Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 867315, 12 pages
doi:10.1155/2011/867315

Research Article

A USIM-Based Uniform Access Authentication Framework in Mobile Communication

Xinghua Li,[1] Jianfeng Ma,[1] YoungHo Park,[2] and Li Xu[3]

[1] *Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an, Shaanxi 710071, China*
[2] *Mobile Network Security Technology Research Center, Kyungpook National University, Daegu 702-701, Republic of Korea*
[3] *Key Lab of Network Security and Cryptology, Fujian Normal University, FuZhou 350007, China*

Correspondence should be addressed to Xinghua Li, lixingh@gmail.com

Received 1 June 2010; Revised 31 August 2010; Accepted 1 October 2010

Academic Editor: Damien Sauveron

With the rapid development of the mobile communication and wireless access technologies, the interworking of heterogeneous networks turns into a trend and various wireless networks are getting connected with the mobile core networks through different measures. At present, in mobile communication, though access authentication methods of various access networks are different from each other, they are all based on the unique authentication algorithm in (U)SIM, which results in several drawbacks and cannot fulfill the requirements of the future mobile communications. The underlying reason is the authentication algorithm is not extensible and the authentication framework is not independent of the communication technologies. In order to solve this problem, we propose a uniform access authentication framework. Making use of the extensive authentication protocol EAP, we add a media-independent authentication layer in USIM which outputs the uniform keys after an authentication, and a key adaptation layer is designed in the terminals which transforms the output keys accordingly to meet the specific requirements of various communication modules. In such a method, USIM is extensible in authentication algorithms and the authentication framework is independent of the communication technologies. Our analysis indicates that the proposed scheme is of great advantages over the current one.

1. Introduction

With the rapid development of the mobile communication and wireless access technologies, the interworking of heterogeneous networks turns into a trend and various wireless networks are getting connected with the mobile core networks through different measures. It can be envisaged that the future mobile communication will not be one technology that dominates the others, instead, different wireless access technologies will coexist and complement each other. They will provide various services and seamless mobility, which can effectively meet the requirements of personal communication and information acquisition.

In 2004, 3GPP launched the Long-Term Evolution (LTE) of wireless access networks [1] and the System Architecture Evolution (SAE) [2] oriented to the all-IP packet core networks. 3GPP hopes to retain its predominance and competition in mobile communication field through its consistent evolution and enhancement from the wireless interface to the core networks. The goal of SAE and LTE is to decrease the networks delay and get higher data rate, higher system volume and better coverage, and to the end the cost of operators and subscribers is reduced.

As the core networks, SAE integrates various wireless access networks, such as the GERAN of 2G, UTRAN of 3G, E-UTRAN of LTE, WLAN, WiMAX. And it can be foreseen that with the development of the mobile communication, more and more wireless access networks will interconnect with the mobile core networks. At the same time, the mobile terminal will be multimode which can support multiple access technologies and provide more measures to acquire information for the users. But different access networks employ different authentication protocols to get access to the core networks, for example, GERAN by GSM authentication [3], UMTS by UMTS AKA [4], LTE by EPS AKA [5], WLAN and WiMAX by EAP-AKA [6]. In the aforementioned authentication protocols, in a mobile terminal the specific authentication algorithm is implemented on (U)SIM card. For GERAN, SIM card runs GSM authentication algorithm. While for the UTRAN, LTE, WLAN and WiMAX, they all employ USIM to run the AKA algorithm though their respective authentication protocols are not same. That is, the present SIM or USIM supports only one authentication algorithm. In the long run of mobile communication, this authentication method will result in the following drawbacks.

(1) If a user updates his communication equipments, for example, from GSM phone to 3G phone, even in the same operator networks, in order to enjoy the 3G service he has to change his SIM card to USIM. Nowadays, the mobile communication technology develops rapidly, and updating mobile communication technologies will adopt new authentication protocols, as the 3GPP TS 33821-800 [7] has pointed out. Therefore, to support the emerging communication technologies USIM will have to be constantly updated.

(2) In the long run, the future mobile communication technology (e.g., 4G) should support various authentication algorithms which are based on either the symmetric key or the asymmetric key. A lot of research has been made and many authentication protocols have been proposed [8–10] in this field. But the present USIM just supports the AKA algorithm, which evidently cannot meet the requirements of future wireless communication technology.

(3) It is expected that USIM not only supports multiple authentication algorithms, but provides the terminal the function to negotiate a suitable authentication protocol with the networks according to a specific user or scenario. But at present the operator implements the same authentication protocol for any user under any circumstance, and it cannot provide personalized authentication services, neither can it adopt different authentication methods according to the different scenario (e.g., roaming or nonroaming), which limits the operator to provide better services and cannot meet the requirements of the future mobile communication.

(4) In addition, in functionality it is expected that USIM is independent of the terminal equipment: USIM is used to identify the user and perform the access authentication, while the terminal equipment is to communicate with the networks. At present, in order to make use of the AKA algorithm in USIM, WLAN or WiMAX modules (or interface cards) in the multimode terminal have to take part in the implementation of the authentication protocol EAP-AKA, which results in "tight couple" between the USIM manufactures and terminal equipment manufactures and detriment their respective development and maintenance.

We find that the fundamental reason resulting in the drawbacks mentioned above is the present USIM is not extensible in terms of authentication algorithm and the authentication framework is not independent of communication technology. For the independence, 3GPP TR 23.882 [11] has also specified this requirement. In order to overcome the drawbacks and meet the development requirements of mobile communication, we propose a uniform access authentication framework. First, taking advantage of the Extensible Authentication Protocol EAP, we realize the media-independent access authentication in USIM which outputs uniform keys after the success authentication. Then, in the terminal, a key adaptation layer is designed which transforms the output keys accordingly to meet the specific requirements of various communication modules in the terminals. In such a way, USIM is extensible in authentication algorithms and the authentication framework is independent of the underlying communication technologies. In addition, the function of USIM and the terminal can be separated from each other, which facilitates their respective development and maintenance.

The rest of this paper is organized as follows. Section 2 briefly presents the background. The proposed uniform access authentication framework and procedure are described in Section 3. Section 4 gives the implementation of the uniform access authentication. Section 5 analyzes its security, performance and advantages. Finally, we conclude this paper in Section 6.

2. Background

2.1. SAE Architecture. SAE architecture is shown in Figure 1, which is made up of two parts: core networks and access networks.

Core Networks. The core networks consist of two parts, and they are UMTS core networks and Evolved Packet Core, respectively, which are connected through the S3 interface.

Access Networks. Access networks consist of the following wireless networks: (1) GERAN of 2G, (2) UTRAN of 3G, (3) E-UTRAN of LTE, (4) Trusted non-3GPP access networks, typically is WiMAX, (5) Untrusted non-3GPP access networks, typically is WLAN.

Different access networks or access technologies adopt different authentication methods to access the SAE:

(i) GERAN adopts GSM authentication;

(ii) UTRAN adopts UMTS AKA;

(iii) LTE adopts EPS AKA;

(iv) WLAN and WiMAX adopt EAP-AKA.

2.2. GERAN Access Authentication: GSM Authentication [3]. The authentication procedure of GSM is shown in Figure 2. The user equipment UE sends the international mobile subscriber identity (IMSI) to the authentication center HLR/AuC in its home networks which generates n authentication vectors using the shared key K with SIM and

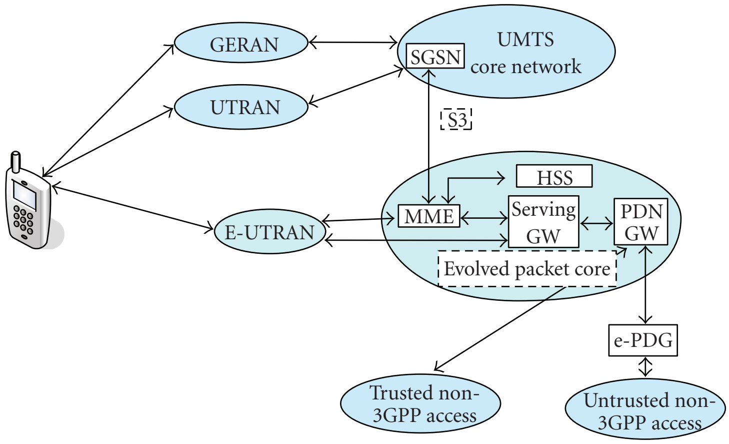

Figure 1: SAE architecture.

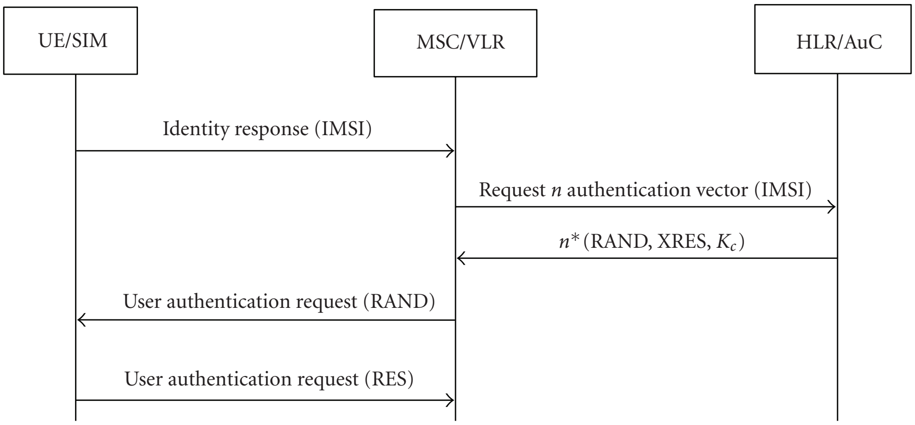
UE/SIM
MSC/VLR
HLR/AuC
Identity response (IMSI)
Request n authentication vector (IMSI)
n* (RAND, XRES, K_c)
User authentication request (RAND)
User authentication request (RES)

Figure 2: GSM Authentication.

sends them to the MSC/VLR. Every authentication vector is a triple (RAND, XRES, K_c) where RAND is a random value, XRES is the expected response of RAND and K_c is the derived encryption key. Upon receiving the authentication vectors, MSC/VLR selects one and sends the RAND to UE. SIM computes the response RES and K_c based on the shared key K and RAND and delivers RES to the MSR/VLR which compares XRES with RES. If equal, UE is authenticated successfully and from then on, UE and the base station use K_c to protect the messages transmitted between them.

In the above procedure just the networks authenticate the UE, but UE does not authenticate the networks. In addition, this protocol is not secure enough and many security drawbacks have been identified [12]. Therefore, 3G improves this authentication procedure using AKA algorithm.

2.3. G Access Authentication: UMTS-AKA [4]. In 3G, USIM shares a key K with the authentication center HE/AuC in the home networks. Based on this key, UE and networks authenticate each other through the UMTS AKA which procedure is shown in Figure 3.

Through the first two messages, VLR/SGSN gets UE's identity and requests the corresponding authentication vectors from HE/AuC which generates and sends n authentication vector back. Each vector is a quintuple (RAND, XRES, CK, IK, AUTN) where RAND is a random value, XRES is the expected response of RAND, CK is the encryption key, IK is the integrity key and AUTN is the network authentication token. Upon receiving these authentication vectors, VLR/SGSN selects one and sends RAND and AUTN to UE. Through verifying AUTN, USIM authenticates the networks. Then, it computes the response RES of RAND using the shared key K and derives the CK and IK. Finally, it delivers RES to the VLR/SGSN which compares XRES with RES. If equal, the UE is authenticated successfully.

2.4. G-WLAN and 3G-WiMAX Authentication: EAP-AKA [6]. Using the shared key K between USIM and the core networks, UE adopts EAP-AKA to get access to the SAE through WLAN or WiMAX. This procedure is similar to the UMTS AKA and the main difference is that it is implemented in EAP framework. The procedure is shown in Figure 4 where

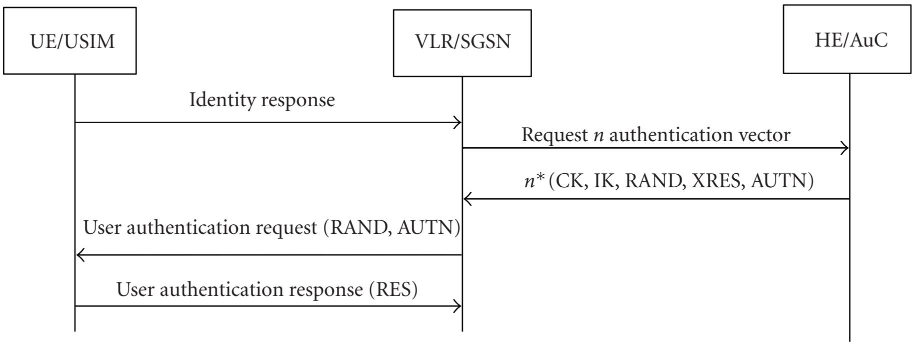
UE/USIM
VLR/SGSN
HE/AuC
Identity response
Request n authentication vector
n* (CK, IK, RAND, XRES, AUTN)
User authentication request (RAND, AUTN)
User authentication response (RES)

Figure 3: UMTS AKA.

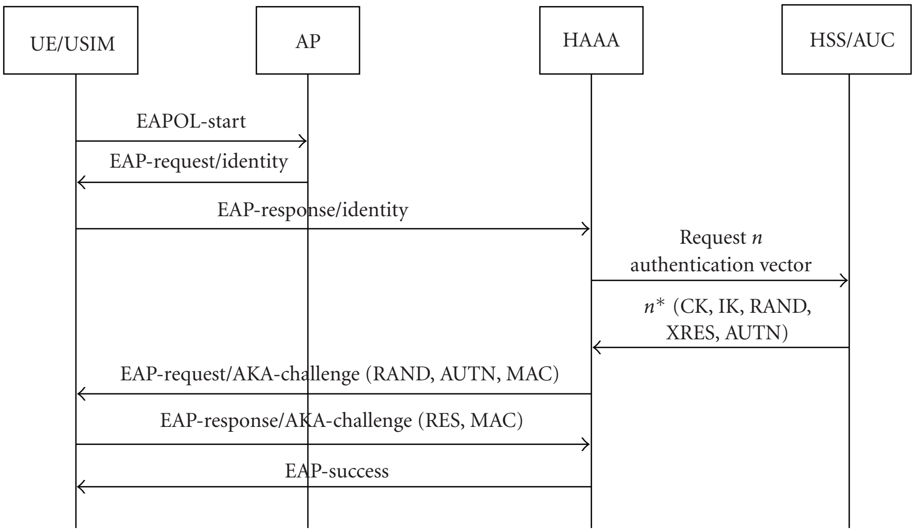
UE/USIM
AP
HAAA
HSS/AUC
EAPOL-start
EAP-request/identity
EAP-response/identity
Request n authentication vector
n* (CK, IK, RAND, XRES, AUTN)
EAP-request/AKA-challenge (RAND, AUTN, MAC)
EAP-response/AKA-challenge (RES, MAC)
EAP-success

Figure 4: EAP-AKA.

the first three messages EAPOL-Start, EAP-Request/Identity and EAP-Response/Identity are inherent in EAP framework. Through these three messages, HAAA gets the UE's identity, and then performs the AKA authentication with UE. Compared with the UMTS AKA, a message authentication code MAC is added to the EAP-Request/AKA-Challenge and EAP-Response/AKA-Challenge, which provides the integrity protection to the EAP messages.

It should be noted that in this procedure the computation of RES and the verification of AUTN is performed by the AKA algorithm on the USIM. While the generation or verification of the MAC is performed by the WLAN and WiMAX wireless interface cards. Therefore, in EAP-AKA, WLAN and WiMAX wireless interface cards take part in the protocol implementation. That is, the communication module is involved in the authentication protocol implementation.

2.5. Access Authentication of LTE: EPS AKA [5]. Similar to UMTS AKA, EPS AKA is also based on the shared key K between USIM and the networks, which procedure is shown in Figure 5. After receiving UE's IMSI, the mobility management entity MME sends the home network HE Authentication Data Request which includes IMSI, serving networks SN identity and network type. Upon receiving the request, HE generates an EPS authentication vector (RAND, XRES, AUTN, KSI_{ASME}) where the first three parameters are same as those in the EAP-AKA, and KSI_{ASME} is the key set identity of access security management entity ASME. MME sends the RAND, AUTN and KSI_{ASME} to the UE which verifies the AUTN and authenticates the networks. If successful, UE generates the response RES and sends it back to MME which compares XRES with RES and authenticates UE. The key hierarchy established in this procedure is shown in Figure 6.

2.6. Analysis of Access Authentication Protocols in SAE. From the procedures above, it can be seen that in UMTS AKA, EPS AKA and EAP-AKA, the terminal in these three cases all makes use of USIM to realize authentications. Though the authentication protocols are different, they all implement the AKA algorithm on USIM which is shown in Figure 7.

From the authentication procedures above, it can be seen that USIM just realizes a specific authentication algorithm AKA which is independent of the underlying communication

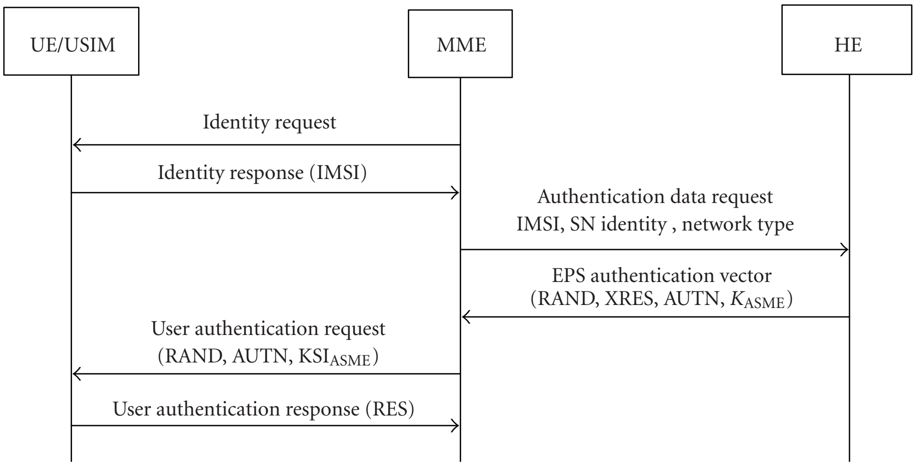
UE/USIM
MME
HE
Identity request
Identity response (IMSI)
Authentication data request
IMSI, SN identity , network type
EPS authentication vector
(RAND, XRES, AUTN, K_{ASME})
User authentication request
(RAND, AUTN, $\mathrm{KSI}_{\mathrm{ASME}}$)
User authentication response (RES)

Figure 5: EPS AKA.

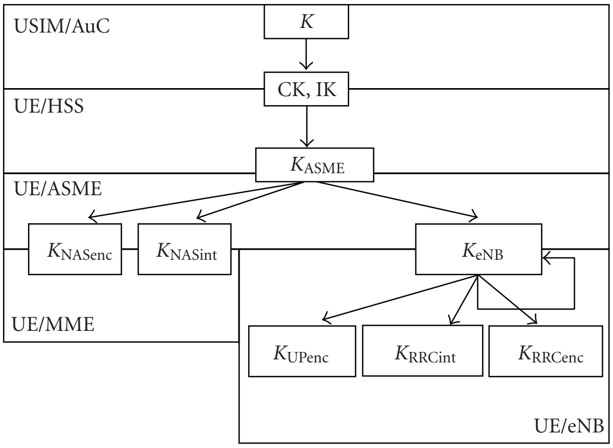

Figure 6: Key hierarchy generated in EPS-AKA.

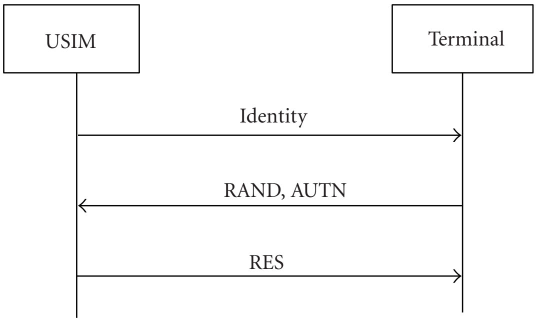

Figure 7: AKA algorithm on USIM.

technologies. That is, regardless of what kind of access networks, USIM always implements this algorithm to realize the mutual authentication with the mobile core networks. The drawbacks resulting from this authentication method have been presented in Section 1, and its underlying reasons are as follows.

(1) The authentication algorithm in USIM is not extensible, and other authentication methods cannot be integrated into it. Therefore, USIM has to be changed to support the authentication protocols in emerging network technologies.

(2) The authentication framework is not independent of underlying communication technologies. At present, USIM just realizes the independence between AKA algorithm and communication technologies, but it cannot integrate other authentication methods to realize the independence between the authentication framework and communication technologies. Therefore, the functions of USIM and terminals cannot be completely separated from each other. Furthermore, UE is not able to negotiate and implement a suitable authentication algorithm with the networks according to a specific user or scenario.

3. The Uniform Access Authentication Framework and Authentication Process

In order to overcome the drawbacks mentioned above, we propose a uniform access authentication method based on USIM, which enables the authentication framework independent from communication technologies, and provides the extensibility to the authentication method. Besides, this framework can integrate the existing protocols and support various wireless access authentication protocols on one USIM, which can meet the authentication requirements of the future communication technology.

3.1. The Uniform Access Authentication Framework on UE. The proposed uniform access authentication framework is shown in Figure 8 which consists of two parts: the “media independence authentication layer” in USIM, and the “key

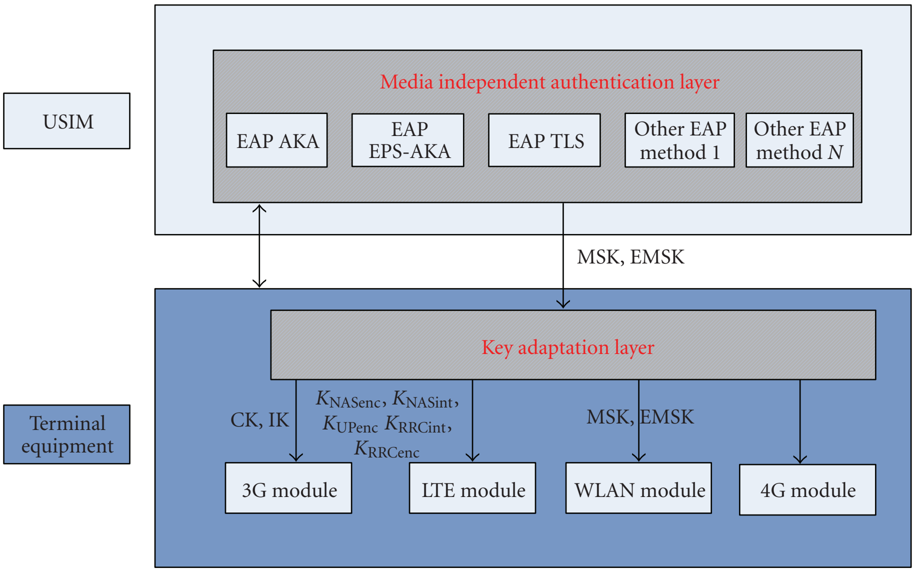

Figure 8: Uniform Access Authentication Framework on UE.

adaptation layer" in the terminal equipment. The terminal equipment is multimode which supports multi communication technologies, such as 3G, LTE, WLAN, WiMAX, 4G.

(1) Media Independent Authentication Layer. This layer enables USIM to support EAP framework [13]. UMTS AKA and EPS AKA are integrated into the EAP framework to form the EAP-AKA and EAP EPS-AKA. In addition, EAP framework is open and new protocols can be integrated according to the specific application, for example, in order to fulfill the access authentication requirements of 4G, some new EAP methods can be introduced (such as "other EAP method 1", "other EAP method *N*" in Figure 8). When the terminal accesses the networks, the media-independent authentication layer negotiates and implements a suitable authentication protocol with the networks. After the successful authentication, it outputs the uniform keys (MSK, EMSK).

(2) Key Adaptation Layer. This layer provides expected keys to different communication modules. Various communication module use different forms of keys. (CK, IK) provide security protection for 3G, (K_{NASenc}, K_{NASint}, K_{UPenc}, K_{RRCint}, K_{RRCenc}) for LTE, and (MSK, EMSK) for WLAN [13]. The uniform keys that media-independent authentication layer outputs are MSK and EMSK, which cannot meet the requirements of various communication modules. In order to provide the expected keys to different communication modules, a key adaptation layer is needed between the media-independent authentication layer and communication module, which adapts MSK and EMSK to the key form that each communication module requires. Specifically, the key adaptation layer in every communication module transforms the (MSK, EMSK) to their respective key form.

3.2. The Uniform Access Authentication Procedure. The message interactions between USIM, the terminal equipment and the networks in the uniform access authentication procedure are shown in Figure 9. First, the terminal activates the EAP module in USIM by sending the "AUTHENTICATE" to USIM which then replies with EAP-Start message back to the server through the terminal. Upon receiving this message, the server requires UE's identity through EAP-Request/Identity. In EAP-Response/Identity, UE delivers its identity to the server. Thereafter, USIM and the server negotiate a suitable authentication protocol to implement. After the successful authentication, USIM outputs (MSK, EMSK) to the terminal.

Meanwhile, in order to support the uniform access authentication, the authenticator (e.g., NodeB in 3G, eNodeB in LTE and AP in WLAN) shall support port-based access control [14]. That is, before the successful authentication only EAP message is permitted to pass through. Thereafter, the port for the data communication is unlocked. In addition, the authentication server also has to support EAP authentication and generally RADIUS server is applicable.

4. Implementation

In order to realize the uniform access authentication, there are three pieces of work that have to be done: (1) introduction of EAP in USIM, (2) introduction of other authentication methods into EAP framework, (3) adaptation of (MSK, EMSK). In the following, we will describe these three procedures in details.

4.1. Introduction of EAP in USIM. In order to introduce EAP in USIM, we shall realize EAP supplicant in USIM.

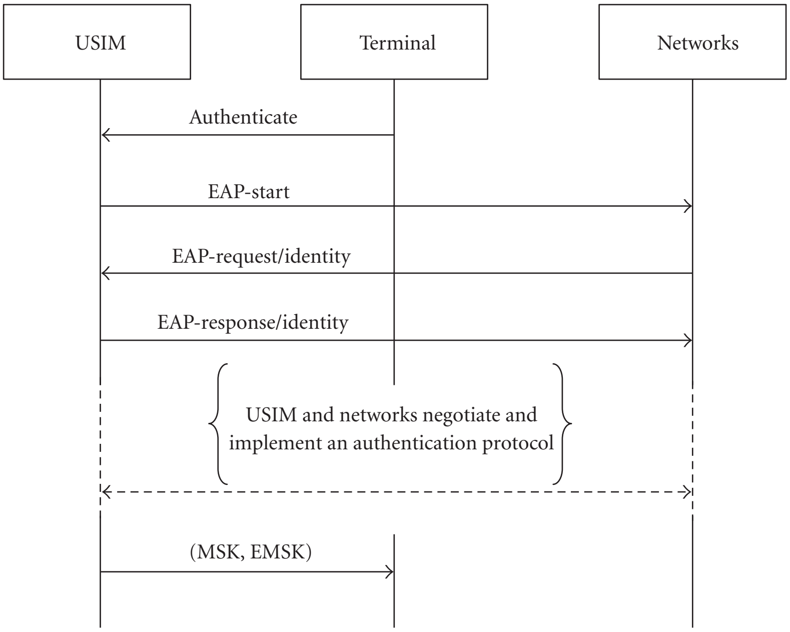

Figure 9: Message interaction procedure in uniform access authentication.

At present, there are two EAP supplicants which are WPA-supplicant [15] and X-supplicant [16]. EAP supplicant is made up of three layers, and from top to bottom they are authentication layer, EAP layer and data-link layer, respectively. In order to realize EAP supplicant in USIM, we need to modify WPA-supplicant and X-supplicant accordingly. Because these two supplicants are mainly used in LAN and the underlying links mainly are 802.2 Ethernet, 802.5 Token Ring and 802.11 WLAN. But in mobile communication, the underlying links are the data-link layers of 3G, LTE, WLAN and 4G. Therefore, these two supplicants are not suitable for the mobile communication environment. In order to adapt EAP supplicants in the mobile communication environment, we replace the data-link layer in WPA-supplicant and X-supplicant with the data-link layer of mobile communication networks.

The realization of EAP framework in UE is shown in Figure 10, where Authentication Layer and EAP Layer are implemented in USIM and Data-Link Layer in the terminal equipment. In the Authentication Layer there are various authentication algorithms, such as UMTS-AKA, EPS-AKA and TLS. EAP Layer is in charge of the authentication protocol negotiation with the networks, and it sends and receives EAP frame. In addition, this layer encapsulates and decapsulates protocol data. The Data-Link Layer encapsulates and decapsulates the EAP message.

In addition, to make USIM support EAP framework, we need to extend the current command "AUTHENTICATE" [17] between USIM and the terminal equipment. Through the extended command, UE activates the EAP authentication module. Then WPA-supplicant or X-supplicant negotiates and implements a suitable authentication algorithm with the authentication server.

4.2. Introduction of Other Authentication Methods into EAP Framework. As shown in Figure 8, the media independent authentication layer should support various authentication methods which includes existing EAP methods (such as the EAP-AKA, EAP-TLS) and some new ones. Therefore, these new authentication methods should be introduced into the EAP framework. In the following, we take the EPS AKA as an example to show how to introduce a new authentication method in the EAP framework.

In order to integrate EPS AKA into the EAP framework as a new method, EPS AKA shall be added into the EAP supplicant (e.g., WPA-supplicant) and RADIUS server as an independent file. Then a unique "type" shall be assigned to this method and this "type" should be registered in EAP state machine. For example, the assigned type of EAP-MD5 is 4. The specific addition method can be referred to RFC 4137 [18] and WPA-supplicant [15] or X-supplicant [16]. In addition, in order to meet the requirement of uniform key output (MSK, EMSK), the key derived from EPS AKA needs to be transformed. After USIM and AAA server complete the EPS AKA, both get K_{ASME}. Based on this key, UE and the server derive MK, MSK and EMSK, respectively:

$$\begin{gathered} \mathrm{MK} = \mathrm{SHA1}(\mathrm{Identity} \mid K_{\mathrm{ASME}}), \\ \mathrm{MSK} \mid \mathrm{EMSK} = \mathrm{PRF}(\mathrm{MK}). \end{gathered} \tag{1}$$

In the above equation, PRF is a pseudo random function. Thereafter, USIM returns (MSK, EMSK) to the terminal.

4.3. Key Adaptation Layer. The goal of the key adaptation layer is to adapt the (MSK, EMSK) to the form that each communication module can accept. In the following, we present the key adaptation method of every communication module.

(1) The Key Adaptation Algorithm in 3G Communication Module. The keys that 3G needs are CK and IK. In order to meet the requirement of 3G, the key adaptation layer in the 3G module takes use of SHA-256 to process MSK and EMSK. The procedure is as follows:

$$\mathrm{CK} \mid \mathrm{IK} = \text{SHA-256}(\mathrm{MSK}), \tag{2}$$

In the above equation, SHA-256 is a secure hash function which output is 256 bits. The first 128 bits are assigned to CK and the latter to IK. Then CK and IK are exported to 3G communication module.

The authentication server delivers MSK to the authenticator NodeB through the EAP-Success [13] and the NodeB derives CK and IK using the same method mentioned above. These two keys provide the security protection to the messages transmitted between UE and NodeB.

(2) The Key Adaptation Algorithm in LTE Communication Module. The keys that the LTE communication module needs are K_{NASenc}, K_{NASint}, K_{UPenc}, K_{RRCint}, K_{RRCenc}. Upon receiving the MSK and EMSK from the USIM, the key adaptation layer in the LTE module computes the following key:

$$\begin{gathered} K_{\mathrm{eNodeB}} = \mathrm{PRF}(\mathrm{MSK}), \\ K_{\mathrm{NASenc}} \mid K_{\mathrm{NASint}} = \mathrm{PRF}(\mathrm{EMSK}). \end{gathered} \tag{3}$$

Then following the method in Figure 6, the LTE communication module computes K_{UPenc}, K_{RRCint}, K_{RRCenc} according to the K_{eNodeB}.

For MME, it first forwards MSK to the eNodeB through EAP-Success, then computes K_{NASenc} and K_{NASint} using the method above. Upon receiving the MSK, eNodeB derives the K_{UPenc}, K_{RRCint}, K_{RRCenc} using the method shown in Figure 6.

Then K_{UPenc}, K_{RRCint}, and K_{RRCenc} provide security protection to data exchange between the eNodeB and UE, while K_{NASenc} and K_{NASint} provide the security protection to the messages transmitted between MME and UE.

(3) The Key Adaptation in WLAN Communication Module. The keys that WLAN communication module needs are MSK and EMSK, and the outputs of EAP framework are right MSK and EMSK. Therefore, the key adaptation layer in WLAN communication module does not need to do anything, and it just outputs these two keys to the WLAN communication module.

(4) The Key Adaptation Algorithm in 4G Communication Module. At present, what kind of keys that 4G needs are unclear and when the specific protection method is determined, the adaptation algorithm can be designed based on MSK and EMSK.

5. Evaluation of the Proposed Authentication Method

5.1. Security Analysis. Compared with the original EAP framework, our proposed framework differs in that the three layers of the EAP framework do not resident in one entity: in our framework, the Authentication Layer and the EAP Layer reside in USIM, while Data-Link Layer in TE. The function of the Data-Link Layer is to encapsulate and decapsulate EAP messages which does not involve security-sensitive operations (e.g., encryption or decryption), therefore, this difference will not result in the security compromise of the EAP framework.

Just as the 802.11i, our scheme just provides a framework for authentication protocols. In the proposed framework, the authentication protocols does not need any change and their security is maintained.

Therefore, the security of the proposed framework mainly lies in the defense of the attacks against USIM because there will be security-sensitive information and operations in it, such as the shared key, as well as the encryption and decryption. The attacks are divided into two classes which are invasive attacks and noninvasive attacks [19].

(1) Invasive attacks mainly include removing the chip from the card, reverse engineering the chipset, and microprobing. To counteract the reverse engineering, a number of copy trap features can be incorporated into the chip designs and to introduce complexity into the chip layout and to use nonstandard cell libraries. To counteract the microprobing, a simple self-test procedure can be added to the smart card that takes an arbitrary input, encrypts and decrypts under an arbitrary key, and compares the result with the original block. Another solution involves disconnecting almost all of the CPU from the bus, leaving only the EEPROM and a CPU component that can generate read accesses [19].

(2) For noninvasive attacks, four major classes can be distinguished [19].

Timing Attacks or Chosen-Plaintext Attack. In order to countermeasure this attack, chosen-plaintext attack-resilient cryptography algorithms should be employed. Or, the maximum times of retrying of PIN should be limited [19].

Software Attacks. For example, a Trojan horse application could be used to transport an attack. A countermeasure to prevent this attack is to use a unique-access device driver architecture. Another way to prevent the attack is by using a smart card that enforces a “one private key usage per PIN entry” policy model [19].

Power and Electromagnetic Analysis Attacks. Simple Power Analysis, differential power analysis (DPA) [20, 21] and electro magnetic analysis (EMA) [22] all belong to this attack. These techniques for preventing DPA and related attacks fall roughly into three categories. Firstly, signal size can be reduced. Secondly, noise may be introduced into power consumption measurements. Another technique involves the use of nonlinear key update procedures [19].

Fault Generation Attacks. These attacks rely on stressing a smart card processor in order to make it perform illegal

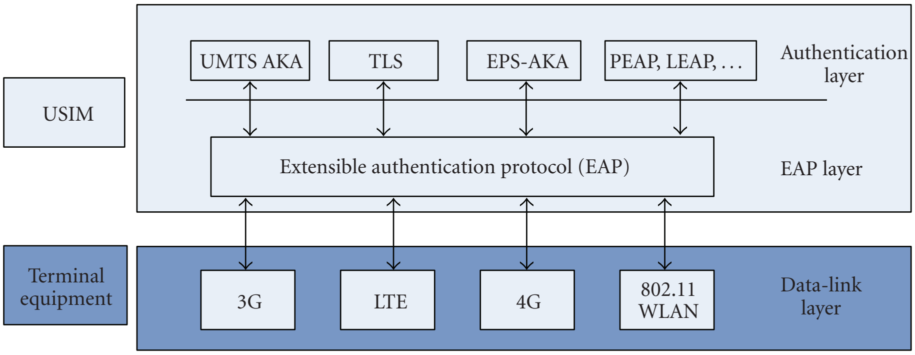

Figure 10: EAP framework in UE.

operations or give faulty results. Power and clock transients can be used to affect the decoding and execution of individual instructions. A possible countermeasure would be to remove completely the clock, transforming the smart card processors in self-timed asynchronous circuits [19].

5.2. Performance Analysis. Here, we mainly concern the influence of the proposed framework on existing authentication methods in the latency aspect. The authentication latency is made up of three parts which are (1) propagation latency, (2) transmission latency and (3) computation latency. In the following, we will analyze the influence resulting from the authentication framework in those three parts.

Propagation Latency. Comparing with 802.11i [13], the four-way handshake is unnecessary in our framework, because in order to be compatible with the existing message protection method for the air interface, we employ the keys of the original authentication protocol (such as the CK and IK of UMTS-AKA) rather than the keys derived from the four-way handshake. In addition, the original authentication protocol remains unchanged in the proposed framework and only three EAP messages are added that are EAPOL-Start, EAP-Request/Identity and EAP-Success, which can be shown by comparing UMTS-AKA (shown in Figure 3) with EAP-AKA (shown in Figure 5).

Transmission Latency. In the proposed framework, the message length will become longer because the EAP encapsulation is introduced. EAP header includes Code, Identifier, Length, and Type fields which length is 40 bits [23]. The bandwidth of UMTS is below 2 Mbps, such as 56 kbps, 64 kbps [24], therefore, the introduction of new transmission delay for each message is more than 0.02 ms. But for the LTE and 4G, their bandwidth is over 20 Mbps [25] and the resulting transmission latency can be neglected.

Computation Latency. In the new framework the computation of the protocol also retains unchanged, for example, the computation of EAP-AKA is same as that of UMTS-AKA. Therefore, the new framework does not introduce extra computation delay.

As a whole, for LTE and 4G, the extra authentication delay resulting from the new framework is the propagation delay of the three EAP messages (EAPOL-Start, EAP-Request/Identity and EAP-Success). While for UMTS, it should plus the extra transmission delays resulting from EAP header which is more than 0.02 ms for each EAP message.

To be more specific, in the following UMTS AKA is taken as an example to show this influence. Without the proposed framework, in UMTS UE has to run the UMTS AKA to authenticate with the core networks. While in our framework, UE will take use of the EAP-AKA to perform the authentication. In the following, we will compute the latency of EAP-AKA and UMTS AKA in the UMTS environment and compare them.

From [26], we can get that in 3G-WLAN interworking the authentication latency of EAP-AKA in nonroaming case is 1540.999 ms − 1038.016 ms = 502.983 ms, among which the calculation delay of AKA algorithm on the USIM is 78.46 ms where the USIM CPU is 3.25 MHz [27]. From this value, we can derive the latency of EAP-AKA in UMTS. The difference resulting from the communication environment will just affects the propagation latency and transmission latency. We think in propagation latency their difference can be neglected, because in the wired part (core network) they are same and in the air part the speed of the electromagnetic wave is so fast (almost $3 * 10^8$ m/s) that the propagation latency in this part can be neglected. Consequently, their only difference lies in the transmission latency in the air part where the total message amount is 2984 bits in EAP-AKA. In the 3G-WLAN interworking the bandwidth of WLAN is 11 Mbps, so the transmission latency is 0.271 ms. While in UMTS, its bandwidth is set as 2 Mbps, therefore, the transmission latency is 1.492 ms. Thus, the authentication latency of EAP-AKA in UMTS is 502.983 ms + (1.492 ms − 0.271 ms) = 504.204 ms. That is, with our proposed scheme, the latency of EAP-AKA in UMTS is 504.204 ms.

From the analysis above, we get that the latency of UMTS AKA should be 504.204 ms − 0.02 ms $*$ 6 = 504.084 ms, because there are 6 EAP messages in EAP-AKA.

From the results above, we can get that for the UMTS AKA, with our framework its authentication latency is almost same as the original one. These results are given in Table 1. For other authentication methods (such as the EPS AKA),

Table 1: Latency influence of the framework: UMTS AKA as an example.

UMTS AKA latency	Latency with our framework
504.084 ms	504.204 ms

their latencies are bigger and the influence of our framework can be neglected.

5.3. Superiority Analysis. Analysis indicates that the proposed uniform access authentication method has following advantages over the present one.

(1) Various authentication algorithms are integrated into USIM which can support access authentications in different wireless communication technologies. Not only the current 3G, LTE and WLAN but also the future 4G are taken into consideration. Therefore, even the terminal is updated (e.g., from LTE to 4G), USIM is unnecessary to be changed.

(2) Various authentication protocols are collectively managed by the media independent authentication layer, and any communication module in the terminal can uniformly call this layer to authenticate with the networks. In such a method, the independence between the authentication framework and communication modules is achieved. Then the operator can choose different protocols according to different users or scenarios (e.g., roaming or nonroaming scenario). In such a way, personalized and fine-grained services can be provided.

(3) The independence between the authentication framework and the underlying communication technologies enables the re-use of existing authentication protocols (e.g., EAP-TLS [28]), which reduces the possibility of developing new authentication protocols for emerging communication technologies.

(4) The key output of USIM is in the uniform form of (MSK, EMSK), which enables the manufactures of communication equipments to derive the expected keys according to the requirement of confidentiality and integrity. In this way, the functions of USIM and terminal equipment can be separated each other, which facilitates the USIM and equipment manufacturers to maintain and develop their own products, respectively.

(5) Unified management of authentication protocols makes them highly extensible, and the framework can add new authentication protocols according to the specific applications.

(6) It is convenient to update and easy to maintain the authentication protocols. When some a new authentication method needs to be added, just the media independent authentication layer needs to be updated. This can be realized through sending short messages to the terminal by the operator to update the USIM. In addition, its advantage over the legacy method lies in that the latter can just replace the old authentication protocol with a new one while our proposal can add a new protocol while retaining the existing ones, which can realize forward compatibility and enables the terminal and the operator to negotiate and choose a suitable protocol.

(7) This scheme not only is applicable for the terminal to access mobile communication networks, but also can provide the terminal WLAN or WiMAX access. In this case, the WLAN or WiMAX network card needs to interact with USIM and activates the EAP function module in USIM by the ”AUTHENTICATE” command. Afterwards, WPA-supplicant or X-supplicant agrees and implements an authentication protocol with the authentication server in WLAN or WiMAX, which procedure is same as the one in Figure 9. That is, using our proposal, USIM enables the UE to access the mobile core networks, WLAN and WiMAX in a uniform authentication method.

From the analysis above, it can be seen that the proposed framework overcomes the drawbacks mentioned in Section 1.

6. Related Work

As digital convergence slowly becomes a reality, the cellular operators have started to offer an increasing number of new services for users. For each service the user is going to use he has to have credentials, therefore, he has to manage a lot of credentials, which is a burden for him [29]. The Generic Authentication Architecture (GAA) is 3GPP’s solution to the aforementioned problems [30]. It provides fresh key material for clients and servers that require shared secret based authentication, and signs certificates for those applications which require asymmetric authentication. The users’ equipments authenticate themselves to the operator’s GAA service by existing 3G or 2G authentication protocols, and in the process receive new keys. Also the services, which the users want to use, are able to fetch them from GAA. In such a way, the clients and servers are able to share secrets [31]. In addition to other services, the method described above can also be used to authenticate clients to a public key infrastructure, which can then be asked to sign certificates for the client’s public key(s) [32].

Kim et al. [33] first proposed a fast handover authentication mechanism based on context transfer which enables a multimode terminal to get a seamless service across the heterogeneous networks. And a unified authentication scheme among various FMC (Fixed Mobile Convergence) networks is presented which enables UE to gain service layer authentication using the single-sign-on access authentication and fast handover authentication.

In the above two works, they are concerned about the unified or general authentication in the service layer, that is, after UE gets access to the networks and demands some services their authentication methods will work. While our scheme mainly focuses on the initial access authentication.

In WLAN, there are two security standards which are IEEE 802.11i and China’s WAPI. They are incompatible with each other, which will bring about a series of issues related with the deployment and implementation. In order to solve this problem, Li et al. [34] proposed a scheme that is compatible with both standards. First, the authentication participators in WAPI which are the mobile node and the access point (AP) are changed into the mobile node and the authentication server, while the framework and protocol itself retain unchanged. And then, the modified WAPI is introduced into the EAP framework as a specific authentication method. Through the change of WAPI and then introduction of it into the EAP framework, UE can support both of them and it can negotiate with the networks and select one when performing the access authentication. This method is similar to our proposed framework, but the difference lies in that UE in ours is multimode which can support various communication technologies and different authentication methods are integrated into USIM card.

In the BcN (Broadband Convergence Netowrk), there are many authentication mechanisms which are different from each other. Therefore, there is a strong requirement for unified authentication. Lee et al. [35] proposed a unified authentication scheme for BcN wherein an AAA core-broker is positioned in the core network and manages the information for the authentication of the mobile nodes. When the mobile node detects a new access network, the information of the new access network is sent to the AAA core-broker which performs the pre-authentication of the mobile node with the AAA server of the new access network. When the mobile node moves into the new access network, a fast authentication procedure can be implemented locally. With the proposed scheme, low latency authentication operations can be achieved. This work seems to provide a sound unified authentication scheme. But in fact, it does not. Because when UE performs the Initial-Authentication, it has to authenticate with the authentication server in the initial access networks. But when the initial access networks changes, what shall UE do? The paper did not mention it. If UE employs another authentication protocol for the new initial access networks, then it is not a unified authentication scheme; otherwise, UE will use the same authentication protocol, that is, no matter what kind of access network, UE will take use one authentication protocol, which is not realistic or unfeasible.

Kambourakis et al. [36] points out that a drawback of the existing AKA procedure is that they are dependent on the underlying network infrastructure and cannot offer a dynamic and flexible authentication and key agreement mechanism. Thus, in the next-generation mobile environments more flexible, dynamic and scalable security mechanisms are desired. And two SSL-based authentication procedures are proposed. The first one is the AKA based on SSL where UE and SGSN run SSL to authenticate each other and then SGSN updates UE's location to HSS. The second one is the AKA based on EAP-TLS which is used for the 3G (or beyond 3G)-WLAN interworking. In this procedure, UE and the AAA server in its home networks run EAP-TLS to authenticate each other. We do not think this scheme is suitable for 3G and beyond 3G. First, at present the public key infrastructure is still not sound and it will take some time to establish them. Secondly, SSL involves the public key operation which is not suitable for the resource-limited mobile terminal. Thirdly, we do not think one specific authentication protocol is suitable for future heterogeneous wireless environments. Instead, a framework that can support various authentication methods is more advisable.

7. Conclusion

First, the drawbacks of the USIM-based authentication method in the current mobile communication are presented. And we point out the fundamental reason is that USIM just supports one authentication algorithm AKA which is not extensible, furthermore it cannot provide the independence between the authentication framework and underlying communication technologies. Consequently, current authentication method cannot fulfill the requirements of the future mobile communications. In order to overcome the drawbacks, a uniform access authentication framework is proposed. Taking use of the EAP, a media independence authentication layer is introduced in USIM which collectively manages various authentication protocols. In such a way, the framework is extensible and the independence between the authentication framework and underlying communication technologies is also achieved, which enables USIM and the networks server to negotiate and run a suitable authentication protocol according to the specific scenario and output keys in a unified format. In the terminal, a key adaptation layer is added which transforms the output keys to the format that the corresponding communication module can accept. Our analysis indicates that the proposed method has obvious advantage over the present one.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (60702059, 61072066, 60972078), the Key Program of National Natural Science Foundation of China (60633020), the Fundamental Research Funds for the Central Universities, Mobile Network Security Technology Research Center of Kyungpook National University, the Opening Foundation of Key Lab of Cryptglogic Technology and Information Security, Ministry of Education, Shandong University, and funds of Key Lab of Fujian Province University Network Security and Cryptology (09A001).

References

[1] "Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN)," 3GPP TR 25.913, 2006, http://www.3gpp.org/ftp/specs/html-info/25931.htm.

[2] "System architecture evolution: report on technical options and conclusions," 3GPP TR 23.882 v1.9.0, 2007, http://www.3gpp.org/ftp/specs/html-info/23882.htm.

[3] "Digital Cellular Telecommunications System (Phase 2+); SecurityRelated Network Functions (Release 5)," 3GPP TS 43.020 v5.3.0, 2007, http://www.3gpp.org/ftp/specs/html-info/43020.htm.

[4] "3G Security; Security architecture (Release 9)," 3GPP TS 33.102 v9.1.0, 2009, http://www.3gpp.org/ftp/specs/html-info/33102.htm.

[5] "3GPP System Architecture Evolution (SAE); Security architecture (Release 8)," 3GPP TS 33.401 V8.1.1, 2008, http://www.3gpp.org/ftp/specs/html-info/33401.htm.

[6] J. Arkko and H. Haverinen, "EAP-AKA authentication," IETF RFC 4187,2006.

[7] "Ratioale and Track of Security decision in Long Term Evolved (LTE)RAN/3GPP System Architecture Evolution (SAE)(Release 8)," 3GPP TR33.821 V8.0.0, 2009, http://www.3gpp.org/ftp/specs/html-info/33821.htm.

[8] Y. Wang, D.-W. Gu, and Y.-C. Bai, "Public key based uniform access framework in 3G systems," *Journal of Harbin Institute of Technology*, vol. 13, no. 4, pp. 404–408, 2006.

[9] D. He, J. Wang, and Y. Zheng, "User authentication scheme based on self-certified public-key for next generation wireless network," in *Proceedings of the IEEE International Symposium on Biometrics and Security Technologies (ISBAST '08)*, pp. 1–8, 2008.

[10] G. Kambourakis, A. Rouskas, and S. Gritzalis, "Performance evaluation of public key-based authentication in future mobile communication systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2004, no. 1, pp. 184–197, 2004.

[11] "System Architecture Evolution: Report on Technical Optionsand Conclusions," 3GPP TR23.882, 2005, http://www.3gpp.org/ftp/specs/html-info/23882.htm.

[12] S. Patel, "Analysis of EAP-SIM session keys agreement," 2003, http://www6.ietf.org/proceedings/57/slides/eap-11.pdf.

[13] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol(EAP)," IETF RFC 2284, 1998.

[14] "Medium Access Control (MAC) Security enhancements, Amendment 6 to 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 Std. 802.11i-2004, 2004, http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9214.

[15] http://hostap.epitest.fi/wpa_supplicant/.

[16] http://open1x.sourceforge.net/.

[17] "Smart Cards;UICC-Terminal interface; Physical and logical characteristics (Release 8)," 3GPP TS 102.221, v8.2.0, 2009, http://www.3gpp.org/ftp/specs/html-info/102221.htm.

[18] J. Vollbrecht, P. Eronen, N. Petroni, and Y. Ohba, "State Machines forExtensible Authentication Protocol (EAP) Peer and Authenticator," IETFRFC 4137, 2005.

[19] N. Boudriga, "Security of mobile communications," in *Proceeding of the International Conference on Signal Processing and Communications (ICSPC '07)*, 2007.

[20] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysisand related attacks," 1998, http://www.cryptography.com/dpa/technical.

[21] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of power analysis attacks on smartcards," in *Proceedings of the USENIX Workshop on Smartcard Technology*, pp. 151–162, 1999.

[22] J.-J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): measures and couter-measures for smart cards," in *Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security (E-smart '01)*, pp. 200–210, 2001.

[23] T. Clancy and W. Arbaugh, "Extensible Authentication Protocol (EAP) Password Authenticated Exchange," IETF RFC 4746, 2006.

[24] A. Klemm, C. Lindemann, and M. Lohmann, "Traffic modeling and characterization for UMTS networks," in *Proceeding of the Global Telecommunications Conference (GLOBECOM '01)*, vol. 3, pp. 1741–1746, 2001.

[25] "Feasibility study for Further Advancements for E-UTRA (LTEAdvanced)," 3GPP TR 36.912, 2010, http://www.3gpp.org/ftp/specs/html-info/36912.htm.

[26] X. Li, X. Lu, J. Ma, Z. Zhu, L. Xu, and Y. Park, "Authentications and key management in 3G-WLAN interworking," *Mobile Networks and Applications*. In press.

[27] "Report on the Design and Evaluation of the MILENAGE AlgorithmSet; Deliverable 5: An Example Algorithm for the 3GPP Authenticationand Key Generation Functions (Release 4)," 3GPP TR 33.909, v4.0.1, 2001, http://www.3gpp.org/ftp/specs/html-info/33909.htm.

[28] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS authentication protocol," IETF RFC 5216, 2008.

[29] P. Laitinen, P. Ginzboorg, N. Asokan, S. Holtmanns, and V. Niemi, "Extending cellular authentication as a service," in *Proceeding of the 1st IEE International Conference on Commercialising Technology and Innovation*, pp. d2/1–d2/4, 2005.

[30] "Generic Authentication Architecture (GAA); System description," 3GPP TR 33.919, 2006, http://www.3gpp.org/ftp/Specs/html-info/33919.htm.

[31] "Generic Authentication Architecture (GAA); Generic bootstrapping architecture," 3GPP TS 33.220, 2006, http://www.3gpp.org/ftp/Specs/html-info/33220.htm.

[32] "Generic Authentication Architecture (GAA); Support for subscriber certificates," 3GPP TS 33.221, 2006, http://www.3gpp.org/ftp/Specs/html-info/33221.htm.

[33] K. Kim, H.-W. Lee, S.-K. Jo, and W. Ryu, "Design of unified authenticationfor multi-mode terminal between service and access network inNGN," in *Proceeding of the 10th International Conference on Advanced Communication Technology (ICACT '08)*, pp. 1288–1292, 2008.

[34] X. Li, J. Ma, and S. Moon, "A new authentication scheme compatiblewith 802.11i and WAPI," in *Proceeding of the International Conferenceon Complex Systems and Applications (ICCSA '07)*, pp. 218–223, 2007.

[35] J. Lee, M. Yu, S. Choi, T. Jeong, and S. Kang, "A new scheme for unified-authentication in BcN," in *Proceeding of the 9th International Conference on Advanced Communication Technology*, pp. 1795–1799, 2007.

[36] G. Kambourakis, A. Rouskas, and S. Gritzalis, "Experimental analysis of an SSL-based AKA mechanism in 3G-and-beyond wireless networks," *Wireless Personal Communications*, vol. 29, no. 3-4, pp. 303–321, 2004.