Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 894549, 9 pages
http://dx.doi.org/10.1155/2015/894549

Research Article

Robust and Efficient Authentication Scheme for Session Initiation Protocol

Yanrong Lu,[1,2] Lixiang Li,[1,2] and Yixian Yang[1,2]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Lixiang Li; li_lixiang2006@163.com

Received 16 October 2014; Revised 4 January 2015; Accepted 5 January 2015

Academic Editor: Elmetwally Elabbasy

The session initiation protocol (SIP) is a powerful application-layer protocol which is used as a signaling one for establishing, modifying, and terminating sessions among participants. Authentication is becoming an increasingly crucial issue when a user asks to access SIP services. Hitherto, many authentication schemes have been proposed to enhance the security of SIP. In 2014, Arshad and Nikooghadam proposed an enhanced authentication and key agreement scheme for SIP and claimed that their scheme could withstand various attacks. However, in this paper, we show that Arshad and Nikooghadam's authentication scheme is still susceptible to key-compromise impersonation and trace attacks and does not provide proper mutual authentication. To conquer the flaws, we propose a secure and efficient ECC-based authentication scheme for SIP. Through the informal and formal security analyses, we demonstrate that our scheme is resilient to possible known attacks including the attacks found in Arshad et al.'s scheme. In addition, the performance analysis shows that our scheme has similar or better efficiency in comparison with other existing ECC-based authentication schemes for SIP.

1. Introduction

Multimedia service is one of the most important application classes of wired or wireless networks. The session initiation protocol (SIP) is one of the most important protocols supporting multimedia services since it could manage sessions including multimedia distribution, internet telephone calls, and internet multimedia conferences [1]. Authentication is an important security requirement when a user wants to access the SIP services. Therefore, the security of SIP [2] has received a lot of attention and the SIP authentication has become a crucial topic in modern multimedia services.

Up to now, various researches have focused on proposing a secure and efficient authenticated key agreement scheme to provide various aspects of security for SIP. In 2005, Yang et al. [3] indicated that the procedure of hyper text transport protocol (HTTP) digest authentication for SIP could not resist the offline password guessing and server-spoofing attacks. To resolve these problems, Yang et al. proposed an improved scheme based on Diffie-Hellman key exchange protocol. Later on, Huang et al. [4] identified that Yang et al.'s protocol was insecure against the offline password guessing attack. To enhance the security of Yang et al.'s scheme, Huang et al. also presented an improved scheme. Later on, Jo et al. [5] demonstrated that Huang et al.'s scheme was still vulnerable to the offline password guessing attack. Based on Yang et al.'s study, Durlanik and Sogukpinar [6] proposed an Elliptic Curve Cryptography (ECC) [7] based authentication scheme for SIP. Compared with other cryptosystems, ECC can achieve the same security with a smaller key size [8]. Therefore, the scheme proposed by Durlanik and Sogukpinar is considered to be more efficient than Yang et al.'s scheme. Later, Wu et al. [9] also proposed an authentication scheme for SIP using ECC. However, Yoon et al. [10] showed that both of Durlanik et al.'s scheme and Wu et al.'s scheme were susceptible to the offline password guessing, Denning-Sacco, and stolen verifier attacks. To overcome these weaknesses, Yoon et al. proposed an enhanced authentication scheme for

SIP with more security. Unfortunately, Pu [11] showed that the scheme of Yoon et al. was still prone to the offline password guessing and replay attacks.

In order to reduce the high computational cost, Tsai [12] suggested an efficient authenticated key agreement scheme only adopting one-way hash functions and exclusive-or operations. Nevertheless, Tsai's scheme was still vulnerable to the offline password guessing attack [13, 14]. Yoon et al. [14] proposed an enhanced scheme to overcome weaknesses in Tsai's scheme. However, Xie [15] demonstrated that Yoon et al.'s scheme did not resist the stolen-verifier and offline password guessing attacks. Xie then proposed an improved scheme to overcome the weaknesses of Yoon et al.'s scheme. Nevertheless, Farash and Attari [16] discovered that Xie's scheme was still insecure against the impersonation and offline password guessing attacks. To enhance security, Farash and Attari presented an improved scheme to solve problems in Xie's scheme. Recently, Zhang et al. [17] proposed an efficient and flexible password authenticated key agreement protocol for SIP using smart card and claimed their protocol was secure against various attacks. However, Zhang et al.'s scheme suffers from the impersonation attack [18, 19]. To tackle the problem, Tu et al. [18] and Irshad et al. [19], respectively, proposed their own improved authentication scheme based on Zhang et al.'s scheme. Unfortunately, Arshad and Nikooghadam [20] demonstrated that Irshad et al.'s scheme could not withstand the user impersonation attack. Arshad and Nikooghadam then proposed an enhancement of Irshad et al.'s scheme suffering from user impersonation attack and claimed that their scheme was immune to many known attacks.

In this study, we identify that the scheme by Arshad and Nikooghadam is insecure against key-compromise impersonation and trace attacks while it fails to provide proper mutual authentication. To conquer the mentioned weaknesses, we propose a robust and efficient authentication scheme using ECC. Through the informal and formal security analyses, we demonstrate that our scheme is resilient to possible known attacks including the attacks found in Arshad and Nikooghadam's scheme. In addition, the performance analysis shows that our scheme has similar or better efficiency in comparison with other related ECC-based authentication schemes for SIP.

The remainder of this paper is organized as follows. Section 2 provides some basic preliminaries and notations used in this paper. The review and security analysis of Arshad and Nikooghadam's scheme are shown in Sections 3 and 4, respectively. Section 5 shows our proposed scheme. Section 6 analyzes our scheme's security. Section 7 shows the performance and functionality comparison among the proposed scheme and other related ones. Section 8 is a brief conclusion.

2. Preliminaries

In this section, some notations used in this paper are described in Section 2.1. We also recall the definitions of the hash function [21] and Elliptic Curve Discrete Logarithm Problem (*ECDLP*) [7] which we use in the security proof of Arshad et al.'s scheme and our improved scheme.

2.1. Notations. We use the notations that are listed below throughout the rest of the paper.

U_i, S: user and sever

ID_i, PW_i: identity and password of U_i

$h(\cdot)$: hash function

k_{U_i}, k_S: secret key selected by U_i and S

$\oplus, \|$: exclusive-or operation and concatenation operation.

2.2. Hash Function. A secure one-way hash function $h : \{0,1\}^* \rightarrow \{0,1\}^n$ takes an input as an arbitrary length binary string $x \in \{0,1\}^*$ and outputs a binary string $h(x) \in \{0,1\}^n$. The probability of $\mathscr{A}$ in finding collision is defined as $Adv^{\mathscr{A}}_{HASH}(t_1) = Pr[\mathscr{A}((x,x'),\ x \neq x') : h(x) = h(x')]$.

2.3. ECDLP. In an elliptic curve cryptosystem, the elliptic curve equation is defined as the form of $E_p(a,b) : y^2 = x^3 + ax + b(\operatorname{mod} p)$ over a finite field F_p, where $a, b \in F_p$ and $4a^3 + 27b \neq 0(\operatorname{mod} p)$.

Given points P, Q over $E_p(a,b)$, the *ECDLP* is to decide $m \in F_p^*$ such that $Q = mP$. The probability of $\mathscr{A}$ can solve the *ECDLP* which is defined as $Adv^{\mathscr{A}}_{ECDLP}(t_2) = Pr[\mathscr{A}(P,Q) = m : m \in F_p^*, Q = mP]$.

3. Review of Arshad and Nikooghadam's Scheme

In this section, we will review Arshad et al.'s authentication scheme for SIP. Their scheme is composed of three phases, which are registration, authentication, and password change.

3.1. Registration

(1) U_i generates a random number N_C, chooses his password PW_i, computes $v_i = h(ID_i \| PW_i \| N_C)$, and sends $\{ID_i, v_i\}$ to S.

(2) S computes $V_i = h(ID_i \| k_S) \oplus v_i$ and stores it into his database.

3.2. Authentication

(1) U_i generates a random number d_C and computes $R_C = d_C K_S$, where $K_S = k_S P$ is the public key of S. Then, U_i sends a message $REQUEST(ID_i, R_C)$ to S.

(2) On receiving the request message, S chooses a random number d_S and computes $Q_S = d_S P$, $Q_{SC} = d_S k_S^{-1} R_C = d_S d_C P$, and $V_S = h(ID_i \| Q_S \| Q_{SC})$. Finally, S sends the message $CHALLENGE(realm, Q_S, V_S)$ to U_i.

(3) After receiving the challenge message, U_i computes $Q_{CS} = d_C Q_S$ and validates whether $V_S' = h(ID_i \| Q_S \| Q_{CS})$ is equal to the received V_S. If it is true, U_i computes $v_i = h(ID_i \| PW_i \| N_C)$, $V_C = h(ID_i \| Q_S \| realm \| Q_{CS} \| v_i)$, and the common session key $SK = h(ID_i \| Q_S \| Q_{CS} \| realm)$. Finally, U_i sends the message $RESPONSE(ID_i, realm, V_C)$ to S.

(4) After receiving the response message, S computes $v_i' = V_i \oplus h(ID_i \| k_S) = h(ID_i \| PW_i \| N_C)$, $V_C' = h(ID_i \| Q_S \| realm \| Q_{CS} \| v_i')$ and compares V_C with the received V_C. If it is correct, S agrees on the common session key $SK = h(ID_i \| Q_S \| Q_{CS} \| realm)$ with U_i.

3.3. Password Change

(1) U_i selects a new random number N_C' and a new password PW_i' and computes $v_i' = h(ID_i \| PW_i' \| N_C')$, $z = h(ID_i \| PW_i \| N_C) \oplus v_i'$, $Z = z \oplus h(ID_i \| SK)$, and $V_z = h(ID_i \| v_i' \| SK \| v_i)$. Then, U_i sends the message $CHANGEPWD(ID_i, Z, V_z)$ to S.

(2) After receiving the message, S computes $v_i = V_i \oplus h(ID_i \| k_S)$ and $v_i' = Z \oplus v_i \oplus h(ID_i \| SK)$ and verifies whether $V_z' = h(ID_i \| v_i' \| SK \| v_i) \overset{?}{=} V_z$. If it holds, S continues to compute $V_i' = V_i \oplus z = h(ID_i \| k_S) \oplus h(ID_i \| PW_i' \| N_C')$ and replaces V_i with V_i'. Then, S sends the message $ACCEPT(h(ID_i \| v_i \| accept \| v_i' \| SK))$ to U_i.

(3) On receiving the message from S, U_i computes $h(ID_i \| v_i \| accept \| v_i' \| SK)$ and checks whether it is equal to the received $ACCEPT$ message or not. If they are equal, U_i replaces N_C with N_C' in his database.

4. Cryptanalysis of Arshad and Nikooghadam's Scheme

In this section, we present the Arshad and Nikooghadam's scheme that is vulnerable to key-compromise impersonation and trace attacks and does not provide proper mutual authentication. The following attacks are based on the assumptions that a malicious attacker $\mathscr{A}$ has completely monitored over the communication channel connecting U_i and S in login and authentication phase. So $\mathscr{A}$ can eavesdrop, modify, insert, or delete any messages transmitted via public channel [22–24].

4.1. Key-Compromise Impersonation Attack. Key-compromise impersonation attack means that $\mathscr{A}$ knows the long-term secret key of one participating entity and can impersonate the entity to other participating entities [25]. In Arshad et al.'s scheme, if S's secret key k_S is compromised by $\mathscr{A}$, he can launch a user impersonation attack as per the following steps.

(1) $\mathscr{A}$ compromises S and steals the information $\{ID_i, V_i\}$ kept in S's database. He then generates a random number d_C' and computes $R_C' = d_C' k_S P$. Finally, he sends the forged message $REQUEST(ID_i, R_C')$ to S.

(2) Once receiving the request message, S generates a random number d_S and computes $Q_S = d_S P$, $Q_{SC} = d_S k_S^{-1} P$, and $V_S = h(ID_i \| Q_S \| Q_{SC})$. Finally, he sends the forged message $CHALLENGE(realm, Q_S, V_S)$ to $\mathscr{A}$ who impersonates as a legal user.

(3) After receiving the challenge message, $\mathscr{A}$ first checks $h(ID_i \| Q_S \| d_C' Q_S) \overset{?}{=} V_S'$. Obviously, the equation holds and $\mathscr{A}$ then computes $V_C = h(ID_i \| Q_S \| realm \| d_C' Q_S \| V_i \oplus h(ID_i \| k_S))$, $SK = h(ID_i \| Q_S \| realm \| d_C' Q_S)$ and sends the message $RESPONSE(ID_i, realm, V_C)$ to S.

(4) After receiving the response message, S checks whether $h(ID_i \| Q_S \| realm \| d_C' Q_S \| V_i \oplus h(ID_i \| k_S))$ is equal to the received V_C. If it is correct, S negotiates the common session key as $SK = h(ID_i \| Q_S \| realm \| d_C' Q_S)$ with $\mathscr{A}$ (Table 1).

In this way, S believes that he has successfully established the session key with U_i whereas it is the adversary who is making fool of S by imitating the legal user.

4.2. Trace Attack. In the authentication phase of Arshad and Nikooghadam's scheme, the user U_i sends the request messages containing the user's identity ID_i to S without any protection. Since the user's identity ID_i is sent over an open communication channel, $\mathscr{A}$ may intercept the message using the assumed capability. With the user's identity ID_i, $\mathscr{A}$ can trace it to know what kind of services the user accesses and how long the user logins into the system. Since S may have the system log recording what the user did, the user's privacy may be leaked. Furthermore, $\mathscr{A}$ may trace the user's location according to the user's IP address. The trace attack seriously invades the user's privacy and can be utilized to commit real crimes such as kidnappings.

4.3. Lack of Proper Mutual Authentication

(1) $\mathscr{A}$ eavesdrops the message $REQUEST(ID_i, R_C)$, and then $\mathscr{A}$ generates a random number d_C' and computes $R_C' = d_C' K_S$.

(2) $\mathscr{A}$ sends the forged message (ID_i, R_C') to S. Obviously, S will accept $\mathscr{A}$'s request because S does not verify the validity of the request message from U. Then, S generates a random number d_S and computes $Q_S = d_S P$, $Q_{SC}' = d_S k_S^{-1} R_C' = d_S R_C'$, $V_S' = h(ID_i \| Q_S \| Q_{SC}')$. Then, S delivers the message $CHALLENGE(realm, Q_S, V_S')$ to $\mathscr{A}$ who masquerades as a legal user.

(3) After receiving the message from S, $\mathscr{A}$ computes $Q_{CS}' = d_C' Q_S$ and checks whether $V_S = h(ID_i \| Q_S \| Q_{CS})$ is equal to the received V_S'. If it is true, $\mathscr{A}$ continues to compute $V_C' = h(ID_i \| Q_S \| realm \| Q_{CS}' \| v_i')$, $SK = h(ID_i \| Q_S \| Q_{CS}' \| realm)$, where $v_i = h(ID_i \| PW_i' \| N_C')$; both PW_i' and N_C' are the forged password and random number. Then, $\mathscr{A}$ delivers the message $RESPONSE(realm, ID_i, V_C')$ to S.

Table 1: Registration and authentication phase of Arshad and Nikooghadam's scheme.

	U_i		S
Registration	(1) *Generate* N_C *Compute* $v_i = h(ID_i \Vert PW_i \Vert N_C)$.	$\xrightarrow{(2)\ ID_i, v_i}$ *Secure Channel*	(3) *Compute* $V_i = v_i \oplus h(ID_i \Vert k_S)$. Store ID_i, V_i.
Authentication	(1) *Generate* d_C $R_C = d_C K_S$.		(3) *Generate* d_S $Q_S = d_S P$,
		$\xrightarrow{(2)\ REQUEST(ID_i, R_C)}$	$Q_{SC} = d_S k_S^{-1} R_C$, $V_S = h(ID_i \Vert Q_S \Vert Q_{SC})$.
		$\xleftarrow{(4)\ CHALLENGE(realm, Q_S, V_S)}$	
	(5) $Q_{CS} = d_C Q_S$,		
			(7) $v_i = V_i \oplus h(ID_i \Vert k_S)$,
	$h(ID_i \Vert Q_S \Vert Q_{CS}) \overset{?}{=} V_S$, $v_i = h(ID_i \Vert PW_i \Vert N_C)$, $V_C = h(ID_i \Vert Q_S \Vert realm \Vert Q_{CS} \Vert v_i)$, $SK = h(ID_i \Vert Q_S \Vert Q_{CS} \Vert realm)$.		$h(ID_i \Vert Q_S \Vert realm \Vert Q_{CS} \Vert v_i) \overset{?}{=} V_C$, $SK = h(ID_i \Vert Q_S \Vert Q_{CS} \Vert realm)$.
		$\xrightarrow{(6)\ RESPONSE(realm, ID_i, V_C)}$	

(4) Upon receiving the message from $\mathscr{A}$ who masquerades as a legal user, S computes $v_i = V_i \oplus h(ID_i \parallel k_S)$, $h(ID_i \parallel Q_S \parallel realm \parallel Q_{SC} \parallel v_i)$ and compares it with the received V_C. It is obvious that they are not equal, and then S immediately stops session.

In this condition, any one can forge and send the request message to S, which leads to S thinking U_i is a cheater, whereas U_i is actually an honest user. This obviously results in making great consumption of computing resources and communication resources.

5. Proposed Authentication Scheme for SIP

In this section, we propose a novel mutual authentication scheme based on ECC, which consists of three phases: registration, authentication, and password change.

5.1. Registration

(1) U_i freely selects his password PW_i and his own secret key k_{U_i} and generates a random number r_1. Then U_i computes $PWD = h(PW_i \parallel k_{U_i})$ and submits $\{ID_i, r_1, PWD\}$ to S through a secure channel.

(2) S computes $VPW = h(ID_i \parallel PWD \parallel r_1) \oplus h(k_S)$ and stores VPW in his database, where k_S is S's secret key.

5.2. Authentication

(1) U_i generates a random number r_2 and computes $T = h(ID_i \parallel PWD \parallel r_1)$, $R = r_2 P$, $M_1 = T r_2 P$, $AID = ID_i \oplus T$, and $M_2 = h(ID_i \parallel R)$. Then, U_i sends the message $REQUEST(M_1, AID, M_2)$ to S.

(2) On receipt of the request message from U_i, S derives T from VPW by computing $VPW \oplus h(k_S)$ and then he computes $ID_i' = AID \oplus T'$ and $R' = T^{-1} M_1$ and checks whether $M_2' = h(ID_i' \parallel R') \overset{?}{=} M_2$ holds or not. If it does not hold, S rejects the request. Otherwise, S generates a random number r_3 and computes $H = r_3 P$, $M_3 = ID_i \oplus H$, $SK_S = r_3 P$, and $Auth_S = h(SK_S \parallel T \parallel R)$. Finally, S sends the message $CHALLENGE(realm, M_3, Auth_S)$ to U_i.

(3) Upon receiving the challenge message from S, U_i retrieves H by computing $M_3 \oplus ID_i$ and then he computes $SK_{U_i} = r_2 H$ and verifies whether $Auth_S' = h(SK_{U_i} \parallel T \parallel R)$ is equal to the received $Auth_S$. If it is not correct, U_i stops the session. Otherwise, U_i computes $Auth_{U_i} = h(SK_{U_i} \parallel T \parallel H)$ and then sends the message $RESPONSE(realm, Auth_{U_i})$ to S.

(4) When receiving the response message from U_i, S checks if $Auth_{U_i}' = h(SK_S \parallel T \parallel H) \overset{?}{=} Auth_{U_i}$. If so, the session key shared between U_i and S is set as $SK = SK_{U_i} = SK_S$ (Table 2).

5.3. Password Change. In this subsection, U_i can change his password any time when he wants. U_i chooses a new password PW_i^{new}, a new secret key $k_{U_i}^{new}$, and a new random number r_1^{new}. Then the following process will be performed by U_i and S.

(1) U_i submits the message $h(h(ID_i \parallel r_1 \parallel h(PW_i \parallel r_1) \parallel SK))$ and $h(ID_i \parallel r_1^{new} \parallel h(PW_i^{new} \parallel r_1^{new}))$ to S.

(2) S computes $h(h(VPW \oplus h(k_S)) \parallel SK)$ and checks whether it is equal to the received $h(h(ID_i \parallel r_1 \parallel h(PW_i \parallel r_1) \parallel SK))$. If it is correct, S computes $VPW^{new} = SK \oplus h(ID_i \parallel r_1^{new} \parallel h(PW_i^{new} \parallel r_1^{new})) \oplus SK \oplus h(k_S)$ and then replaces VPW with VPW^{new}.

Table 2: Registration and authentication phase of our scheme.

	U_i		S
Registration	(1) *Generate* r_1		(3) *Compute*
	$PWD = h(PW_{U_i} \parallel k_{U_i})$.		$T = h(ID_i \parallel r_1 \parallel PWD)$,
		$\xrightarrow{(2)\, ID_i, r_1, PWD}$	$VPW = T \oplus h(k_S)$.
		Secure Channel	*Store* VPW.
Authentication	(1) *Generate* r_2		(2) *Compute*
	$T = h(ID_i \parallel r_1 \parallel PWD)$,		$T = VPW \oplus h(k_S)$,
	$R = r_2 P$,		$ID_i = AID \oplus T$,
	$M_1 = T \cdot r_2 P$,		$R = T^{-1} M_1$,
	$AID = ID_i \oplus T$,	$\xrightarrow{REQUEST(M_1, AID, M_2)}$	$h(R \parallel ID_i) \overset{?}{=} M_2$,
	$M_2 = h(R \parallel ID_i)$.		*Generate* r_3
			$H = r_3 P$,
	(3) $H = M_3 \oplus ID_i$,		$M_3 = ID_i \oplus H$,
		$\xleftarrow{CHALLENGE(realm, M_3, Auth_S)}$	
	$SK_{U_i} = r_2 H$,		$SK_S = r_3 R$,
	$h(SK_{U_i} \parallel T \parallel R \overset{?}{=} Auth_S$,		$Auth_S = h(SK_S \parallel T \parallel R)$.
			(4) $h(SK_S \parallel T \parallel H) = Auth_{U_i}$
	$Auth_{U_i} = h(SK_{U_i} \parallel T \parallel H)$.		
		$\xrightarrow{RESPONSE(realm, Auth_{U_i})}$	
		$SK = SK_{U_i} = SK_S$	

6. Analysis Security

In this section, we first adopt Burrows-Abadi-Needham (BAN) logic [26] to demonstrate that the proposed scheme is working correctly by achieving the authentication goals. Then, we conduct a security analysis of the enhanced scheme through both the informal and formal analyses.

BAN Logic Notations

$A| \equiv X$: A believes a statement X

$U_i \overset{K}{\longleftrightarrow} S$: share a key K between U_i and S

$\#X$: X is fresh

$A \triangleleft X$: A sees X

$A| \sim X$: A said X

$\{X, Y\}_K$: X and Y are encrypted with the key K

$(X, Y)_K$: X and Y are hashed with the key K

$\langle X \rangle_K$: X is xor-ed with the key K.

6.1. Verifying Authentication Scheme with BAN Logic. BAN logic [26] is a set of rules for defining and analyzing information exchange schemes. It helps its users determine whether exchanged information is trustworthy, secured against eavesdropping, or both. It has been highly successful in analyzing the security of authentication schemes [27, 28]. In this subsection, we prove that a session key between communicating parties can be correctly generated within authentication process using BAN logic. First, we introduce some notations and logical postulates of BAN logic that we will use in our scheme.

(1) BAN logical postulates the following.

(a) Message-meaning rule $(A| \equiv A \overset{K}{\longleftrightarrow} B, A \triangleleft \{X\}_K)/(A| \equiv |B \sim X)$: if A believes that the key K is shared by A and B and sees X encrypted with K, then A believes that B once said X.

(b) Nonce-verification rule $(A| \equiv \#X, A| \equiv B| \sim X)/(A| \equiv B| \equiv X)$: if A believes that X could have been uttered only recently and that B once said X, then A believes that B believes X.

(c) The belief rule $(A| \equiv X, A| \equiv Y)/(A| \equiv (X, Y))$: if A believes X and Y, then A believes (X, Y).

(d) Fresh conjuncatenation rule $(A| \equiv \#X)/(A| \equiv \#(X, Y))$: if A believes freshness of X, B believes freshness of (X, Y).

(e) Jurisdiction rule $(A| \equiv B \Rightarrow X, A| \equiv B| \equiv X)/(A| \equiv X)$: if A believes that B has jurisdiction over X and A believes B on the truth of X, then A believes X.

(2) Idealized scheme:

$$U_i\text{: } R_{U_i \overset{T}{\longleftrightarrow} S}, \langle ID_i \rangle_{U_i \overset{T}{\longleftrightarrow} S}, (ID_i)_R, (U_i \overset{SK}{\longleftrightarrow} S, H)_{U_i \overset{T}{\longleftrightarrow} S},$$

$$S\text{: } (U_i \overset{SK}{\longleftrightarrow} S, R)_{U_i \overset{T}{\longleftrightarrow} S}, \langle ID_i \rangle_H.$$

(3) Establishment of security goals:

$$(g_1)\ S| \equiv U_i| \equiv U_i \overset{SK}{\longleftrightarrow} S,$$

(g_2) $S| \equiv U_i \overset{SK}{\longleftrightarrow} S$,

(g_3) $U_i| \equiv S| \equiv U_i \overset{SK}{\longleftrightarrow} S$,

(g_4) $U_i| \equiv U_i \overset{SK}{\longleftrightarrow} S$.

(4) Initiative premises:

(p_1) $U_i| \equiv \#r_1$,

(p_2) $U_i| \equiv \#r_2$,

(p_3) $S| \equiv \#r_3$,

(p_4) $U_i| \equiv U_i \overset{T}{\leftrightarrow} S$,

(p_5) $S| \equiv U_i \overset{T}{\leftrightarrow} S$,

(p_6) $U_i| \equiv S \Rightarrow (U_i \overset{SK}{\longleftrightarrow} S)$,

(p_7) $S| \equiv U_i \Rightarrow (U_i \overset{SK}{\longleftrightarrow} S)$.

(5) Scheme analysis: consider the following.

(a_1) Since p_4 and $U_i \triangleleft (U_i \overset{SK}{\longleftrightarrow} S, R)_{U_i \overset{T}{\leftrightarrow} S}$, we apply the message-meaning rule to obtain $U_i| \equiv S| \sim (U_i \overset{SK}{\longleftrightarrow} S, R)$.

(a_2) Since p_2 and a_1, we apply the fresh conjuncatenation rule and nonce-verification rule to obtain $U_i| \equiv S| \equiv (U_i \overset{SK}{\longleftrightarrow} S, R)$.

(g_1) Since a_2, we apply the belief rule to obtain $U_i| \equiv S| \equiv U_i \overset{SK}{\longleftrightarrow} S$.

(g_2) Since p_6 and g_1, we apply the jurisdiction rule to obtain $U_i| \equiv U_i \overset{SK}{\longleftrightarrow} S$.

(a_3) Since p_5 and $S \triangleleft (U_i \overset{SK}{\longleftrightarrow} S, H)_{U_i \overset{T}{\leftrightarrow} S}$, we apply the message-meaning rule to obtain $S| \equiv U_i| \sim (U_i \overset{SK}{\longleftrightarrow} S, H)$.

(a_4) Since p_3 and a_3, we apply the fresh conjuncatenation rule and nonce-verification rule to obtain $S| \equiv U_i| \equiv (U_i \overset{SK}{\longleftrightarrow} S, H)$.

(g_3) Since a_4, we apply the belief rule to obtain $S| \equiv U_i| \equiv U_i \overset{SK}{\longleftrightarrow} S$.

(g_4) Since g_3 and p_7, we apply the jurisdiction rule to obtain $S| \equiv U_i \overset{SK}{\longleftrightarrow} S$.

By analyzing the security of our scheme with BAN logic, the results demonstrate that the proposed scheme can effectively achieve the security goal of the mutual authentication of U_i and S.

6.2. Informal Security Analysis. In this subsection, we will examine whether the enhanced scheme is safe and consider its ability to resist various known attacks. The following attacks are also based on the assumptions that a malicious adversary $\mathscr{A}$ has total control over the communication channel connecting U_i and S in authentication phase. So $\mathscr{A}$ can intercept, insert, delete, or modify any messages transmitted via public channel [22–24].

6.3. User is Anonymous and Untraceable. Suppose $\mathscr{A}$ eavesdrops the request messages $REQUEST(M_1, AID, M_2)$, the challenge message $CHALLENGE(realm, M_3, Auth_S)$, and the response message $RESPONSE(realm, Auth_{U_i})$ from the public channel. To obtain ID_i from these values by means of guessing and verifying, $\mathscr{A}$ must have the knowledge of $\{\{PW_i, r_1, k_{U_i}\}, \{r_3\}, \{r_2\}\}$. Due to U_i and S compute different M_1 and M_3 with a new random number (r_1, r_2) and r_3 for each session, and $\mathscr{A}$ is not able to trace who communicates with S by monitoring the channel. This shows the proposed scheme provides the attribute of anonymous.

6.4. Insider Attack. In our scheme, it is computationally impossible to derive the password PW_i from the $PWD = h(PW_i \parallel k_{U_i})$ because of the difficulties of hash function with the secret key k_{U_i} of U_i. Therefore, the proposed scheme can withstand the insider attack.

6.5. Perfect Forward Secrecy. If U_i's password PW_i, the secret key k_{U_i}, and S's secret key k_S are all compromised, this does not allow $\mathscr{A}$ to determine the session key SK for the past session. $\mathscr{A}$ cannot compute $r_1 r_2 P$ from M_1 and M_3 because of secure one-way hash function and $ECDLP$.

6.6. Mutual Authentication. In our scheme, S and U_i can authenticate each other by checking M_2, $Auth_{U_i}$, and $Auth_S$, separately. Therefore, our scheme can provide mutual authentication.

6.7. Key-Compromise Impersonation Attack. Assume that $\mathscr{A}$ intercepts the request, the challenge, and the response messages. Supposing the secret key k_{U_i} of U_i is compromised by $\mathscr{A}$, he cannot go through the verification process of U as the random number r_1 is not known. On the other hand, supposing the secret key k_S of S is compromised by $\mathscr{A}$, he cannot impersonate U to cheat S. Since $\mathscr{A}$ cannot know the values of the identity ID_i and r_1 of U_i, he cannot compute the correct value T and hence cannot be authenticated by S. Therefore, the proposed scheme can withstand the key-compromise impersonation attack.

6.8. Replay Attack. Assuming that $\mathscr{A}$ eavesdrops $REQUEST(M_1, AID, M_2)$ and replays it to impersonate U_i, S then verifies the condition $M_2 \overset{?}{=} h(r_2 P \parallel ID_i)$. The message verification does not hold, so try to guess r_2 from R is the $ECDLP$ and r_2 is different in each authentication message. On the other hand, suppose $\mathscr{A}$ eavesdrops $CHALLENGE(realm, M_3, Auth_S)$ and replays it to impersonate S. The replied message cannot pass the verification process $Auth_S = h(SK_S \parallel h(ID_i \parallel PWD \parallel r_1) \parallel r_2 P)$, since both r_1 and r_2 are new random numbers chosen by U_i in each session, and $\mathscr{A}$ has no control of it. Therefore, $\mathscr{A}$ has no opportunity to successfully replay used messages.

6.9. Offline Password Guessing Attack. Even if $\mathscr{A}$ intercepts all the exchanged messages $(M_1, M_2, AID, M_3, Auth_{U_i}, Auth_S)$ by passive attack, he cannot guess the correct password of U_i.

```
Eavesdrop request message $REQUEST(M_1, AID, M_2)$
Call the reveal oracle 2. Let $(T', r_2') \leftarrow Reveal2(M_1)$
Call the reveal oracle 1. Let $(ID_i', PW_i', r_1') \leftarrow Reveal1(T')$
Eavesdrop challenge message $CHALLENGE(realm, M_3, \mathrm{Auth}_S)$
Call the reveal oracle 1. Let $(SK', T'', R') \leftarrow Reveal1(Auth_S)$
Call the reveal oracle 2. Let $(r_2'') \leftarrow Reveal2(R')$
if $(r_2' = r_2'')$ then
    Accept the derived $ID_i'$, $PW_i'$, and $SK'$ as the correct $ID_i$ and $PW_i$ of the user $U_i$
    and the session key $SK$ between $U_i$ and $S$, respectively
        return 1 (success)
else
        return 0 (failure)
end if
```

Algorithm 1: Algorithm $EXP^{REASSIP,\mathscr{A}}_{HASH,ECDLP}$.

Since $\mathscr{A}$ cannot know the values of the user's identity ID_i, the secret key k_{U_i}, and the random number r_1, he cannot compute the value $T = h(ID_i \parallel r_1 \parallel h(PW_i \parallel k_{U_i}))$ to verify the guessed password PW_i through the recorded messages. Therefore, our scheme can resist the offline password guessing attack.

6.10. Known Session Key Security. Because of the randomness and independence of the generations of r_1 and r_3 in all the sessions, the session key $SK = r_1 r_3 P$ of each session is independent of that of any other sessions. Therefore, the proposed scheme can ensure known session key security.

6.11. Formal Security Analysis of the Proposed Scheme. In this subsection, we provide the formal security analysis of our scheme and show that our scheme is secure. We first define the following oracles.

Reveal 1. This random oracle will unconditionally output the input x from the given hash value $y = h(x)$.

Reveal 2. This random oracle will unconditionally output m from given points P and $Q = mP$ in an elliptic curve $E_p(a, b)$.

Theorem 1. *Under the ECDLP assumption, our scheme is secure against an adversary $\mathscr{A}$ for deriving the identity ID_i and password PW_i of a legal user U_i and the session key SK between U_i and S if the hash function $h(\cdot)$ closely behaves like a random oracle.*

Proof. The formal security proof of our scheme is similar to that as in [29–31]. $\mathscr{A}$ runs the experimental algorithm showed in Algorithm 1, $EXP^{REASSIP,\mathscr{A}}_{HASH,ECDLP}$ for our robust, and efficient authentication scheme for session initiation protocol; say *REASSIP*.

Define the success probability for $EXP^{REASSIP,\mathscr{A}}_{HASH,ECDLP}$ as $Succ^{REASSIP,\mathscr{A}}_{HASH,ECDLP} = |2Pr[EXP^{REASSIP,\mathscr{A}}_{HASH,ECDLP} = 1] - 1|$ and the advantage function for this experiment then becomes $Adv^{REASSIP,\mathscr{A}}_{HASH,ECDLP}(t, q_{R_1}, q_{R_2}) = \max_{\mathscr{A}} Succ^{REASSIP}_{HASH,ECDLP}$, where the maximum is taken over all $\mathscr{A}$ with execution time t, and the number of queries q_{R_1}, q_{R_2} made to the Reveal 1 and Reveal 2 oracles, respectively. If $\mathscr{A}$ has the ability to solve the hash function and the *ECDLP*, then he can directly derive U_i's identity ID_i, password PW_i, and the session key SK between U_i and S. In this case, $\mathscr{A}$ will discover the complete connections between U_i and S. However, it is a computationally infeasible problem to invert the input from a given hash value and output m from given points P, Q; that is, $Adv^{\mathscr{A}}_{HASH}(t_1) \leq \epsilon$, $Adv^{\mathscr{A}}_{ECDLP}(t_2) \leq \epsilon$, $\forall \epsilon > 0$. Hence, we have $Adv^{REASSIP,\mathscr{A}}_{HASH,ECDLP}(t, q_{R_1}, q_{R_2}) \leq \epsilon$, as it is dependent on $Adv^{\mathscr{A}}_{HASH}(t_1)$ and $Adv^{\mathscr{A}}_{ECDLP}(t_2)$. Therefore, our scheme is probably secure against $\mathscr{A}$ for deriving ID_i, PW_i, and SK. □

7. Security Properties and Performance Comparison

In this section, we show that our proposed scheme satisfies many security attributes and has lower computation cost. Security properties and performance cost comparisons between our scheme and the other related schemes in [13–20] are given in Table 3 and Figure 1, respectively.

Table 3 shows that our scheme is more secure than Arshad et al.'s scheme and other related schemes and achieves more functionality features. In performance comparison, we mainly focus on computations of the authentication phase, since it is the main body of an authentication scheme, and the registration phase only performs one time before authentication. Let PA, PM, INV, SE, M, and H be the time for performing an elliptic curve point addition, an elliptic curve point multiplication, a modular inversion, a symmetric key encryption or decryption, a modular multiplication, and a hash function. Since xor operations require very little computations, we omitted it. From Figure 1 we can see that our scheme has similar or better efficiency in comparison with other related ECC-based authentication schemes.

8. Conclusion

We have analyzed the security of a recently proposed Arshad et al.'s SIP authentication scheme. We have pointed out that

Table 3: Comparison of security attributes.

	Ours	Arshad and Ikram [13]	Yoon et al. [14]	Xie [15]	Farash and Attari [16]	Zhang et al. [17]	Tu et al. [18]	Irshad et al. [19]	Arshad and Nikooghadam [20]
T_1	Yes	No	No	No	No	—	No	No	No
T_2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
T_3	Yes	Yes	Yes	Yes	Yes	Yes	—	Yes	Yes
T_4	Yes	Yes	Yes	Yes	—	—	—	Yes	Yes
T_5	Yes	No	No	No	No	No	Yes	Yes	Yes
T_6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
T_7	Yes	—	—	—	—	—	—	—	—
T_8	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes

T_1: providing anonymity and untraceable; T_2: providing mutual authentication; T_3: providing perfect forward secrecy; T_4: known session key security; T_5: resist insider attack; T_6: resist replay attack; T_7: resist key-compromise impersonation attack; T_8: resist offline password guessing attack.

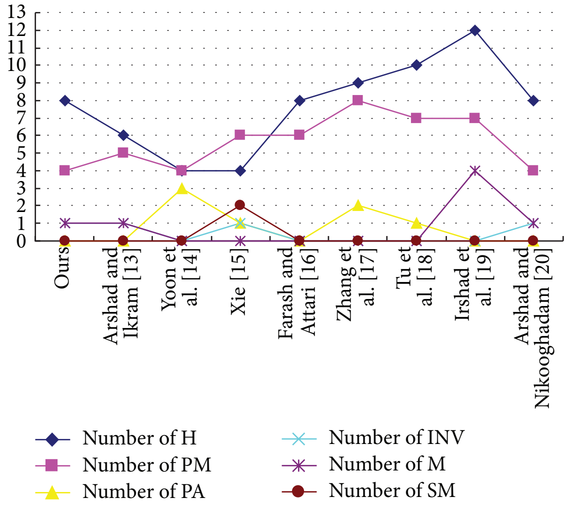


Figure 1: Comparison of computational cost.

an adversary can successfully launch the trace and key-compromise impersonation attacks on Arshad et al.'s scheme. We also have shown that Arshad et al.'s scheme does not achieve proper mutual authentication. The cryptanalysis of Arshad and Nikooghadam's scheme thus shows that the security of their scheme is compromised. In order to eliminate the security pitfalls found in Arshad et al.'s scheme, we have then presented a robust and efficient ECC based authentication scheme for SIP. Our scheme is immune to the trace, key-compromise impersonation, and insider attacks which Arshad and Nikooghadam's scheme fails to satisfy. Meanwhile, our scheme can withstand the replay, offline password guessing, and insider attacks. In addition, our scheme achieves the known session key security and perfect forward secrecy. We present a cryptanalysis of our scheme through both informal and formal security analyses. Besides, our scheme is computationally efficient as compared to other related ECC based SIP authentication schemes. Considering the security and efficiency provided by our scheme, we conclude that our scheme is more appropriate for practical applications in comparison with other related schemes.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors are grateful to the anonymous referees for their valuable comments and suggestions to improve the presentation of this paper. This paper is supported by the National Natural Science Foundation of China (Grant nos. 61472045 and 61121061), the Beijing Higher Education Young Elite Teacher Project (Grant no. YETP0449), the Asia Foresight Program under NSFC Grant (Grant no. 61411146001), and the Beijing Natural Science Foundation (Grant no. 4142016).

References

[1] C. Shen, E. Nahum, H. Schulzrinne, and C. P. Wright, "The impact of TLS on SIP server performance: measurement and modeling," *IEEE/ACM Transactions on Networking*, vol. 20, no. 4, pp. 1217–1230, 2012.

[2] S. Salsano, L. Veltri, and D. Papalilo, "SIP security issues: the SIP authentication procedure and its processing load," *IEEE Network*, vol. 16, no. 6, pp. 38–44, 2002.

[3] C.-C. Yang, R.-C. Wang, and W.-T. Liu, "Secure authentication scheme for session initiation protocol," *Computers and Security*, vol. 24, no. 5, pp. 381–386, 2005.

[4] H. Huang, W. Wei, and G. E. Brown, "A new efficient authentication scheme for session initiation protocol," in *Proceedings of the 9th Joint Conference on Information Sciences*, 2006.

[5] H. Jo, Y. Lee, M. Kim, S. Kim, and D. Won, "Off-line password-guessing attack to Yang's and Huang's authentication schemes for session initiation protocol," in *Proceedings of the 5th International Joint Conference on INC, IMS and IDC (NCM '09)*, pp. 618–621, August 2009.

[6] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," *World Enformatika Socity Transactions on Engineering Computing and Technology*, vol. 8, pp. 350–353, 2005.

[7] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[8] Y.-P. Liao and S.-S. Wang, "A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves," *Computer Communications*, vol. 33, no. 3, pp. 372–380, 2010.

[9] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 286–291, 2009.

[10] E.-J. Yoon, K.-Y. Yoo, C. Kim, Y.-S. Hong, M. Jo, and H.-H. Chen, "A secure and efficient SIP authentication scheme for converged VoIP networks," *Computer Communications*, vol. 33, no. 14, pp. 1674–1681, 2010.

[11] Q. Pu, "Weaknesses of SIP authentication scheme for converged VoIP networks," IACR Cryptology ePrint Archive 464, 2010, http://eprint.iacr.org/2010/464.

[12] J. L. Tsai, "Efficient nonce-based authentication scheme for session initiation protocol," *International Journal of Network Security*, vol. 8, no. 3, pp. 312–316, 2009.

[13] R. Arshad and N. Ikram, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," *Multimedia Tools and Applications*, vol. 66, no. 2, pp. 165–178, 2013.

[14] E.-J. Yoon, Y.-N. Shin, I.-S. Jeon, and K.-Y. Yoo, "Robust mutual authentication with a key agreement scheme for the session initiation protocol," *IETE Technical Review*, vol. 27, no. 3, pp. 203–213, 2010.

[15] Q. Xie, "A new authenticated key agreement for session initiation protocol," *International Journal of Communication Systems*, vol. 25, no. 1, pp. 47–54, 2012.

[16] M. S. Farash and M. A. Attari, "An enhanced authenticated key agreement for session initiation protocol," *Information Technology and Control*, vol. 42, no. 4, pp. 333–342, 2013.

[17] L. Zhang, S. Tang, and Z. Cai, "Efficient and flexible password authenticated key agreement for Voice over Internet Protocol Session Initiation Protocol using smart card," *International Journal of Communication Systems*, vol. 27, no. 11, pp. 2691–2702, 2014.

[18] H. Tu, N. Kumar, N. Chilamkurti, and S. Rho, "An improved authentication protocol for session initiation protocol using smart card," *Peer-to-Peer Networking and Applications*, 2014.

[19] A. Irshad, M. Sher, S. A. Ch, M. U. Hassan, and A. Ghani, "A single round-trip SIP authentication scheme for Voice over Internet Protocol using smart card," *Multimedia Tools and Applications*, 2013.

[20] H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC," *Multimedia Tools and Applications*, 2014.

[21] P. Sarka, "A simple and generic construction of authenticated encryption with associated data," *ACM Transactions on Information and System Security*, vol. 13, no. 4, article 33, 2010.

[22] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[23] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. Shalmani, "On the power of power analysis in the real world: a complete break of the KeeLoq code hopping scheme," in *Advances in Cryptology—CRYPTO 2008*, vol. 5157 of *Lecture Notes in Computer Science*, pp. 203–220, Springer, Berlin, Germany, 2008.

[24] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Computers and Security*, vol. 18, no. 8, pp. 727–733, 1999.

[25] M. Hölbl, T. Welzer, and B. Brumen, "An improved two-party identity-based authenticated key agreement protocol using pairings," *Journal of Computer and System Sciences*, vol. 78, no. 1, pp. 142–150, 2012.

[26] M. Burrows, M. Abadi, and R. Needham, "Logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

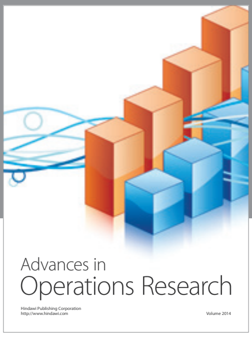
[27] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 4, pp. 2004–2013, 2013.

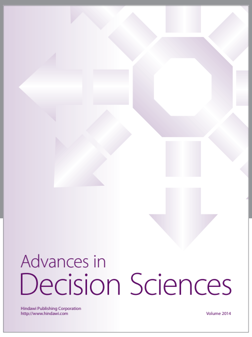
[28] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247–269, 2013.

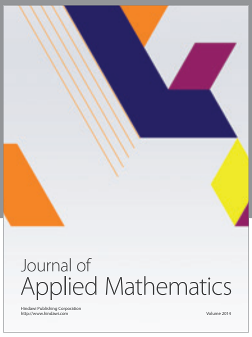
[29] V. Odelu, A. K. Das, and A. Goswami, "A secure effective key management scheme for dynamic access control in a large leaf class hierarchy," *Information Sciences*, vol. 269, pp. 270–285, 2014.

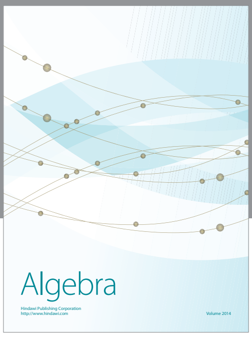
[30] S. Chatterjee, A. K. Das, and J. K. Sing, "An enhanced access control scheme in wireless sensor networks," *Ad-Hoc and Sensor Wireless Networks*, vol. 21, no. 1-2, pp. 121–149, 2014.

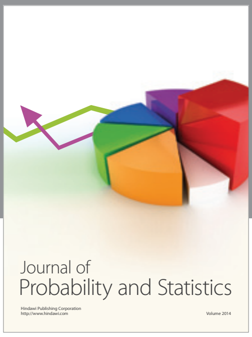
[31] A. K. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 37, no. 3, article 9948, 2013.


Advances in
Operations Research

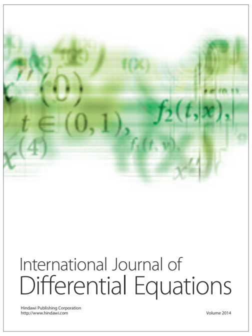

Advances in
Decision Sciences


Journal of
Applied Mathematics

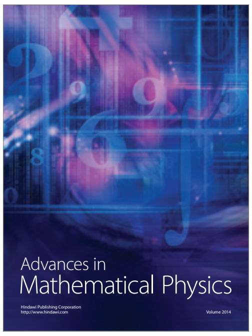

Algebra

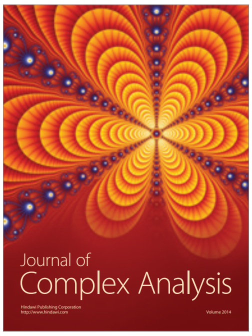

Journal of
Probability and Statistics

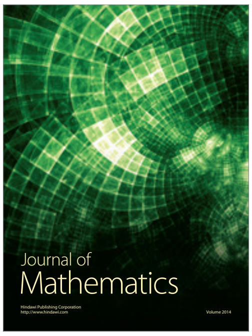
The Scientific
World Journal

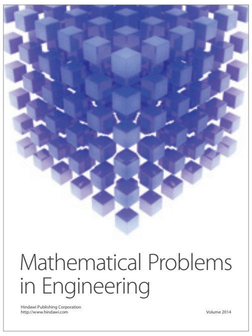

International Journal of
Differential Equations

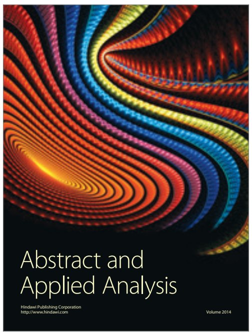
International Journal of
Combinatorics

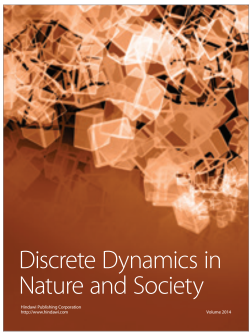

Advances in
Mathematical Physics

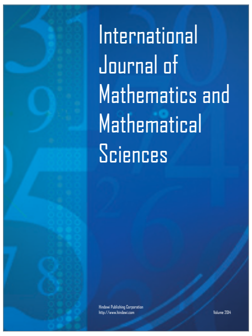

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

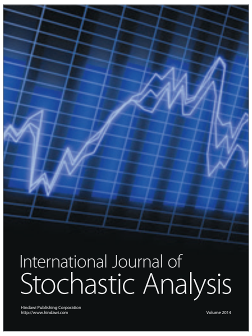

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization