and AP AKA protocols use AV to decrease frequency of access to the HN. However, the usage of AV causes the loss of bandwidth between HN and SN. To solve this problem E-UMTS AKA and proposed protocols use the temporary key instead of AV. In UTMS AKA, HN cannot authenticate MS. While in some other protocols, HN uses the U_{MS} to authenticate MS. In all protocols, MS uses U_{HN} to authenticate the HN.

To calculate U_{HN} and U_{SN} the random numbers are used that entails MS to be sure of U_{HN} and U_{SN} novelty. In the former protocols, the

disclosure of the private long-term K key lead to the exposure of the former relations while in the proposed protocol, the disclosure of the K key has no effect on the former relations.

Furthermore, the disclosure of the short-term keys available at AVs in UMST AKA and AP AKA protocols and also in proposed protocol has no effect on the security of other AVs. On the other hand, in the E-UMTS AKA protocol, the disclosure of the short-term K_{TEMP} key causes the exposure of former relations. Because of disregarding the use of ID_{SN} in UMTS AKA, there is a possibility of false SN attack but in proposed protocol there is no possibility for this attack.

In the former protocols, IMSI is sent as a decrypted text that threatens the confidentiality of the user ID but the secrecy is maintained in the proposed protocol.

CONCLUSION

In this paper we have scrutinized some authentication and key agreement protocols in the network environment of the UMTS. First, we examined the IAP AKA protocol that was proposed as a solution to overcome the shortcomings of UMTS AKA protocol and also we showed that this protocol has its own drawbacks; namely, the lack of confidentiality for the user ID and having no forward secrecy feature. Therefore, we proposed a protocol that not only fixes the former problems but also has some new features. The proposed protocol offers a new method for making the confidentiality of user ID that precludes the serving network from accessing to the temporary ID of the user.

REFERENCES

1. Fox, D., Der IMSI-catcher. *Datenschutz und Datensicherheit,* 2002; **26**(4): 212-215.
2. Hankerson, D., Vanstone, S., & Menezes, A. J., *Guide to elliptic curve cryptography*: Springer, 2004.
3. Harn, L., & Lin, H. Y., *Modification to enhance the security of the GSM protocol.* Paper presented at the Proceedings of the 5th national conference on information security, 1995.
4. J.AL-Saraireh, & S.Yousef., Extension of authentication and key agreement protocol (AKA) for universal mobile telecommunication system (UMTS),. *Theoretical and Applied Computer Sciences,,* 2006; ***1***(1), 109–118.
5. Kambourakis, G., Rouskas, A., & Gritzalis, S.., Performance evaluation of public key-based authentication in future mobile communication systems. *EURASIP Journal on wireless Communications and Networking,* 2004; 2004(1): 184-197.
6. Lee, C.-H., Hwang, M.-S., & Yang, W.-P., Enhanced privacy and authentication for the global system for mobile communications. *Wireless networks,* 1999; **5**(4): 231-243.
7. Niemi, V., & Nyberg, K., *Front Matter*: Wiley Online Library, 2003.
8. Park, D., Boyd, C., & Moon, S.-J., *Forward secrecy and its application to future mobile communications security.* Paper presented at the Public key cryptography, 2000.
9. Shalmany, N. A., & Rahbar, A. G. P.., *Improved Adaptive Protocol for authentication and key agreement*. Paper presented at the Telecommunications, 2008. IST 2008. International Symposium on, 2008.
10. Third Generation Partnership Project, & Technical Specification Group SA., Network Architecture,version 4.4.0, 2002.
11. Release 4," 3GPP,TS 23.002, .
12. Third Generation Partnership Project, & Technical Specification Group SA;3G Security., Cryptographic Algorithm requirements,version 4.2.0, Release 4," 3GPP,TS 33.105, 2004.
13. Third Generation Partnership Project, & Technical Specification Group SA;3G Security.., Security Architecture,version 4.2.0, Release 4," 3GPP,TS 33.102, 2001.
14. USECA Project., UMTS security architecture: Intermediate report on a PKI architecture for UMTS, . Public Report, 1999.
15. Zhang, M., & Fang, Y., Security analysis and enhancements of 3GPP authentication and key agreement protocol. *Wireless Communications, IEEE Transactions on,* 2005; **4**(2): 734-742.