Light-Weight Authentication and Key Exchange Protocols with Forward Secrecy for Digital Home

Chun-I Fan*, Tsung-Pin Chiang, and Ruei-Hau Hsu

Department of Computer Science and Engineering

National Sun Yat-sen University

Kaohsiung, Taiwan, ROC

*cifan@cse.nsysu.edu.tw vanix0924@gmail.com xyzhsu@gmail.com

Received 1 April 2007; Revised 27 April 2007 ; Accepted 1 June 2007

Abstract. In this paper we propose a complete solution of authentication and key exchange for digital home environments such that mobile devices can securely access the home devices. Some digital home authentication and key exchange protocols performed between mobile devices and home gateways are assisted by the AAA servers, which are provided by telecommunication companies, but they have some security flaws. In our proposed protocol, the necessary security requirements for digital home security mechanisms are satisfied, such as mutual authentication, authenticated key exchange, and forward secrecy. In our digital home security scheme, a mobile device can authenticate his home gateway and exchange a session key with each home device without pre-sharing keys with the home gateway and with the home device. The proposed authentication and key exchange protocol can also cooperate with the AAA server. Furthermore, we propose another authentication and key exchange protocol with forward secrecy between mobile devices and home devices. The computation capabilities of the mobile devices also are considered in our proposed protocols, where we only employ symmetric encryption/decryption and low-cost operations in order to reach the aim of light-weight computation cost.

Keywords: identity authentication, key exchange, forward secrecy, security protocols, digital home

1 Introduction

Nowadays, a new idea, digital home, is brought up. It is in order to provide more convenient and more integrated environments for householders. Therefore, digital home has received significant attentions in recent years. It was proposed that every user can use his mobile equipment or device to remotely connect the home network and then use the in-home applications further [10]. Moreover, Digital Living Network Alliance (DLNA) focuses on integrating technologies of all DLNA member companies into open industry standards related to the domain of digital home.

In digital home security, most related papers [7, 11, 12] make use of S/Key [5] to ensure identity authentication without addressing some other security issues, like key exchange and content privacy. It is more important that none of them defines the detailed framework of digital home, and they illustrated the components of the framework incompletely.

You and Jung [12] proposed a light-weight authentication protocol for digital home networks to improve Lee-Chen scheme [7] in 2006. Most parts of this scheme are the same as those of Lee-Chen scheme. Especially, the proposed method can withstand an attack, called the compromise of pass session keys via stolen passwords. However, there is not any discussion about key exchange in You-Jung scheme.

You's scheme [11] is extended from You-Jung scheme [12]. You's scheme does not only provide authentication but also authorization services. In order to reach the goal, a Lightweight Attribute Certificate (LAC) and Lightweight Authorization Protocol (LAP) were proposed by You. However, this scheme needs much more computation cost such that it is not suitable for mobile equipments or devices which only have limited computation capabilities.

Jeong, Chung, and Choo [6] do not employ S/Key to design their scheme. They adopt public-key systems and integrate trusted third parties into the design of their scheme. The computation ability of a mobile equipment or device is not enough to fit the proposed security environment of digital home since it adopts public-key cryptosystems. In addition, this scheme has another problem. It is possible that the session keys between a user and the AAA server can be obtained by attackers because that the offline dictionary attack is valid in the scheme.

* Correspondence author

The security of S/Key relies on the difficulty of reversing cryptographic one-way hash functions and secrets which are shared between a user and the authentication server. However, S/Key cannot withstand the man-in-the-middle attack. On the other hand, some researchers also utilize public-key cryptosystems to design their authentication schemes for digital home, and some combine S/Key with public-key cryptosystems. Nevertheless, there are still weaknesses in these schemes, such as high computation cost and vulnerability to the offline dictionary attack [11].

Digital home contains some security issues, such as identity authentication and key exchange. Some ideas were first provided by You's scheme [11] and Jeong-Chung-Choo scheme [6], including the concept of out-home networks and in-home networks, and the access control lists. Digital home security mechanism should not provide identity authentication only. It also needs to cover key exchange between a user and a home device since the user may remotely access the home device after passing identity authentication. Therefore, it is necessary to integrate key exchange mechanisms into digital home environments. How can the user be authenticated by the home gateway and share keys with the home gateway without pre-sharing any common secret? It is possible that the user communicates with the home gateway through the assistance of telecommunication companies. Telecommunication companies have some capabilities, such as managing users' information, confirming users' identities, and so on. Therefore, we assume that the telecommunication companies act as trusted third parties (TTP) which can assist our protocol to verify users' identities. We also consider several important security properties, such as forward secrecy and content privacy. Forward secrecy ensures that the past session keys will not be derived even if the long-term keys are revealed. It can greatly reduce the damages resulting from the reveal of long-term secrets.

The rest of the paper is organized as follows. Section 2 will review Jeong-Chung-Choo scheme [6] and Section 3 will present the architecture of digital home. In Section 4, we describe our basic ideas about the design of the security protocols for digital home. Our proposed protocol is shown in Section 5. Finally, Section 6 contains the discussions of the proposed protocols and a remark concluding is given in Section 7.

2 Jeong-Chung-Choo Scheme

Jeong-Chung-Choo scheme was proposed in 2006 [6], which is different from the schemes based on S/Key. In the authentication phase of the scheme, a user is authenticated by TTP, such as Integrated Authentication Server (IAS) or the Authentication Authorization Accounting (AAA) server. It means that the home gateway does not need to authenticate the user, and it only verifies the user's ticket which is generated by the AAA server.

Notations. The notations used in Jeong-Chung-Choo scheme are summarized as follows.

Table 1. Notations of Jeong-Chung-Choo scheme

U	the user
AAA	the Authentication Authorization Accounting server
HGW	the home gateway
R_1	$R_1 = h(U_{ID}, Password)$ which is computed by AAA
R_2	a random string generated by AAA
$E_{P\text{-}AAA}()$	an encryption using AAA's public key
S_{key}	$S_{key} = h(R_1, R_2)$ which is a shared session key between U and HGW
U_{ID}	the identifier of U
AAA_{ID}	the identifier of AAA
$E_{AAA\text{-}HGW}()$	an encryption using a symmetric key shared between AAA and HGW
$E_K()$	an encryption using key K
T	a timestamp to decide the validation of a session key

The Proposed Authentication Scheme.

(Step1) U → AAA: U_{ID}, $E_{P\text{-}AAA}(h(Password))$

(Step2) U ← AAA: $E_{R_1}(AAA_{ID}, U_{ID}, R_2, h(S_{key}, U_{ID}), T)$, $E_{AAA\text{-}HGW}(U_{ID}, AAA_{ID}, R_1, R_2, T)$

(Step3) U → HGW: $E_{AAA\text{-}HGW}(U_{ID}, AAA_{ID}, R_1, R_2, T)$, $E_{S_{key}}(U_{ID}, Services)$

(Step4) U ← HGW: $E_{S_{key}}(R_1)$

The user first communicates with AAA in order to prove the validity of his identity. If the user identity is valid, AAA will reply an authentication ticket which contains $E_{\text{AAA-HGW}}(U_{ID}, AAA_{ID}, R_1, R_2, T)$ and $E_{R_1}(AAA_{ID}, U_{ID}, R_2, h(S_{key}, U_{ID}), T)$. The user can decrypt $E_{R_1}(AAA_{ID}, U_{ID}, R_2, h(S_{key}, U_{ID}), T)$ to get R_2 and further compute $S_{key} = H(R_1, R_2)$. Then, the user sends the authentication ticket and $E_{S_{key}}(U_{ID}, Services)$ to request the services. The identity information of the services are encrypted by the session key S_{key}. The home gateway can get R_2 from the ticket $E_{\text{AAA-HGW}}(U_{ID}, AAA_{ID}, R_1, R_2, T)$ and obtain the session key by computing $h(R_1, R_2)$. Finally, the home gateway replies $E_{S_{key}}(R_1)$ to the user in order to notify the user that the login authentication is successful. Nevertheless, an attacker can engage in the offline dictionary attack to obtain the session key shared between the user and the home gateway. The attacker first intercepts $E_{R_1}(AAA_{ID}, U_{ID}, R_2, h(S_{key}, U_{ID}), T)$ and then performs the dictionary attack to attempt to decrypt $E_{R_1}(AAA_{ID}, U_{ID}, R_2, h(S_{key}, U_{ID}), T)$. The attacker then can check the correctness of AAA_{ID} and U_{ID} to examine whether the decryption is successful or not.

3 The Architecture of Digital Home

In this section we give some assumptions and describe the functionalities of each component in digital home environments in order to provide a complete security mechanism. Digital home allows users to perform out-home accesses where the users can use mobile devices to control their home appliances, such as video recorders, televisions, monitors, and personal computers, i.e., the users can take their own mobile devices to control the home devices. For examples, the users remotely control monitors to deliver images to them and remotely control their personal computers to send mails. The system of digital home contains mobile equipments, service providers, a home gateway, home appliances, and an authentication server. Mobile equipments are used to connect the home gateway and further control the home appliances by the holders. We will describe the functionalities and assumptions of each component in digital home in the following subsections.

3.1 The Components of Digital Home

Now we will briefly depict each component and its functionality in digital home environments as follows.

Mobile Equipments (User Equipments, UE). They must be authenticated before accessing home appliances. Users can control their mobile equipments to access home devices and the home gateway via communication networks.

Home Gateway (HG). This component is the only entry of the digital home. Before user equipment communicates with a home device, it is necessary for the home gateway to verify the identity of the user equipment.

Home Appliances (Home Devices, HD). The concept of digital home is to remotely control the devices, named home appliances, in home. What are the home appliances? There are some examples such as TVs, PCs, and monitors. They can be controlled by the authenticated users. Therefore, we must assume that the home appliances possess the abilities to deal with some complex commands which are assigned by the users.

The AAA Server: The Authentication Authorization Accounting Server. The main work of the AAA server is to perform the authentication for the users registered in telecommunication companies. In digital home applications, we assume that the AAA server shares some common secret information with each of UE and HG for performing authentication and key exchange with each of them.

Service Providers. Service providers supply many kinds of services, such as e-health, music, and other network services, for digital home users. It means that digital home will support these kinds of services for the users.

The architecture of digital home is shown in Figure 1.

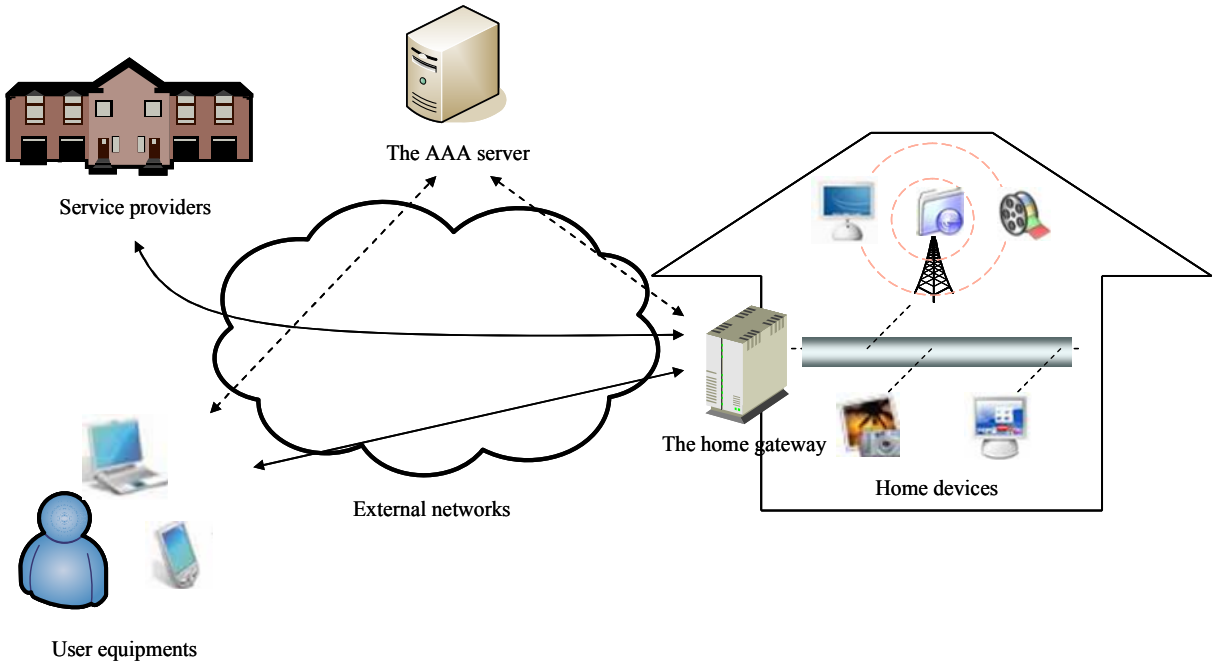

Fig. 1. The structure of digital home

3.2 Assumptions for Digital Home

The computation cost of components. The computation cost is an important factor in digital home security mechanisms and it will affect the design of authentication and key exchange protocols and the selection of cryptographic algorithms. User equipments have lower computation power. Only symmetric cryptographic algorithms can be performed in user equipments. Home devices are more powerful than user equipments. Therefore, some more complex algorithms can be performed by home devices, such as the RSA encryption and decryption, the Rabin [8] decryption and modular exponentiation computations. We also assume that the home gateway has the same computation ability as that of a home device. The only difference is that the home gateway can process multiple authentication and key exchange requests.

Secure and insecure regions. Our proposed protocol can be divided into several parts. The division between user equipment and the AAA server, the division between the user equipment and the home network, and the division between the AAA server and the home network are all in the internet which is an open network environment. Therefore, these three divisions must be protected by robust security mechanisms. On the other hand, the division inside the home can be assumed to be a secure region. It means that there is a secure channel between the home gateway and each home appliance.

Pre-sharing keys between components. Due to the aim of mutual authentication and key exchange, we assume that the SIM card of the user equipment pre-shares the $K_{\text{UE-AAA}}$ key with the AAA server and the AAA server must pre-share the $K_{\text{AAA-HG}}$ key with the home gateway. The two keys can assist us in accomplishing the goal of mutual authentication and key exchange between UE and HG.

Figure 2 illustrates the assumptions and the environments of digital home. It indicates the status of key-sharing in digital home.

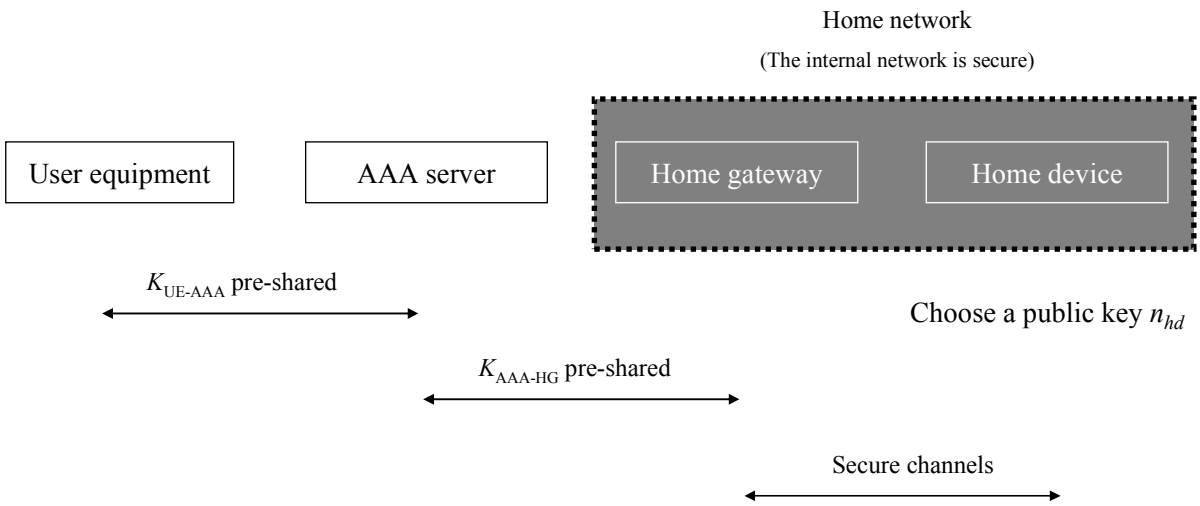

Fig. 2. The assumptions of digital home

4 Basic Ideas and Contributions of Our Proposed Scheme

4.1 Basic Ideas

Complete Authentication and Key Exchange Mechanisms with Low Cost Computation in Digital Home. We consider the authentication and key exchange protocol not only between UE and HG but also between UE and HD. The authentication and key exchange protocol between UE and HD has never been discussed before. The computation cost also needs to be considered when UE are low-computation mobile devices. Thus, we utilize Rabin's encryption algorithm in the authentication and key exchange protocol between UE and HD, because that the computation cost of Rabin's encryption is much lower than that of other public-key encryptions. The Rabin encryption can be performed on UE in order to achieve forward secrecy with low computation.

Integration of the AKA Standard. Most proposed schemes adopt S/Key and public key cryptosystems to reach their goals of mutual authentication and key exchange between UE and HG. However, some proposed protocols cannot still provide mutual authentication with low computation. We will propose an authentication and key exchange protocol which integrates AKA [2] standard into the mutual authentication and key exchange protocol between UE and HG. We just need only few alterations in AKA to adapt to our protocol. Moreover, the major benefit of integrating AKA standard into our scheme is the high compatibility with some standard environments, such as GSM, 3G, and 4G.

Forward Secrecy. We provide the property of forward secrecy by means of Rabin's encryption algorithm in the authentication and key exchange protocol between UE and HD. Each of UE and HD randomly generates a number to construct a session key. Our design philosophy is that we make use of a public-key algorithm to protect the random numbers. In the key exchange protocol, it is necessary to utilize some long-term secret information to protect the random numbers, which are produced by UE and HD, for producing session keys. If the utilization of the secret information, which is used to protect the random numbers, is in a symmetric way, the loss of the secret information will cause that attackers can gain the past session keys. In our protocol, we do not have such problems because that we adopt Rabin's encryption to protect these random numbers. The Rabin encryption algorithm has a good property that the encryption process just only needs one modular multiplication. If we adopt Rabin's encryption in UE and the corresponding decryption in HD, it will suffice our assumptions.

4.2 Contributions

Complete Authentication and Key Exchange Mechanisms. There are some researchers who have designed mutual authentication and key exchange mechanisms between UE and HG in their protocols. However, there is no discussion about the phase of mutual authentication and key exchange between UE and HD. This phase is necessary for the digital home security environment since users must access their home devices after passing the authentication processes of the home gateway. In the proposed scheme, we will design not only a mutual authentication and key exchange phase between UE and HG but also a mutual authentication and key exchange phase between UE and HD.

The Property of Low Computation. One component of our scheme is the mobile equipment which is with limited computation capabilities. We will adopt low-computation encryption operations, i.e., a symmetric encryption and Rabin's encryption, in order to reduce the computation cost of the user. We also successfully integrate the AKA standard into our scheme to reach the goal of low computation for the user because that all operations in the AKA standard are quite efficient.

Implementation in Standard Environments. One of the major features of our proposed scheme is to integrate the AKA standard into our scheme. We can implement the proposed scheme in standard environments. It means that our scheme can be integrated into standard environments and we can adopt multiplex authentication standards widely, such as 802.1X. For example, EAP [3] (Extensible Authentication Protocol) is an authentication framework and it contains various authentication and key exchange solutions, such as EAP-AKA [4], where it can also be integrated into our scheme. The proposed scheme can be adapted and implemented in several popular standard environments.

5 The Proposed Scheme

If a user decides to access his home network, it will be necessary for the user to be authenticated before accessing the network. Therefore, we focus on identity authentication, key exchange, and some important properties, such as light-weight cost and forward secrecy. Our proposed scheme is composed of two phases: the authentication and key exchange phase between UE and HG and the authentication and key exchange phase between UE and HD. We make use of the standard authentication and key exchange protocol for 3G to construct our first phase of authentication and key exchange. Hence, we will introduce the 3G standard authentication and key exchange protocol and then describe our scheme.

5.1 The Authentication and Key Agreement Protocol for UMTS

We give a brief description about the AKA (Authentication and Key Agreement) protocol of 3GPP in this subsection [2]. The AKA protocol contains three participants: Mobile Station (MS), Serving Network (SN), and Home Network (HN). MS shares a secret key K and some cryptographic algorithms with HN. They share cryptographic algorithms, including message authentication code functions $f1$ and $f2$ and key generation functions $f3$, $f4$, and $f5$. These functions can generate MAC, $XMAC$, RES, and $XRES$ in order to verify the messages and identities. In addition, HN maintains a sequence number (SQN_{HN}) for each mobile user, and MS maintains a sequence number (SQN_{MS}). The AKA protocol is shown in Figure 3.

MS first sends the request of authentication to HN through SN. HN performs some operations as shown in Figure 3 to generate $RAND_i$, $XRES_i$, CK_i, IK_i, AK_i, $AUTH_i$, and MAC_i after HN got IMSI of MS. HN generates the array of authentication vectors (AVs) where each AV has five components, such as a random number $RAND_i$ choosen by HN, an expected response $XRES_i = f2_K(RAND_i)$, a cipher key $CK_i = f3_K(RAND_i)$, an integrity key $IK_i = f4_K(RAND_i)$, and an authentication token $AUTH_i$. HN will distribute AVs to SN via a secure channel. SN stores AVs and assists HN in authenticating MS after SN got AVs.

SN returns $RAND_i$ and $AUTH_i$ to MS. Upon receiving these messages, SN gets $SQN_{HN}i$ by computing $f5_K(RAND_i) \oplus AK_i \oplus SQN_{HN}i$. SN must verify the freshness of $SQN_{HN}i$ and check whether $SQN_{HN}i > SQN_{MS}i$ or not. If the verification fails, MS will reject the connection. If the verification is successful, MS computes $XMAC_i$ and checks the correctness of MAC_i. If it is correct, MS generates CK_i, IK_i, AK_i, and $RES_i = f2_K(RAND_i)$. Then, MS sends RES_i to SN in order to let SN be able to check if RES_i is equal to $XRES_i$. If the check is passed, the authentication process is successful.

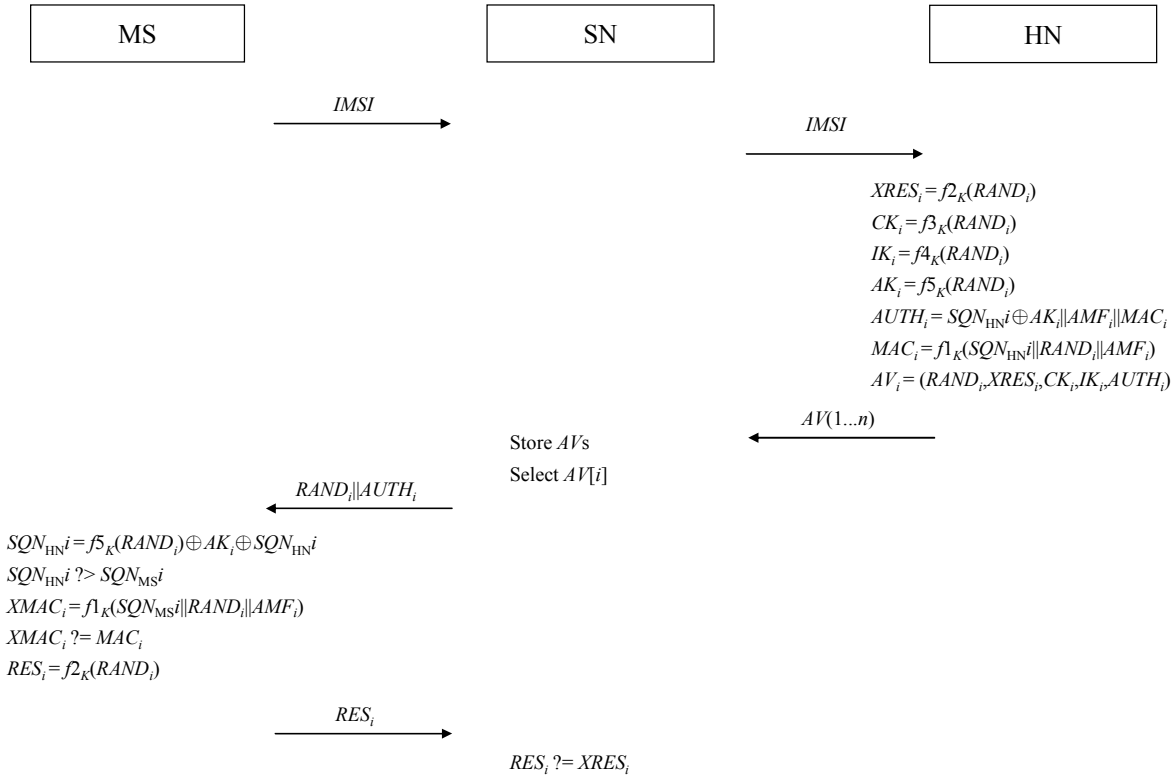

Fig. 3. The AKA protocol

5.2 Mutual Authentication and Key Exchange Phase between UE and HG

We slightly modify the AKA [2] protocol to fit our scheme since the protocol has been widely used for authentication and session key distribution in the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM). The proposed authentication and key exchange protocol between UE and HG and some required notations are described as follows.

Notations. The notations used in the first phase of our scheme are summarized as follows.

Table 2. Notations of the protocol in Section 5.2

$IMSI$	international mobile subscriber identity
$RAND_{HG}$	a random number generated by the home gateway
$RAND_{UE}$	a random number generated by the user equipment
$K_{AAA\text{-}HG}$	a pre-shared symmetric key between AAA and HG
$K_{UE\text{-}AAA}$	a pre-shared symmetric key between UE and AAA
$f()$	a key generating function for computing CK
$CK_{AAA\text{-}HG}$	a cipher key between AAA and HG
$CK_{UE\text{-}AAA}$	a cipher key between UE and AAA
$E_K()$	an encryption using key K
$SK_{UE\text{-}HG}$	a shared short-term session key between UE and HG
$H()$	a one-way hash function
$AKA\ PARAM_{AAA\text{-}HG}1$	parameters generated and used by AKA between AAA and HG
$AKA\ PARAM_{AAA\text{-}HG}2$	parameters generated and used by AKA between AAA and HG
$AKA\ PARAM_{UE\text{-}AAA}1$	parameters generated and used by AKA between UE and AAA
$AKA\ PARAM_{UE\text{-}AAA}2$	parameters generated and used by AKA between UE and AAA

The Protocol.

(Step 1) A user equipment → the AAA server: *IMSI*

A user equipment sends *IMSI* to the AAA server in order to request authentication and key exchange. The AAA server will relay *IMSI* to the home gateway after it got the message.

(Step 2) The AAA server → The home gateway: *IMSI*

The AAA server relays *IMSI* to the home gateway. Then, the AKA protocol will be performed twice. One is between the home gateway and the AAA server and another is between the AAA server and the user equipment.

(Step 3) The AAA server ← The home gateway: $AKA\ PARAM_{\text{AAA-HG}}1$, $RAND_{\text{HG}}$

When the home gateway got *IMSI*, it will perform the AKA protocol with the AAA server in order to reach the goal of mutual authentication between the home gateway and the AAA server. Therefore, the home gateway will generate the AKA parameters which are used to perform mutual authentication with the AAA server. It also chooses a random number $RAND_{\text{HG}}$ and computes $CK_{\text{AAA-HG}} = f_{K_{\text{AAA-HG}}}(RAND_{\text{HG}})$ which is used to generate a session key in the AKA protocol.

(Step 4) The user equipment ← the AAA server: $AKA\ PARAM_{\text{UE-AAA}}1$, $RAND_{\text{HG}}$

The AAA server will verify the AKA parameters after getting these parameters. If the parameters are valid, the AAA server will generate the AKA parameters between AAA and UE in order to mutually authenticate the user equipment. It also computes $CK_{\text{UE-AAA}} = f_{K_{\text{UE-AAA}}}(RAND_{\text{HG}})$. Finally, the AAA server sends the AKA parameters and $RAND_{\text{HG}}$ to the user equipment.

(Step 5) The user equipment → the AAA server: $AKA\ PARAM_{\text{UE-AAA}}2$, $E_{CK_{\text{UE-AAA}}}(RAND_{\text{UE}})$

The user equipment first verifies the AKA parameters between AAA and UE. It chooses $RAND_{\text{UE}}$ which will be used to generate $SK_{\text{UE-HG}} = H(RAND_{\text{UE}} \oplus RAND_{\text{HG}})$. It also computes $CK_{\text{UE-AAA}} = f_{K_{\text{UE-AAA}}}(RAND_{\text{HG}})$ to protect $RAND_{\text{UE}}$ through $E_{CK_{\text{UE-AAA}}}(RAND_{\text{UE}})$. Finally, the user equipment sends the AKA parameters between the AAA server and UE and $E_{CK_{\text{UE-AAA}}}(RAND_{\text{UE}})$ to the user equipment.

(Step 6) The AAA server → the home gateway: $AKA\ PARAM_{AAA\text{-}HG}2$, $E_{CK_{\text{AAA-HG}}}(RAND_{\text{UE}})$

The AAA server first verifies the identity of UE via the AKA parameters. If it is valid, the mutual authentication between AAA and UE will be successful. The AAA server will decrypt $E_{CK_{\text{UE-AAA}}}(RAND_{\text{UE}})$ and further compute $E_{CK_{\text{AAA-HG}}}(RAND_{\text{UE}})$. Finally, the AAA server transmits the AKA parameters between HG and AAA and $E_{CK_{\text{AAA-HG}}}(RAND_{\text{UE}})$ to the home gateway. The home gateway will verify the identity of the AAA server by the AKA parameters. If it is valid, the mutual authentication between HG and AAA is successful. We can get $RAND_{\text{UE}}$ from $E_{CK_{\text{AAA-HG}}}(RAND_{\text{UE}})$ in order to generate $SK_{\text{UE-HG}} = H(RAND_{\text{UE}} \oplus RAND_{\text{HG}})$. Therefore, the user equipment and the home gateway share a session key $SK_{\text{UE-HG}}$.

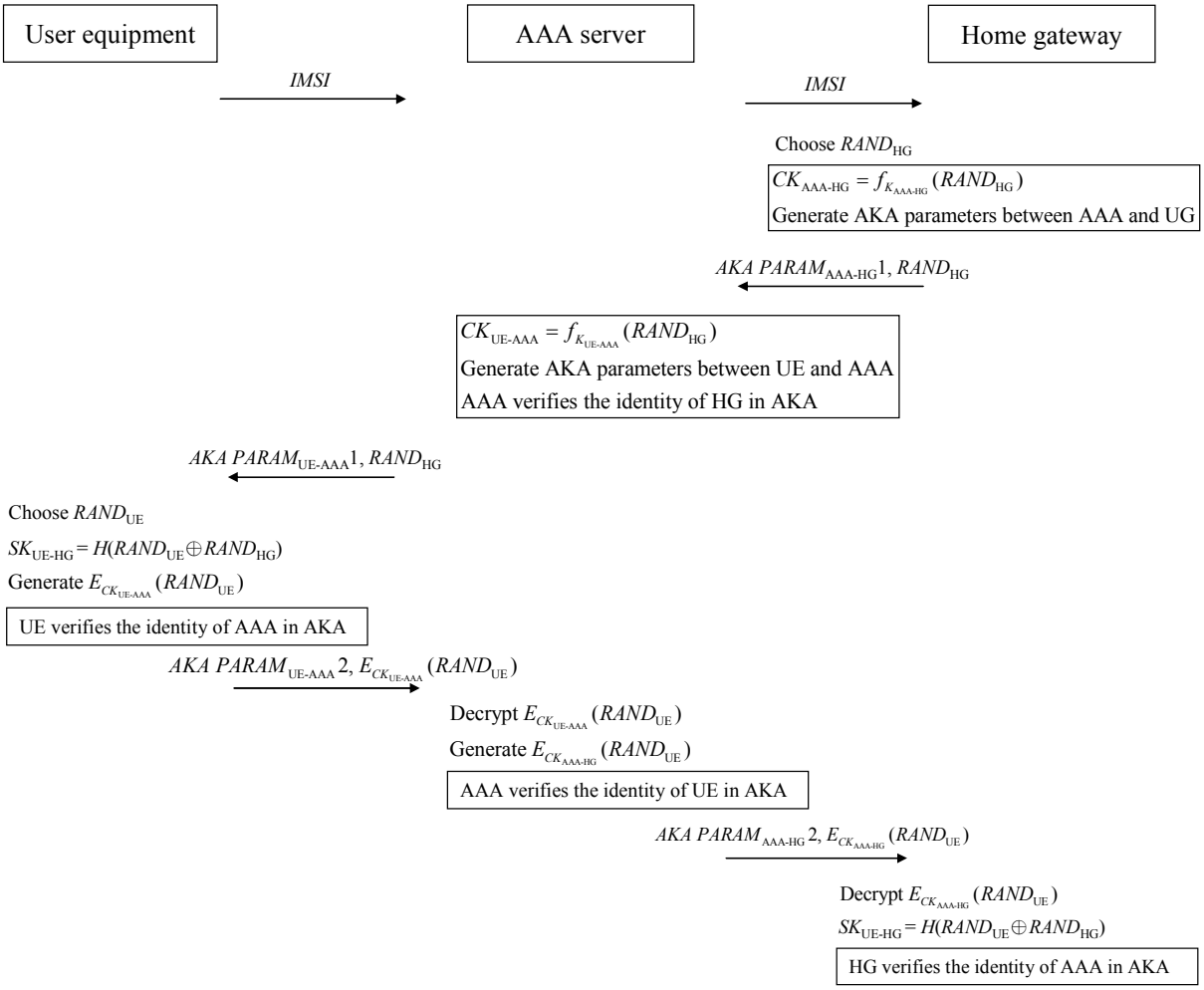

Fig. 4. Mutual authentication and key exchange phase between UE and HG

5.3 Mutual Authentication and Key Exchange Phase between UE and HD

There is no discussion in the literature about key exchange between user equipments and home devices. However, it is necessary for each user to securely and remotely communicate with home devices and therefore, the security mechanism for digital homes should contain the key exchange protocol between user equipments and home devices. The proposed security mechanism can provide content privacy in home networks such that the home gateway cannot gain any content transmitted between each user equipment and home device. In this subsection we will introduce the authentication and key exchange protocol between user equipments and home devices. We adopt Rabin's encryption algorithm in our protocol to achieve the property of forward secrecy. We let the user equipment perform Rabin's encryption because of low cost of computation, so that our design in this protocol can be suitable for digital home environments. The proposed authentication and key exchange protocol and the required notations are shown as follows.

Notations. The notations used in the second phase of our scheme are summarized as follows.

Table 3. Notations of the protocol in Section 5.3

IMSI	international mobile subscriber identity
D	a random number
r_a	a random number generated by the user equipment
r_b	a random number generated by a home device
n_{hd}	a public key generated by the home device
$SK_{\text{UE-HD}}$	a shared session key between UE and HD
β	r_a^2 mod n_{hd}
$H()$	a one-way hash function
$E_{SK_{\text{UE-HG}}}()$	an encryption using the shared symmetric key between UE and HG
$E_{SK_{\text{UE-HD}}}()$	an encryption using the shared symmetric key between UE and HD

The Protocol.

(Step 1) The user equipment → the home gateway: *IMSI*, *Set*

The user equipment randomly chooses a number *D* which is used to challenge the home gateway. Therefore, the user equipment sends *IMSI* and $Set = E_{SK_{\text{UE-HG}}}(D||H(D))$ to the home gateway first.

(Step 2) The home gateway → a home device: *IMSI*

After the home gateway got the message, it decrypts *Set* to get *D* and $H(D)$ and further checks the value of *D*. If the verification is passed, the home gateway will relay *IMSI* to a home device.

(Step 3) The home gateway ← the home device: n_{hd}, r_b

When the home device received *IMSI* which is sent from the home gateway, the home device randomly chooses r_b and generates the public key n_{hd} and the corresponding private key of Rabin's encryption. The home device then stores the pair (*IMSI*, r_b) in its database. The parameter r_b is one of the components which will generate a session key. Both r_b and $n_{hd} = pq$ are sent to the home gateway where *p* and *q* are two distinct large primes randomly chosen by the home device.

(Step 4) The user equipment ← The home gateway: *Set'*, n_{hd}

The home gateway computes $Set' = E_{SK_{\text{UE-HG}}}(r_b \,||H(r_b)||D)$ and sends *Set'* and n_{hd} to the user equipment. Then the user equipment confirms the value of *D*. If the value of *D* is the same as the original value of that the user equipment chose, the home gateway is successfully authenticated by the user equipment.

(Step 5) The user equipment → The home gateway: *Set''*, $E_{SK_{\text{UE-HD}}}(H(r_a))$

The user equipment randomly chooses a number r_a first. Then the user equipment will decrypt *Set'* to get *D* and r_b and then check the correctness of *D*. If the check is passed, the user equipment will get r_b and r_a which are used to generate a session key. The user equipment computes $\beta = r_a^2$ mod n_{hd} and generates a shared session key $SK_{\text{UE-HD}} = H(r_a||r_b)$ between the user equipment and the home device. Finally, the user equipment sends $Set'' = E_{SK_{\text{UE-HG}}}(H(r_b)||\beta||H(\beta))$ and $E_{SK_{\text{UE-HD}}}(H(r_a))$ to the home gateway.

(Step 6) The home gateway → the home device: β, $E_{SK_{\text{UE-HD}}}(H(r_a))$

The home gateway should decrypt *Set''* to get β and check the correctness of $H(r_b)$ to authenticate the user equipment. When the authentication is passed, the home gateway then relays β and $E_{SK_{\text{UE-HD}}}(H(r_a))$ to the home device. The home device can get r_a from decrypting β. The home device uses r_a and r_b to generate $SK_{\text{UE-HD}}$ to decrypt $E_{SK_{\text{UE-HD}}}(H(r_a))$ in order to verify the value of r_a. If the check is passed, the home device and the user equipment can take the session key, $SK_{\text{UE-HD}}$, to protect the transmission data between the user equipment and the home device.

All steps of the authentication and key exchange protocol between the user equipment and the home device are shown in the following figure.

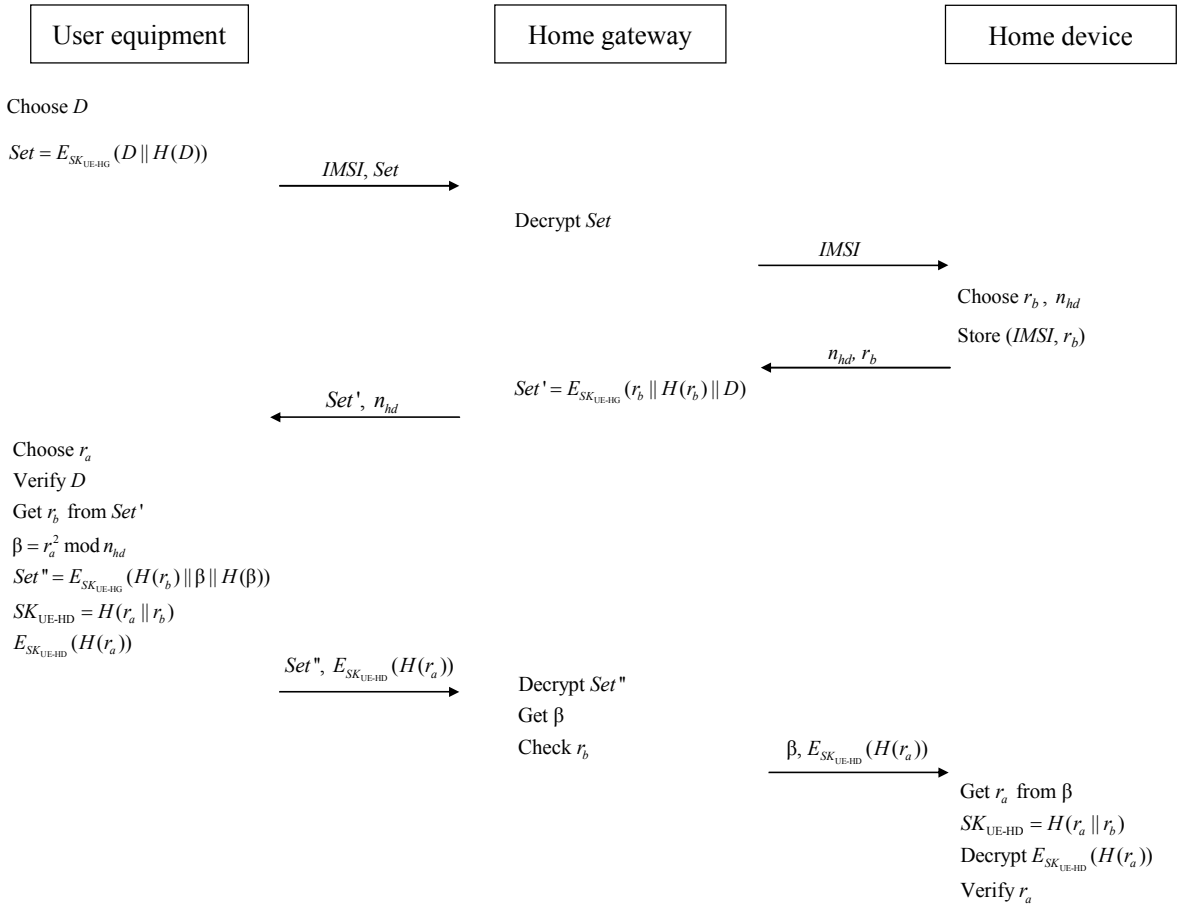

Fig. 5. Mutual authentication and key exchange phase between UE and HD

6 Security Analysis and Discussions

Mutual Authentication and Key Exchange Phase between UE and HG. Our mutual authentication and key exchange protocol can ensure mutual authentication between user equipments and the AAA server and between the AAA server and the home gateway. Thus, we can achieve mutual authentication between UE and HG indirectly. We also employ the standard 3G authentication and key exchange protocol, AKA, as the foundation of our protocol. The design possesses many advantages for our defined digital home environments, such as compatibility and efficiency. Since 3G AKA is an examined protocol which has the property of mutual authentication, our protocol also inherits such a property. The security analysis of 3G AKA can be found in [1].

Mutual Authentication and Key Exchange Phase between UE and HD. If the user equipment wants to remotely control the home device, mutual authentication and key exchange between the user equipment and the home device will be required. The session key $SK_{\text{UE-HD}}$ will be produced to protect the transmission data in this phase. The session key cannot be computed by other people, including eavesdroppers and other family members. We will have some choices on the algorithms for the design of the key exchange phase, such as Rabin's algorithm [8] and Diffie-Hellman algorithm [9]. We finally choose Rabin's algorithm since the computation cost of Rabin's encryption algorithm is lower than that of Diffie-Hellman algorithm.

Light-Weight Cost. We adopt symmetric key cryptosystems in the first phase of our scheme. The public key algorithm, Rabin's encryption algorithm, is used in the second phase of our scheme. Rabin's encryption algorithm has a good property that the encryption operation only needs one modular exponentiation computation. Thus, we can let the encryption operation be performed in the user equipment without affecting the property of light-weight cost.

Withstanding the Replay Attack. We will not discuss the replay attack in the network inside the home owing to the existence of secure environments. First, we discuss the replay attack in authentication and key exchange between the user equipment and the home gateway. In this phase, the design of the protocol is based on the standard 3G authentication and key exchange protocol such that it can withstand the replay attack. Secondly, we consider the replay attack in the authentication and key exchange protocol between the user equipment and the home device. We assume that an attacker captures the authentication information in Step 4 and Step 5 to try to impersonate the home gateway or user equipment. Here, if the attacker captures the information of Step 4 to impersonate the home gateway, it will not be successful. The authentication message $Set' = E_{SK_{\text{UE-HG}}}(r_b \| H(r_b) \| D)$ includes a random number D which needs to be checked in every session. The random number D is the challenge of the user equipment. Therefore, it is impossible that the attacker obtains the past authentication information of Step 4 to impersonate the home gateway successfully. Besides, assume that the attacker obtains the authentication information of Step 5. The replay attack cannot still succeed. The challenge of the home gateway is the random number r_b which is encrypted in $Set' = E_{SK_{\text{UE-HG}}}(r_b \| H(r_b) \| D)$. Thus, when the user equipment decrypts Set' to obtain r_b, the home equipment will generate the hashed value of r_b and encrypt it by computing $Set'' = E_{SK_{\text{UE-HG}}}(H(r_b) \| \beta \| H(\beta))$. The random number r_b is also different in every session, so that it is impossible for the attacker to use old authentication information to be authenticated successfully.

Forward Secrecy. The session key $SK_{\text{UE-HD}}$ shared between the user equipment and the home device are generated via r_a and r_b. If an attacker can obtain these two numbers which are randomly generated in every session, the session key $SK_{\text{UE-HD}}$ can be derived by the attacker. Even though the only secret key $SK_{\text{UE-HG}}$ is lost in the second phase, r_b is the only random number that will be leaked. Since r_a is protected by Rabin's encryption and the Rabin encryption parameters are different in every session, the attacker is hard to obtain all past session keys when the long-term secret was lost.

7 Conclusions

We have proposed a complete security mechanism for digital home. It suffices the security requirements, such as mutual authentication, key exchange, and forward secrecy. Our scheme does not employ time-consuming operations in user equipments in order to reduce the computation cost for mobile devices. Furthermore, the definitions and assumptions in digital home security also are discussed in this paper. Our proposed security mechanism can be easily deployed in current telecommunication networks because that we use the 3G standard authentication protocol and the AAA server in our security mechanism.

Acknowledgement

This work was supported in part by National Science Council under grant 95-2219-E-110-004 and TWISC@NCKU under the grant NSC 94-3114-P-006-001-Y.

References

[1] 3rd Generation Partnership Project, Technical Specification Group SA, and 3G Security, "Formal Analysis of the 3G Authentication Protocol," *3GPP Specifications*, TR 33.902, Version 3.1.0, 1999.

[2] 3rd Generation Partnership Project, Technical Specification Group SA, and 3G Security, "Security Architecture, Version 4.2.0, Release 4," *3GPP Specifications*, TS 33.102, 2001.

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," *RFC3748*, 2004.

[4] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," *RFC 4187*, 2006.

[5] N. Haller, "The S/KEY One-Time Password System," *RFC 1760*, 1995.

[6] J. Jeong, M.Y. Chung, and H. Choo, "Secure User Authentication Mechanism in Digital Home Network Environments," *Lecture Notes in Computer Science*, Vol. 4096, pp.345-354, 2006.

[7] N.Y. Lee and J.C. Chen, "Improvement of One-Time Password Authentication Scheme Using Smart Cards," *IEICE Transactions on Communications*, Vol. E88-B, No.9, pp.3765-3767, 2005.

[8] M.O. Rabin, *Digitalized Signatures and Public-key Functions as Intractable as Factorization*, Technical Report LCS/TR212, Cambridge MA:MIT, 1979.

[9] E. Rescorla, "Diffie-Hellman Key Agreement Method," *RFC 2631*, 1999.

[10] H. Sun, "Home Networking," *Mitsubishi Electric Research Laboratories*, 2004. (available at http://www.merl.com/projects/hmnt/)

[11] I. You, "Analysis and Extension of S/Key-based Authentication Schemes for Digital Home Networks," *Lecture Notes in Control and Information Sciences*, Vol. 344, pp.1022-1033, 2006.

[12] I. You and E. Jung, "A Light Weight Authentication Protocol for Digital Home Networks," *Lecture Notes in Computer Science*, Vol. 3983, pp.416-423, 2006.