EFFICIENT DELEGATION-BASED AUTHENTICATION PROTOCOL WITH STRONG MOBILE PRIVACY

Jian-Zhu Lu, Hong-Qing Ren and Jiping Zhou
Department of Computer Science, Jinan University, Guangzhou, 510632 Guangdong, China

Keywords: Security, Privacy, Mobile communication, Mutual authentication.

Abstract: In 2008, Tang and Wu designed a one-time alias mechanism for protecting the mobile privacy of a user. Recently, Youn and Lim proposed an improved delegation-based authentication protocol to provide private roaming service. In this article, we show that a link between requests may disclose information about the mobile privacy of a sender, and that the aliases of a user fail to achieve the unlinkability in Tan-Wu's scheme. We remedy this situation by suggesting an enhanced protocol that utilizes a pseudorandom function. Compared to Youn-Lim's protocol, our design is more efficient than theirs.

1 INTRODUCTION

Recent years have witnessed the dramatic and continuous increase of e-commerce transactions. E-commerce makes it easier for a service provider to get and collect users' personal information. Privacy is one of the major concerns of users when exchanging information through a network. In a roaming environment, it's important to provide a secure way to simultaneously protect the interests of both the service provider and the users and thereby establish a trust relationship.

To meet the challenge of providing access control for a content provider and privacy protection for users, several authentication schemes have been proposed for roaming service (Lee, 2005), (Tang, 2008a), (Tang, 2008b). In 2005, Lee and Yeh (Lee, 2005) proposed a delegation-based authentication (DBA) protocol for the use in portable communication system. Tang and Wu designed a possible attack to Lee-Yeh's scheme in (Tang, 2008a), and then proposed a scheme of protecting mobile privacy in wireless networks (Tang, 2008b). Recently, Youn and Lim (Youn, 2010) showed that the protocol in (Lee, 2005) cannot achieve private roaming service. They then presented an improved protocol to fix the problem.

In Tan-Wu's scheme (Tang, 2008b), authors designed a one-time alias mechanism for various levels of privacy protection. A new alias was generated by hashing either the previous used alias or the user identity. In this article, we show that Tan-Wu's protocol cannot provide the mobile privacy for a roaming user since the aliases of the user fails to achieve the unlinkability. We remedy this situation by suggesting an enhanced protocol that utilizes a pseudorandom function(PRF). We also demonstrate how the enhanced protocol is more efficient compared to the implementation in (Youn, 2010).

2 REVIEW OF TANG-WU'S SCHEME

2.1 Description

In 2008, Tan and Wu proposed a mutual authentication scheme for mobile communications (Tang, 2008b), which is briefly described below. First, the notation used in the scheme is defined as follows. Let G be a cyclic additive group with generator T, p is the largest prime factor of the order of T, $h : Z_p^* \mapsto Z_p^*$ be a collision-resistant hash function, and $\prod : G \mapsto Z_p^*$ be a point representation function. The symbol '$\uplus$' denotes a point addition operator in G, and $[X]_K$ denotes encrypting a message X with a key K using a symmetric encryption algorithm. We assume that IDV and IDH be the identities of VLR and HLR, respectively. HLR has a private/public key pair (x, Y), where $x \in Z_p^*$ is a random number, and $Y = xT$

The scheme in (Tang, 2008b) consists of two protocols:TDI and EMA. TDI is described below.

Step (1). First, MS sends his/her real identity IDM and a alias IDMA to HLR for registration.

Lu J., Ren H. and Zhou J..
EFFICIENT DELEGATION-BASED AUTHENTICATION PROTOCOL WITH STRONG MOBILE PRIVACY.
DOI: 10.5220/0003606901230127
In *Proceedings of the International Conference on Wireless Information Networks and Systems* (WINSYS-2011), pages 123-127
ISBN: 978-989-8425-73-7

Step (2). HLR sets key usage restrictions in m_w, and generates a random number κ, and computes $\Gamma = (h(\text{IDMA}|m_w)T) \uplus (\kappa T)$ and $\sigma = -xh(\Pi(\Gamma)) - \kappa \bmod p$ for a mobile station MS. Afterwards, $(\text{IDMA}, m_w, \Gamma)$ is published, while (IDMA, σ) is stored in HLR's database and (σ, m_w) is sent to MS via a secure channel.

Step (3). If $h(\text{IDMA}|m_w)T = (\sigma T) \uplus (h(\Pi(\Gamma))Y) \uplus \Gamma$, MS accepts the delegation key σ.

There are three parties involved in EMA: MS, VLR, and HLR. Suppose there is a secure channel to protect the traffic between VLR and HLR, and $K_{(V,H)}$ is their share key. Three parties perform the following steps:

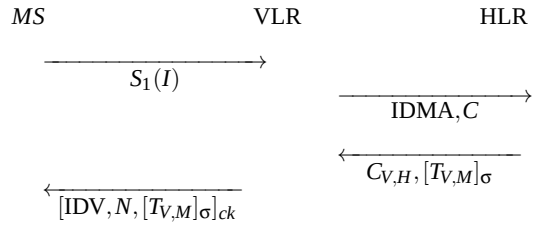
Step (1). MS randomly generates a communication key *ck* and two numbers *nonce* and κ, and computes $C = [ck, ts, T_{\text{exp}}, nonce]_\sigma$, $R = kT$ and $s = -kh(\Pi(R)|nonce) + \sigma \bmod p$. Here, ts is the current timestamp, and *nonce* is a nonce. *ck* is only valid for a certain time length T_{exp}. Then, MS sends $S_1 = \{R, s, \text{IDH}, m_w, C, nonce\}$ to VLR.

Step (2). After receiving S_1, VLR checks the warrant m_w for restrictions, and authenticates MS by using the attached digital signature (R, s). If both are true, VLR sends a request $S_2 = \{\text{IDMA}, C\}$ to HLR.

Step (3). HLR first searches the corresponding σ in its database according to IDMA, then decrypts C to obtain *ck*, *ts*, T_{exp} and *nonce*. If *ck* is valid, HLR provides strong mobile privacy for MS by performing the following three tasks: (*a*) generation of new alias $\text{IDMA} = h(\text{IDX}) \in Z_p^*$, where IDX be the previous used alias or IDM; (*b*) substitution of delegation key σ' for σ and public information Γ' for Γ, where $\Gamma' = (h(\text{IDMA}|m_w)T) \uplus (\kappa' T)$ and $\sigma = -xh(\Pi(\Gamma')) - \kappa' \bmod p$ for a random number κ'; and (*c*) sending $C_{V,H} = [\text{IDMA}, T_{exp}, ts, ck, nonce]_{K_{(V,H)}}$ to VLR and forwarding $[T_{V,M}]_\sigma$ to MS, where $T_{V,M} = \{\text{IDV}, nonce, \sigma'\}$.

Step (4). Receiving the response $\{C_{V,H}, [T_{V,M}]_\sigma\}$ from HLR, VLR decrypts $C_{V,H}$, and check the validity not only for *ck* that isn't an expired key, but also for *nonce* that is equal to the one in **Step (2)**. If it is true, VLR computes $[\text{IDV}, nonce, [T_{V,M}]_\sigma]_{ck}$ and sends it to MS.

Step (5). MS decrypts $[\text{IDV}, nonce, [T_{V,M}]_\sigma]_{ck}$ and $[T_{V,M}]_\sigma$ using *ck* and σ, respectively. By the consistency of *IDV* and *N*, MS can authenticate VLR. If true, and MS and VLR authenticate each other successfully.



$C = [ck, ts, T_{\text{exp}}, \text{IDV}, N, \text{IDMA}']_\sigma$
$S_1(I) = \{\text{IDMA}, C, \text{Sig}_\sigma(N), N, m_w, \text{IDH}\}$
$C_{V,H} = [\text{IDMA}, T_{exp}, ts, ck, N]_{K_{(V,H)}}$
$T_{V,M} = \{\text{IDV}, N, \sigma'\}$

Figure 1: Efficient DBA Protocol with Strong Mobile Privacy.

2.2 Mobile Privacy of Users in EMA

The mobile privacy of a user can be disclosed by using the tracking and activity recognition when a link between the requests from the user exists. Suppose that the service-region is divided into n areas and MS visits them in the following order: $A_1 \to A_2 \to \cdots \to A_n$. There are n service providers. Each service provider VLR_i is responsible for one area A_i, $1 \le i \le n$. A request $S_1(I_i)$ for a service item I_i is generated in the area A_i by MS and is sent to the VLR_i through a wireless channel. Using a pseudonym technique, MS is able to interact with the system without revealing his identity. However, an attacker can track the unique pseudonym. This problem can be addressed with a one-time alias technique for MS. The one time alias IDMA_i is used by MS to transmit the request messages $S_1(I_i)$ to VLR_i. If a link between these requests is obtained by some means, an attacker can take action to track MS's moving history and current location.

There is a link between one-time aliases of MS in (Tang, 2008b). As describe in (Tang, 2008b, page1040, line 15), a new alias of MS is simply IDMA=h(IDX), where IDX be the previous used alias or IDM. In the first request $S_1(I_1)$, there isn't any previous used alias for MS. The first alias in $S_1(I_1)$ can be computed as $\text{IDMA}_1 = h(\text{IDM})$. After the first request, MS computes the one-time alias $\text{IDMA}_i = h(\text{IDX})$ in $S_1(I_i)$, where $\text{IDX} \in G_{i-1} = \{\text{IDM}, \text{IDMA}_1, \cdots, \text{IDMA}_{i-1}\}$, and $2 \le i \le n$. For a given set Ω, we denote $\{h(e)|e \in \Omega\}$ as $h(\Omega)$. The above process may be regarded as selecting an element IDMA_i from the set $h(G_{i-1}) = \{h(e)|e \in G_{i-1}\}$. Note that $G_1 = \{\text{IDM}, h(\text{IDM})\}$ and $G_i = G_{i-1} \cup \{\text{IDMA}_i\}$. Since $\text{IDMA}_i \in h(G_{i-1})$, we have $G_i \subseteq (G_{i-1} \cup h(G_{i-1}))$. Thus, $G_2 \subseteq \{\text{IDM}, h(\text{IDM}), h^2(\text{IDM})\}$ using $G_1 = \{\text{IDM}, h(\text{IDM})\}$, and $G_3 \subseteq \{\text{IDM}, h(\text{IDM}), h^2(\text{IDM}), h^3(\text{IDM})\}$ using the result of G_2, and so on. Each set G_{i-1} can be rep-

resented as a subset of D_{i-1}=$\{\text{IDM}, h(\text{IDM}), \cdots, h^{i-1}(\text{IDM})\}$, and thereby $h(G_{i-1}) \subseteq h(D_{i-1})$. We note that $h(D_1) \subset h(D_2) \subset \cdots \subset h(D_{n-1})$ and $h(D_{n-1})$= $\{h(\text{IDM}), h^2(\text{IDM}), \cdots, h^n(\text{IDM})\}$. Every set $h(G_{i-1})$ is a subset of $h(D_{n-1})$, so that when IDMA_i is chosen by MS from $h(G_{i-1})$, it belongs to $h(D_{n-1})$. However, the elements in $h(D_{n-1})$ form a hash chain that can be generated by the seed $h(\text{IDM})$. For each MS's alias couple $(\text{IDMA}_{i-1}, \text{IDMA}_i)$, there exists an integer $l \in Z_{n-1}$ such as IDMA_i=$h^l(\text{IDMA}_{i-1})$ or IDMA_{i-1}=$h^l(\text{IDMA}_i)$. Hence, an attacker can link two different aliases of MS, and conclude that MS visits areas (from A_{i-1} to A_i) in consecutive order.

3 EFFICIENT DBA PROTOCOL WITH STRONG MOBILE PRIVACY

3.1 Basic Idea

Let IDMA be the current alias of MS and assume that F is taken from a pseudorandom function (PRF). For the unlinkability, an alias of MS is derived from F with delegation key σ and input IDMA and output of the appropriate length for the subsequent authentication. HLR generates a new delegation key pair (σ', Γ') for each new alias IDMA$'$, and transmits σ' to MS in a secure way. Then MS and HLR store (IDMA', σ') instead of (IDMA, σ). They use the updated delegation key pair for a new authentication.

3.2 Description of Enhanced Protocol

Since the setup procedure is the same as TDI proposed in (Tang, 2008b), we only describe the efficient mutual authentication (EMA) procedure as shown in Fig. 1. Let l be an integer representing the length of an alias and $\mathcal{B}_l(m)$ denote the first l bits of binary string m. For each execution of EMA protocol , three parties perform the following steps:

Step (1). MS sends a request $S_1(I)$ to VLR for the service item I. First, MS computes a new alias IDMA'= $\mathcal{B}_l(F(\sigma, \text{IDMA}))$ for the next authentication. MS randomly generates a communication key ck and two numbers N and κ, and computes C=$[ck, ts, T_{\text{exp}}, \text{IDV}, N, \text{IDMA}']_\sigma$ and $\text{Sig}_\sigma(N)$=(R,s), where R=kT, and s=$-kh(\Pi(R)|N) + \sigma \bmod p$. Here, ts is the current timestamp, and N is a nonce. ck is only valid for a certain time length T_{exp}. Then, MS sends $S_1(I) = \{\text{IDMA}, C, \text{Sig}_\sigma(N), N, m_w, \text{IDH}\}$ to VLR.

Step (2). After receiving S_1, VLR checks the warrant m_w for restrictions, and authenticates MS by using the attached digital signature (R,s). If both are true, VLR sends a request S_2=$\{\text{IDMA}, C\}$ to HLR. Otherwise, VLR rejects MS's request.

Step (3). HLR retrieves σ according to IDMA, and decrypts C to obtain ck, ts, T_{exp}, IDV, N and IDMA'. Then, HLR verifies if IDV is identical to the identity of sender in Step (2), at the same time, checks if ck is not expired. If $\text{IDMA}' = \mathcal{B}_l(F(\sigma, \text{IDMA}))$, HLR performs the substitution of delegation key (IDMA', σ') for (IDMA, σ) and public information $(\text{IDMA}', \Gamma', m_w)$ for $(\text{IDMA}, \Gamma, m_w)$, where $\Gamma' = (h(\text{IDMA}|m_w)T) \uplus (\kappa' T)$ and $\sigma = -xh(\Pi(\Gamma')) - \kappa' \bmod p$ for a random number κ'. Then, HLR sends $C_{V,H} = [\text{IDMA}, T_{exp}, ts, ck, N]_{K_{(V,H)}}$ to VLR, and forwards $[T_{V,M}]_\sigma$ to MS, where $T_{V,M} = \{\text{IDV}, N, \sigma'\}$.

Step (4). Receiving the response $\{C_{V,H}, [T_{V,M}]_\sigma\}$ from HLR, VLR decrypts $C_{V,H}$, and checks the validity not only for ck that isn't an expired key, but also for N that is equal to the one in **Step (2)**. If it is true, VLR computes $[\text{IDV}, N, [T_{V,M}]_\sigma]_{ck}$ and sends it to MS.

Step (5). MS decrypts $[\text{IDV}, N, [T_{V,M}]_\sigma]_{ck}$ and $[T_{V,M}]_\sigma$ using ck and σ, respectively. By the consistency of IDV and N, MS can authenticate VLR. If true, MS and VLR authenticate each other successfully. MS stores $(\text{IDMA}', \sigma', m_w)$ instead of $(\text{IDMA}, \sigma, m_w)$.

3.3 Security Discussion and Performance Comparison

3.3.1 Security

HLR is assumed to be completely trustworthy and nontamperable. As indicated in (Youn, 2010), we also assume that legitimate entities (including HLR and VLR) are trustworthy. In this case, we can trust anyone who is verified as a valid entity.

We analyze the security provided by the enhanced protocol. As the basic requirements on mobile authentication in (Tang, 2008b) are entirely preserved, the associated security properties hold true here as well and we will not repeat them. The enhanced protocol does not suffer from the ailments of traditional pseudonymous authentication protocols. Attacks such as DOS attack to HLR or the privacy disclosure of requests described in Section 2.2 are avoided.In the following, we only discuss the enhanced security features of the proposed scheme:

Unlinkability. We now analyze the unlinkability of enhanced protocol in terms of the various parts of the

request message $S_1(I)$. Recall that IDMA is the output of PRF F and C is the output of an IND-CCA secure symmetric encryption scheme. Due to the indistinguishability property of a PRF F, it is computationally infeasible to distinguish between IDMA and a random value in $\{0,1\}^l$. The probability of success for an attacker to distinguish between C and a random element in the ciphertext space is negligible under the IND-CCA assumption (Bellare, 1997). The nonce N is randomly selected from Z_p^*. At the same time, MS runs a secure digital signature scheme in (NIST, 2009) to generate $\mathrm{Sig}_\sigma(N)$ for a service item I, giving one-time σ and $(\mathrm{IDMA}, \Gamma, m_w)$. It is also straightforward to show that events E_1 and E_2 occur with negligible probability, where E_1 is the event that a HLR-generated verification key $(\mathrm{IDMA}, \Gamma, m_w)$ is used more than once, and E_2 is the event that an attacker forges a new, valid message/signature pair with respect to any HLR-generated verification key. We have assumed that the probability of deriving MS identity information from its associated delegation constraint information m_w is negligible. The part "IDH" is used to point to the end of the ciphertext C. Therefore, an attacker can't find a link of part in $S_1(I)$ with the past.

Impersonation Attacks. The enhanced protocol can efficiently prevent an attacker from impersonating attacks, since the scheme provides secure mutual authentication mechanisms between a roaming MS and VLR, MS and HLR, or VLR and HLR. Consider the following impersonation attack scenarios in this protocol.

An attacker cannot impersonate a legitimate VLR to cheat MS, since he does not possess the correct values N and $[T_{V,M}]_\sigma$. By intercepting the exchanging messages in steps (2) and (4), an outside attacker first obtain C=$[ck, ts, T_{\mathrm{exp}}, \mathrm{IDV}, N, \mathrm{IDMA}']_\sigma$ and $[\mathrm{IDV}, N, [T_{V,M}]_\sigma]_{ck}$. Then, she/he tries to cheat MS by replaying previously reply messages (e.g., $[\mathrm{IDV}, N', [T'_{V,M}]_\sigma]_{ck}$). However, N is different from those within C in the replayed messages and, therefore, it would be rejected by MS. Furthermore, an inside attacker cannot impersonate the visited VLR to cheat MS. Since the delegation key σ is unknown to the inside attacker, and she/he cannot generate $[T_{V,M}]_\sigma$, where $T_{V,M}$=$\{\mathrm{IDV}, N, \sigma'\}$, IDV and N are chosen by MS, and σ' can be verified with the public information Γ'.

An attacker hasn't the power to impersonate HLR while communicating with VLR and to impersonate VLR while communicating with HLR, since neither the long-term secret key $K_{(V,H)}$ nor a valid IDV in C is possessed. Hence, while communicating with HLR, an attacker can neither generate the valid messages in step (2) to guarantee that the matching of IDV is done in a consistent way. At the same time, the lack of key $K_{(V,H)}$ implies that it can not decrypt the response $C_{V,H}$. Likewise, she/he generate the responding confirmation $C_{V,H}$ while communicating with VLR.

MS and its HLR can authenticate their messages so that an attacker cannot impersonate them any more. Since the delegation key σ is unknown to the attacker, and she/he cannot generate a valid ciphertext C=$[ck, ts, T_{\mathrm{exp}}, \mathrm{IDV}, N, \mathrm{IDMA}']_\sigma$. Here, IDMA' =$\mathcal{B}_l(F(\sigma, \mathrm{IDMA}))$, and ts and N are generated by M. Similarly, the attacker can neither generate the responding confirmation $[T_{V,M}]_\sigma$.

Replay Attacks and DoS Attacks. In DoS attacks, the attackers may flood a large number of illegal access requests to the HLR. Their aim is to consume critical resources in the HLR. By exhausting these critical resources, the attacker can prevent the HLR from serving legitimate users. In HLR-online authentication, for every access request $S_1(I)$ from all users that have registered in the HLR, HLR has to perform two decryption operations and check the validity of the requesters. These can easily be exploited by the attacker.

The basic idea as adopted in (Tang, 2008a) is to use a proxy signature along with mobile authentication. HLR performs a mobile authentication only when the proxy signature can be verified by a VLR.

The following steps describe the proxy signature verification procedure performed by a VLR. For each request $S_1(I)$ that is received, extract the nonce N and its signature $Sig_\sigma(N)$=(R,s). VLR verifies this value $Sig_\sigma(N)$ with the corresponding verification information $(\mathrm{IDM}, \Gamma, m_w)$ of MS, then $S_1(I)$ is considered to be legitimate if $(sT) \uplus (h(\prod(R)|N)R) = \Gamma$. Otherwise, the request is illegitimate. Then, VLR construct a request message $S_2 = \{\mathrm{IDMA}, C\}$ for legitimate $S_1(I)$, and send it to the HLR. Thus, it is difficult for an attacker to launch an effective DoS attack to HLR.

Furthermore, we make use of the nonce N to prevent replay attacks. Thus, our solution does not suffer from this attacks.

Table 1: Security comparison with other related schemes.

	(Lee, 2005)	(Tang, 2008b)	(Youn, 2010)	Ours
SP_1	No	No	Yes	Yes
SP_2	No	No	Yes	Yes
SP_3	Yes	Yes	Yes	Yes
SP_4	Yes	Yes	Yes	Yes
SP_5	Yes	Yes	Yes	Yes

We also compare our scheme to other contributory mobile authentication schemes including the schemes in (Lee, 2005; Tang, 2008b; Youn, 2010). Table 1 summarizes the security properties of four schemes.

The security properties against unlinkability, impersonation attacks, mobile DoS attacks to HLR, replay attacks, and session key agreement are are denoted as: SP_1, SP_2, SP_3, SP_4 and SP_5, respectively.

Tang and Wu (Tang, 2008a) showed that Lee-Yeh scheme in (Lee, 2005) suffers from an impersonated HLR attack such that the session key is compromised. Lu and Zhou (Lu, 2010) described a dishonest VLR$'$ for Tang-Wu (Tang, 2008a) scheme to obtain the communication key generated by MS. The above comparisons show that our scheme and provides the strongest security protection.

3.3.2 Performance

The storage and the computation and communication in the enhanced protocol are about the same costs as that in the scheme (Tang, 2008b). No computation cost needs to be added by MS, except the additional communication cost $2l$.

Table 2: Computation costs comparison.

	Ours			(Youn, 2010)		
	MS	VLR	HLR	MS	VLR	HLR
Public key oper.	1	0	1	1	0	1
Sig. veri.	0	1	0	0	1	0
Nonce gen.	1	0	0	0	0	0
Hash+PRF oper.	1+1	0+0	0+1	2+0	0+0	1+0
Sym. key oper.	3	2	2	1	1	2

Our protocol uses overall structure similar to a recent protocol (Youn, 2010), but our design is more efficient than theirs. Table 2 shows the computation costs of both protocols. The time used to perform a symmetric encryption operation is negligible compared with the time needed to execute a public-key computation. Thus, Our computation cost is almost identical to Youn-Lim's. Table 3 shows that the communication costs and storage space of both protocols depend upon the choices of parameters, where cr is the number of communication round, and $L = |ts| + |T_{\text{exp}}| + |m_w|$. It is recommended that the security strength of $|p|$ isn't less than 160 bits in (NIST, 2009)[Page 27], and the minimum of the security strength of the $(|p^*|, |q|)$ pair is $(1024, 160)$ in (NIST, 2009)[Page 15]. Therefore, our design is a less strong requirement in the communication cost and storage space than Youn-Lim's, especially for the mobile user MS.

4 CONCLUSIONS

In this paper, we showed that Tan-Wu scheme (Tang, 2008b) doesn't provide the protection of mobile privacy in roaming services. We also proposes an enhanced delegation-based authentication protocol. Compared to Youn-Lim's protocol in (Youn, 2010), our design is more efficient than theirs.

Table 3: Communication costs and storage spaces comparison.

		cr	Commun. Messages	Storage spaces
Ours	MS	2	$6p+3l+L$	$p+l+\|m_w\|$
	VLR	2	$4p+2l+L$	$2p+l$
	HLR	2	$5p+2l+L$	$3p+2l+\|m_w\|$
(Youn, 2010)	MS	4	$3p^*+2q+2l$	p^*+q
	VLR	4	$2p^*+5q+3l$	$h+l$
	HLR	2	$p^*+5q+l+\|h\|$	p^*+2q+l

ACKNOWLEDGEMENTS

This work was supported in part by the National Natural Science Foundation of China under Grants 60773083, and in part by the Provincial Natural Science Foundation of Guangdong under Grants 2008B090500201, 2009B010800023 and 2010B090400164.

REFERENCES

Lee W.-B., Yeh C.-K., 2005. A New Delegation-based Authentication Protocol for Use in Portable Communication Systems. In *IEEE Transactions Wireless Communication*, vol. 4, no.1, pp. 57-64

Tang C., Wu D. O.,2008. An Efficient Mobile Authentication for Wireless Networks. In *IEEE Transactions Wireless Communication*, vol. 7, no.4, pp. 1408-1416

Tang C., Wu D. O., 2008. Mobile Privacy in Wireless Networks Revisited. In *IEEE Transactions Wireless Communication*, vol. 7, no.3, pp.1035-1042

Youn T.-Y., Lim J., 2010. Improved Delegation-Based Authentication Protocol for Secure Roaming Service with Unlinkability. In *IEEE Communications Letters*, vol. 14, no. 9, pp.791-793

Bellare M., Desai A., Jokipii E., Rogaway P., 1997. A Concrete Security Treatment of Symmetric Encryption. In: *Proc. of the 38th IEEE Symp. on Found. of Computer Sci.*, pp. 394-403

Lu J., Zhou J., 2010. The security of an efficient mobile authentication scheme for wireless networks, In *WiCOM 2010: 6th International Conference on Wireless Communications Networking and Mobile Computing*, Chengdu (China).

NIST, 2009. NIST FIPS PUB 186-3, Digital Signature Standard (DSS) . U.S. Department of Commerce.