An Efficient Authenticated Key Transfer Scheme in Client-Server Networks

Runhua Shi and Shun Zhang*
School of Computer Science and Technology, Anhui University, Hefei City, China
Email: shirh@ahu.edu.com, *shzhang27@163.com

Abstract. In this paper, we presented a novel authenticated key transfer scheme in client-server networks, which can achieve two secure goals of remote user authentication and the session key establishment between the remote user and the server. Especially, the proposed scheme can subtly provide two fully different authentications: identity-base authentication and anonymous authentication, while the remote user only holds a private key. Furthermore, our scheme only needs to transmit 1-round messages from the remote user to the server, thus it is very efficient in communication complexity. In addition, the most time-consuming computation in our scheme is elliptic curve scalar point multiplication, so it is also feasible even for mobile devices.

1. Introduction
Secure remote user authentication over insecure channel is an important issue for many distributed applications, especially electronic transactions (e.g., on-line shopping, Internet banking and pay-TV). Furthermore, in order to ensure the session’s confidentiality, it needs to establish a secure session key between the remote user and the server over insecure communication channel. Therefore, remote user authentication with key establishment in client-server networks is becoming the focus of widely attentions.

Currently, there appeared lots of novel authenticated key transfer schemes [1-12] in client-server networks. According to the way of authentications among these schemes, there are two well-known but fully different categories: identity-based authentication and anonymous authentication.

With our best knowledge, there is not a scheme that can meet both two different authentication requests, i.e., identity-based authentication and anonymous authentication. However, in some real applications, it needs to provide different authentications according to the different conditions. For example, suppose there is a client-server system, which is composed of a server and multiple remote users. The server manages an important storage space (or database), which is shared (or created) by all legal users. When a remote user wants to upload files (or data) to the storage space (or database) of the server, the server must authenticate the identity of the user to avoid false or illegal files (or data). However, when he downloads files (or data) from the server, the user expects to guarantee his anonymity. In fact, there are lots of similar application scenarios, what’s more, e.g., in some private forums, it needs the registered user to publish the information in the real-name way, but it is anonymous to browse the information.

Motivated by these concerns, in this paper, we present a novel authenticated key transfer scheme for client-server networks, which can satisfy both two different authentications under the condition of the user only holding a private key in secret. Obviously, this scheme can not only save system resources, but can also help the server to more efficiently manage the users’ private keys.
1.1 Related work
In 2009, to achieve two secure goals of remote user authentication and key establishment between the remote user and the server in client-server networks, Yang and Chang [1] proposed an efficient identity-based and authenticated key agreement protocol. However, Yoon and Yoo [2] demonstrated that Yang and Chang’s protocol is vulnerable to the impersonation attack and does not provide perfect forward secrecy, and then proposed an improved protocol. Later, He et al. [3] again confirmed that Yoon and Yoo’s protocol does not provide perfect forward secrecy yet and fails to achieve forward secrecy. In addition, they also pointed out that a special hash function called MapToPoint function which is used to map an identity information into a point on elliptic curve is required in the previous protocols. To improve the efficiency, they presented a new remote user authentication protocol without the MapToPoint function [3]. Subsequently, there appeared more improved protocols of authenticated key establishment for client-server networks [4-7].

The authentications in the protocols mentioned above are all identity-based (i.e., identifiable), which cannot protect user’s privacy. For this, Islam and Biswas [8] proposed an anonymous authentication protocol with key establishment, but only against outside attackers. In 2014, Kumari et al. [9] proposed a password-based anonymous authentication scheme similarly against the outside adversary. However, Chaudhry et al. [10] analyzed that Kumari et al.’s scheme is vulnerable to anonymity violation attack, and further proposed an improved anonymous authentication scheme. Later, Liu et al. [11] presented certificateless remote anonymous authentication schemes against outside attackers for wireless body area networks. Recently, Shi et al. [12] presented a novel anonymous and authenticated key transfer protocol in client-server networks, which perfectly protects the remote user’s anonymity against not only outside attackers, but also other legal users and the server. In addition, for secure roaming services in wireless networks, Yang et al. [13] presented two efficient anonymous roaming protocols, and defined the notion of Strong User Anonymity that protects user’s identity against both eavesdroppers and foreign servers. In the same year, Chang and Tsai [14] presented an anonymous and self-verified mobile authentication scheme with key agreement in large-scale wireless networks. Subsequently, similar anonymous authentication schemes for secure roaming services were proposed [15-18].

1.2 Contributions
In this paper, we present a novel authenticated key transfer scheme for client-server networks. Compared with existing authentication key establishment schemes in client-server networks, our scheme has the following advantages:

(1) In the proposed scheme, by using the same private key, the user can complete two fully different kinds of authentications: identity-based authentication and anonymous authentication.

(2) In order to achieve two secure goals: user authentication and session key establishment between the remote user and the server, the proposed scheme only needs to send 1-round messages. Thus, it is very efficient in communication complexity.

(3) In the proposed scheme, the most time-consuming operation is elliptic curve scalar point multiplication, so it is feasible even for mobile devices.

(4) In the proposed scheme, the server does not need to store the private keys of all authorized users. Thus, it reduces the risk of the leakage of these keys.

(5) The proposed scheme can provide the confirmation of the user’s private key.

2. Proposed Scheme
The proposed scheme mainly includes three phases: Initialization, User Registration, and Authentication with Key Transfer, where the last phase includes two different kinds of authentications: identity-based authentication and anonymous authentication. The detailed description is as follows:

2.1 Initialization
The server generates the system parameters as follows: (1) The server chooses an elliptic curve equation $E_p(a, b)$ defined on finite field $F_p$ [19-22], where $p$ is a large prime. (2) The server selects a base point $P$ with the prime order $q$ over $E_p(a, b)$. (3) The server randomly generates its master key
and computes the corresponding public key \( Q_s = k_sP \). (4) In addition, the server chooses a secure hash function, \( H: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^* \). (5) Finally, the server publishes these system parameters: \( \{p, E_p(a, b), q, P, Q_s, H(\cdot)\} \).

### 2.2 User Registration

**Step 1.** Each user \( u_i \) (1 ≤ i ≤ n) sends his identity, \( ID_i \), to the server. Then the server checks the authenticity and legality of each identity. After confirming the authenticity and legality of the user \( u_i \), the server prepares a smart card including a secret \( k_i \), where \( k_i = H(ID_{i1}, ID_{i2}, k_s) \). Here \( ID_{i1} \) and \( ID_{i2} \) denote the identities of the user \( u_i \) and the server, respectively, and \( k_s \) is the master key of the server. Then the server privately sends the smart card with the secret \( k_i \) to the user \( u_i \).

**Step 2.** Suppose that in all there are \( n \) authorized users who have each obtained their respective secret \( k_i \)'s. The server constructs a polynomial function \( f(x) \) by all secrets, \( k_i \)'s, as follows:

\[
f(x) = (x - k_1)(x - k_2)\cdots(x - k_n) \mod q
\]

The above function can be rewritten as the following expression,

\[
f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \mod q
\]

Furthermore, the server computes and publishes: \( \{c_0P, c_1P, c_2P, \ldots, c_{n-1}P\} \) and \( \{c_2Q_s, c_3Q_s, \ldots, c_{n-1}Q_s\} \) on his bulletin board. In addition, the server announces two lists of the authorized users and the revoked users. Finally, the server deletes all \( k_i \)'s and \( c_i \)'s (for \( i = 1 \) to \( n \)), while he only privately holds the master key, \( k_s \), and the coefficient of the constant term of \( f(x) \), \( c_0 \), which can be stored in a smart card for security considerations.

**Step 3.** By the public information of the server, each user \( u_i \) verifies the validity of the secret in his smart card as follows.

Compute:

\[
Ki = k_i^n P + k_i^{n-1} (c_{n-1} P) + \cdots + k_i^2 (c_2 P) + k_i (c_1 P)
\]

Verify:

\[
Ki = -(c_0 P)
\]

Otherwise, he broadcasts a complaint about the dishonesty of the server to the whole client-server networks. After a waiting period, if he does not receive any complaint about the server, then the user \( u_i \) believes that the server is honest.

### 2.3 Identity-based Authentication with Key Transfer

**Step 1.** Suppose that the \( i \)-th user \( u_i \) requests the server to verify his legality and expects to share a session key between him and the server. The user \( u_i \) inserts the smart card into the terminal device, reads out his private key \( k_i \), and further computes \( U, V, w \) and \( k \) by the following equations:

\[
U = rP
\]

\[
(Q_x, Q_y) = rk_iQ_s
\]

\[
V = S \oplus Q_x
\]

\[
w = H(S, t, ID_i)
\]

\[
k = H(S, t, 1)
\]

Where \( r \in \mathbb{Z}_q^* \), \( S \in \mathbb{Z}_q^* \), \( Q_x \) and \( Q_y \) denote the x and y coordinates of the point \( rk_iQ_s \), \( t \) is a timestamp that denotes the current time, and \( k \) is a session key for later communications between the user \( u_i \) and
the server. Furthermore, the user $u_i$ sends the messages $\{ID_i, U, V, w, t\}$ to the server. Finally the user $u_i$ takes out the smart card and deletes $r$ and $S$ from the memory.

**Step 2.** After receiving the messages $\{ID_i, U, V, w, t\}$ from the user $u_i$, the server verifies if $t$ is valid. If $t$ is not fresh, the server aborts the process; otherwise, he performs the next step.

**Step 3.** The server computes:

$$k_i = H(ID_i, ID_j, k_i)$$

$$(Q_i, Q'_i) = k_i, k_i U$$

$$S' = V \oplus Q'_i$$

Then he verifies if $w = H(S', t, ID_j)$ holds. If the equation holds, the verification passes successfully. Furthermore, the server computes the session key $k = H(S', t, 1)$. Otherwise, the verification fails.

### 2.4 Anonymous Authentication with Key Transfer

**Step 1.** Suppose that the $i$-th user $u_i$ requests the server to verify his legality and expects to share a session key between him and the server. Then the user $u_i$ inserts the smart card into the terminal device, reads out his private key $k_i$ and further computes $Q_i$ by the server’s public information and his private key $k_i$:

$$Q_i = k_i^x Q_s + k_i^{i+1} (c_{e_i} Q_s) + \cdots + k_i^j (c_i Q_s) + k_i^j (c_i Q_s)$$

Further he computes:

$$U = rP$$

$$(Q_i, Q'_i) = rQ_i$$

$$V = S \oplus Q_i$$

$$w = H(S, t, 0)$$

$$k = H(S, t, 1)$$

Where $r \in R$ and $t$ is a timestamp that denotes the current time, and $k$ is a session key for future communications between the user $u_i$ and the server. Furthermore, the user $u_i$ sends the messages $\{U, V, w, t\}$ to the server. Finally the user $u_i$ takes out the smart card, and deletes $r, S$ and $Q_i$ from the memory.

**Step 2.** After receiving the messages $\{U, V, w, t\}$ from the user $u_i$, the server verifies if $t$ is valid. If $t$ is not fresh, the server aborts the process; otherwise, he performs the next step.

**Step 3.** The server computes and further verifies,

$$Q_i = Q'_i - c_i k_i U$$

$$S' = V \oplus Q'_i$$

$$w = H(S', t, 0)$$

If the above equation holds, the verification passes successfully. That is, the server confirms that the initiator of this session (i.e., the user $u_i$) is an authorized user. Finally, the server computes the session key $k = H(S', t, 1)$. Otherwise, the verification fails.

### 3. Analysis

The security of our scheme mainly relies on the difficulties of solving Elliptic Curve Discrete Logarithm (ECDL) problem (Given two points $P$ and $Q$ over an elliptic curve $E_p(a, b)$, it is computationally infeasible to find an integer $k$ such that $Q = k \cdot P$) and Elliptic Curve Computational Diffie-Hellman (ECCDH) problem (Given three points $P, a \cdot P$ and $b \cdot P$ over $E_p(a, b)$, it is
computationally infeasible to compute a point \( \mathbf{W} \) such that \( \mathbf{W} = a \mathbf{b} \cdot \mathbf{P} \) [5]. And then, we give Performance comparisons of some related schemes.

### 3.1 Security Analysis

In this section, we analyze that the proposed scheme can withstand various related security attacks.

#### 3.1.1 Outside Attack

Assume that an outside attacker wants to compute \( k_t \) from the public information \( \{ c_0 \mathbf{P}, c_1 \mathbf{P}, c_2 \mathbf{P}, \ldots, c_{n-1} \mathbf{P} \} \) or \( \{ c_0 \mathbf{Q}_s, c_1 \mathbf{Q}_s, \ldots, c_{n-1} \mathbf{Q}_s \} \) of the server. On the one hand, based on the difficulty of solving ECDL problem, the attacker can obtain the corresponding coefficients \( c_0, c_1, \ldots, c_{n-1} \), and then directly get \( k_t \) by solving the linear equation of \( f(x) = 0 \mod q \). On the other hand, if the attacker first guesses \( k \) and directly computes \( f(k)\mathbf{P} \) by the public information \( \{ c_0 \mathbf{P}, c_1 \mathbf{P}, c_2 \mathbf{P}, \ldots, c_{n-1} \mathbf{P} \} \), then he can verify if \( k \) is a valid secret, that is, he can verify if \( f(k)\mathbf{P} = \mathbf{Q}_s \) holds, where \( \mathbf{Q}_s \) denotes a point at infinity (i.e., the identity element of the group of points on elliptic curve). But the successful probability of guessing a right secret is not more than \( q^{-n} \) (\( n \) is far less than \( q \)). Thus, it is infeasible to compute \( k_t \) only by the public information \( \{ c_0 \mathbf{P}, c_1 \mathbf{P}, c_2 \mathbf{P}, \ldots, c_{n-1} \mathbf{P} \} \). In addition, it is impossible for the attacker to get \( k_t \) from the server’s public key \( \mathbf{Q}_s \) based on the difficulty of solving ECDL problem.

Furthermore, suppose that the outside attacker wants to compute the session key by the transmitted messages \( \{ ID_p, \mathbf{U}, \mathbf{V}, \mathbf{w}, t \} \) (or \( \{ \mathbf{U}, \mathbf{V}, \mathbf{w}, t \} \)) from the remote user to the server. By Eq. (5) (or Eq. (8)), obviously the attacker must first extracts \( S \) from \( \mathbf{U} \) and \( \mathbf{V} \), and then can compute \( k = H(S, t, 1) \). But, for the attacker, there are three unknowns: \( r, S \) and \( k_t \) (or \( Q_s \)) in two equations of respectively computing \( \mathbf{U} \) and \( \mathbf{V} \). Here, we assume that \( H(\cdot) \) is a secure hash function. Thus, the attacker cannot get any secret information \( S \) only by the transmitted messages \( \{ ID_p, \mathbf{U}, \mathbf{V}, \mathbf{w}, t \} \) (or \( \{ \mathbf{U}, \mathbf{V}, \mathbf{w}, t \} \)), and he cannot obtain the session key without \( S \) obviously.

Therefore, outside attack is infeasible for the proposed scheme.

#### 3.1.2 Replay attack

In the proposed scheme, the server can verify the freshness of the transmitted messages by the freshness of the timestamp \( t \). Furthermore, the timestamp \( t \) is embedded in the hashed message \( w = H(S, t, ID_p) \) (or \( w = H(S, t, 0) \)) by the remote user, such that it can guarantee the integrity of the timestamp. Therefore, the proposed scheme can resist replay attack.

#### 3.1.3 Impersonation Attack

Assume that an attacker wants to impersonate a legal user \( u_t \). In order to pass the verification of the server, the attacker has to construct a valid triple \( \{ \mathbf{U}', \mathbf{V}', S' \} \), such that the equation of \( S' = V' \oplus F_x(k_t \mathbf{Q}_s) \) (or \( S' = V' \oplus F_x(-c_0k_x \mathbf{U}^r) \)) holds, where \( F_x(\mathbf{Q}_s) \) denotes the \( x \) coordinate of the point \( \mathbf{Q}_s \). However, without knowing the secret \( k_t \) (or \( c_0 \)), it is impossible for the attacker to rightly generate the valid triple \( \{ \mathbf{U}', \mathbf{V}', S' \} \).

Furthermore, if the attacker intercepts the session messages \( \{ ID_p, \mathbf{U}, \mathbf{V}, \mathbf{w}, t \} \) (or \( \{ \mathbf{U}, \mathbf{V}, \mathbf{w}, t \} \)) and gets \( S \) rightly from \( w \), he can impersonate a legal user to perform an attack as follows: The attacker first computes \( F_x(rk_t \mathbf{Q}_s) = V \oplus S \) (or \( F_x(rQ_s) = V \oplus S \)), and then he generates and sends new messages \( \{ ID_p, \mathbf{U}, \mathbf{V}_\text{new}, \mathbf{w}_\text{new}, t_\text{new} \} \) (or \( \{ \mathbf{U}, \mathbf{V}_\text{new}, \mathbf{w}_\text{new}, t_\text{new} \} \)) to the server, where \( \mathbf{V}_\text{new} = S_{\text{new}} \oplus (V \oplus S) \), \( \mathbf{w}_\text{new} = H(S_{\text{new}}, t_{\text{new}}, ID_p) \) (or \( \mathbf{w}_\text{new} = H(S_{\text{new}}, t_{\text{new}}, 0) \)), \( S_{\text{new}} \) is random integer, and \( t_{\text{new}} \) is a new timestamp. Obviously, the fake messages \( \{ ID_p, \mathbf{U}, \mathbf{V}_\text{new}, \mathbf{w}_\text{new}, t_\text{new} \} \) (or \( \{ \mathbf{U}, \mathbf{V}_\text{new}, \mathbf{w}_\text{new}, t_\text{new} \} \)) can also pass the verification of the server. However, due to the one-way property of hash function, an outsider cannot extract \( S \) from \( w = H(S, t, ID_p) \) (or \( w = H(S, t, 0) \)).

In addition, obviously any authorized user cannot impersonate the server to obtain the resulting session key of other authorized user, because it requires the server’s master key to compute the session key in Eqs. (6) and (9).

Therefore, the proposed scheme can resist impersonation attack.
3.1.4 Known-key Attack. In our scheme, the session key $k = H(S, t, 1)$ is computed by using a secure hash function. Obviously, the session key only depends on the short-term secret $S$, instead of the long-term secret $k_i$. Furthermore, each session has different short-term secret $S$, and $S$ is randomly generated in $\mathbb{Z}_p^*$. Thus, the current session key is independent of the previous session. That is, an outsider cannot compute the current session key even he knows some previous session keys. Therefore, Known-key attack is infeasible for the proposed scheme.

3.1.5 Perfect Forward Secrecy. Perfect forward secrecy means that if a long-term private key is compromised, this does not compromise any earlier session keys. Here, we suppose that the user $u_i$’s secret $k_i$, is compromised to a attacker, and the attacker further gets the earlier messages $\{ID_{u_i}, U, V, w, t\}$ (or $\{U, V, w, t\}$), which was transmitted from the user $u_i$ to the server before his secret is compromised. For this attack, we will analysis in the following two cases.

Case 1 for identity-based authentication with key transfer: Though the attacker gets the user’s secret $k_i$, the attacker does not know the server’s secret $k_s$. Even given $rp$ (i.e., $U$) and $k_i k_r P$ (where $Q_s = k_s P$ is public and $k_i$ is revealed), it is still computationally hard for the attacker to compute $r k_i k_r P$ based on the difficulty of solving ECCDH Problem. Accordingly, it is impossible for him to rightly compute $S$ and then obtain the session key $k$, since $S = V \oplus F_U(rk_i k_r P)$ and $k = H(S, t, 1)$.

Case 2 for anonymous authentication with key transfer: On the one hand, the attacker does not known the server’s secrets $k_s$ and $cp$, thus he cannot rightly compute $c_0 k_i U$. On the other hand, even given $rP$ (i.e., $U$) and $Q_i$, (suppose that $Q_i = yP, y \in \mathbb{Z}_p^*$), it is still computationally hard for him to compute $rQ_i$, (i.e., $rP$) based on the difficulty of solving ECCDH Problem. Without knowing $c_0 k_i U$ or $rQ_i$, obviously the attacker cannot get the session key $k = H(S, t, 1)$, where $S = V \oplus F_U(rQ_i)$ or $S = V \oplus F_U(-c_0 k_s U)$.

Therefore, the proposed protocol can provide perfect forward secrecy.

3.1.6 User Authentication and Anonymity. We analyze two cases of “Identity-based Authentication with Key Transfer” and “Anonymous Authentication with Key Transfer”, respectively.

In the case of Identity-based Authentication with Key Transfer, the user’s identity is embedded in the hashed message $w = H(S, t, ID_{u_i})$. Thus, any attacker cannot modify the identity $ID_{u_i}$ of the sender in the transmitted messages, because the hashed message can provide its integrity. Furthermore, the server can check the legality of the sender by verifying if he knows the secret $k_i$, which is shared only between the user $u_i$ and the server. Therefore, this protocol can guarantee remote user authentication.

In the case of Anonymous Authentication with Key Transfer, on the one hand, for a legal user $u_i$, we can easy infer that the following equation holds,

\[
rQ_i = r (k_i^s Q_s + k_i^{n-1} (c_{x_{n-2}} Q_{n-2}) \cdots + k_i^1 (c_{x_0} Q_0) + k_i^0 (c_{x_0} Q_0))
\]

\[
= r (k_i^n + k_i^{n-1} (c_{x_{n-2}}) + k_i^{n-2} (c_{x_{n-3}}) \cdots + k_i^1 (c_{x_1}) Q_s)
\]

\[
= r ( (f(k_i) - c_p ) \mod q) Q_s
\]

\[
= -r c_p Q_s (f(k_i) = 0 \mod q)
\]

\[
= r c_p k_s P
\]

\[
= -c_p k_i (rP)
\]

\[
= -c_p k_i U
\]

Thus, the server can rightly compute $S = V \oplus F_U(-c_0 k_s U)$ and then verify the legality of the user. However, for an outside attacker, obviously he cannot forge a fake $Q_i$, such that $rQ_i = -c_0 k_s U$. Thus, the proposed protocol can provide user authentication. On the other hand, for the remote user $u_i$, obviously there exists the equation of $Q_i = -c_0 Q_0$ (Please note that the server does not publish $c_0 Q_0$).
That is, all $q_i$ are equal, which can guarantee the unconditional anonymity of the remote user against outsiders, other authorized users and the server.

### 3.2 Security and Performance Comparisons

We have analyzed the security of the proposed scheme in the above section. Furthermore, we give security comparisons of our proposed scheme and other related works, as shown in Table 1. In addition, we evaluate the performance of our proposed scheme in terms of the computation and communication costs, and list performance comparisons in Table 2. In Table 1, partial anonymity denotes that it is anonymous only for outsiders, but not for the server; while unconditional anonymity denotes that it is anonymous for anyone, including the server. In Table 2, same as References [5, 7] we assume the timestamp length is 16-bit, the size of $p$ used in the ECC of the scheme is 160-bit, the digest message size of hash function (e.g., SHA-1) is 160-bit, and the identity size is 80-bit. In addition, off-line implies that the computation can be precomputed in advance (e.g., Eq. (7)).

### Table 1 Security Comparisons

| Security properties                  | Yang et al.’s scheme [1] | Isam et al.’s scheme [8] | Liu et al.’s scheme [11] | Shi et al.’s scheme [12] | Proposed scheme |
|--------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-----------------|
| Private key confirmation             | Not Provided             | Not Provided             | Provided                 | Not Provided             | Provided        |
| Outside attack                       | yes                      | yes                      | yes                      | yes                      | yes             |
| Replay attack                        | yes                      | yes                      | yes                      | yes                      | yes             |
| Impersonation attack                 | no                       | yes                      | yes                      | yes                      | yes             |
| Known-key attack                     | yes                      | yes                      | yes                      | yes                      | yes             |
| Forward secrecy                      | no                       | yes                      | yes                      | no                       | yes             |
| User authentication                  | yes                      | yes                      | yes                      | yes                      | yes             |
| User anonymity                       | no                       | partial                  | partial                  | unconditional            | unconditional   |

### Table 2. Performance Comparisons

| Schemes                          | Communication costs | Computation costs | Server |
|----------------------------------|---------------------|-------------------|--------|
|                                 | Round | Message size | User (on-line) | User (off-line) | |
| Yang et al.’s scheme [1]         | 2     | 1392 bits   | 4EM+2EA+4H       | -               | 4EM+2EA+4H       |
| Isam et al.’s scheme [8]         | 3     | 1440 bits   | 3EM+2EA+4H       | -               | 4EM+2EA+5H       |
| Liu et al.’s scheme [11]         | 2     | 1296 bits   | 4EM+2EA+1P+2H+1M | -               | 1EM+1EA+2P+2H+1MAC |
| Shi et al.’s scheme [12]         | 2     | (n+2)160 bits | nM+1H               | -               | (n+1)mM+1H       |
| Proposed scheme – (Identity-base)| 1     | 736 bits    | 2EM+2H             | -               | 1EM+2H           |
| Proposed scheme – (Anonymous)    | 1     | 656 bits    | 2EM+2H             | nEM+(n-1)EA     | 1EM+2H           |

Note: EM, EA, P, H, and M denote the time complexity of Elliptic Curve Scalar Point Multiplication, Elliptic Curve Point Addition, Bilinear Pairing, Hash Function, and Scalar Multiplication, respectively.

According to Table 1 and Table 2, clearly the proposed scheme has the following advantages:

1. The proposed scheme can withstand all related security attacks.
2. The proposed scheme can provide the confirmation of the user’s private key.
(3) The proposed scheme needs lower communication costs and computation costs, thus it is more efficient in both communication and computation complexity.

(4) The proposed scheme can provide unconditional anonymity for the remote user in client-server networks.

(5) The proposed scheme can subtly provide two fully different kinds of authentications: identity-based authentication and anonymous authentication.

Furthermore, when the server in our scheme wants to revoke a user, he first adds the identity of the revoked user to the revoked user list and then renews the public information, while the secrets of other authorized users remain unchanged. Similarly, when the server authorizes a new user, he first generates a secret key for the new user, adds the identity of the new user to the authorized user list, and then renews the public information, while the secrets of other authorized users remain unchanged. In actual applications, the server may update the public information in batch way, i.e., after a certain period of time, but not whenever new user registering to the server.

In addition, in the proposed scheme, we focus on the remote user authentication, not mutual authentication between the remote user and the server. If achieving mutual authentication, it only requires the server to return $\text{MAC}_k(w)$ as the response, and then the remote user checks the integrity of $\text{MAC}_k(w)$, where $\text{MAC}_k(w)$ denotes Message Authentication Code (MAC) of the message $w$ by using the session key $k$.

Finally, we consider the extendibility of the proposed scheme. In order to increase the number of the remote users, the proposed scheme can be easily and naturally extended into the multi-level architecture (server – sub-server – user), where the authentication of each level can be implemented in the proposed method.

4. Conclusion
In this paper, we proposed a novel authenticated key transfer scheme to achieve two secure goals: remote user authentication and key establishment between the user and the server. Especially, for the different secure requests in some practical applications (e.g., uploading/downloading files to/from the private forum), the proposed protocol can subtly provide two different kinds of authentications: identity-based authentication and anonymous authentication, while the remote user only holds a single secret, which is written into a smart card for the security considerations. In addition, our scheme only costs 1-round messages transmitted from the remote to the server, few elliptic curve scalar point multiplications and hash functions, thus it is very efficient in the communication and computation complexity.

5. Acknowledgment
This work was supported by National Natural Science Foundation of China (No.61772001), and Talents Youth Fund of Anhui Province Universities (No 2013SQRL006ZD1).

6. References
[1] J.H. Yang, C.C. Chang, “An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” Computers & Security, vol. 28, pp. 138-143, May 2009.
[2] E.J. Yoon, K.Y. Yoo, “Robust ID-based remote mutual authentication with key agreement protocol for mobile devices on ECC,” Proceeding of 2009 international conference on computational science and engineering, IEEE Computer Society Washington, DC, USA, Aug 2009, Vol. 02, pp 633–640.
[3] D.B. He, J.H. Chen, J. Hu, “An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security,” Information Fusion, vol. 13, pp. 223–230, Jul 2012.
[4] E.J. Yoon, S.B. Choi and K.Y. Yoo, “A Secure and Efficiency Id-based Authenticated Key Agreement Scheme based on Elliptic Curve Cryptosystem For Mobile Devices,” International Journal of Innovative Computing, Information and Control, vol. 8, pp. 2637-2653, Apr 2012.
[5] C.H. Chou, K.Y. Tsai, C.F. Lu, “Two ID-based authenticated schemes with key agreement for mobile environments,” Journal of Supercomputing, vol. 66, pp. 973–988, Nov 2013.

[6] D. Wang, C.G. Ma, “Cryptanalysis of a remote user authentication scheme for mobile client-server environment based on ECC,” Information Fusion, vol. 14, pp. 498-503, Oct 2013.

[7] M.S. Farash, M.A. Attari, “A secure and efficient identity-based authenticated key exchange protocol for mobile client-server networks,” Journal of Supercomputing, vol. 69, pp. 395-411, Jul 2014.

[8] S.K. Hafizul Islam, G.P. Biswas, “A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” The Journal of Systems and Software, vol. 84, pp. 1892-1898, Nov 2011.

[9] S. Kumari, M.K. Gupta, M.K. Khan, et al., “An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement,” Security and Communication Networks, vol. 7, pp. 1921-1932, Nov 2014.

[10] S. A. Chaudhry, M. S. Farash, h. Naqvi, et al., “An enhanced privacy preserving remote user authentication scheme with probable security,” Security and Communication Networks, vol.8, pp. 3782-3795, Jun 2015.

[11] J. Liu, Z. Zhang, X. Chen and K.S. Kwak, “Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks,” IEEE Transactions on parallel and distributed systems, vol. 25, pp. 332-342, Feb 2014.

[12] R.H. Shi, H. Zhong and L.S. Huang, “A novel anonymous authentication scheme without cryptography,” Transactions on Emerging Telecommunications Technologies, vol. 25, pp. 875-880, Sep 2014.

[13] G. Yang, Q. Huang, D.S. Wong, and X. Deng, “Universal Authentication Protocols for Anonymous Wireless Communications,” IEEE Transactions on Wireless Communications, vol. 9, pp. 168-174, Jul 2010.

[14] C.C. Chang and H.C. Tsai, “Mobile Authentication withAuthenticated Key Agreement for Large-Scale Wireless Networks,” IEEE Transactions on Wireless Communications, vol. 9, pp. 3346-3353, Oct 2010.

[15] H.J. Jo, J.H. Paik, and D.H. Lee, “Efficient Privacy-Preserving Authentication in Wireless Mobile Networks,” IEEE Transactions on Mobile Computing, vol. 13, pp. 1469-1481, Jul 2014.

[16] Q. Xie, X. Tan, D.S. Wong, et al., “A practical anonymous authentication protocol for wireless roaming,” Security and Communication Networks, vol. 7, pp. 1264-1273, Aug 2014.

[17] J.K. Liu, C.K. Chu, S. S.M. Chow, et al., “Time-Bound Anonymous Authentication for Roaming Networks,” IEEE Transactions on Information Forensics and Security, vol. 10, pp. 178-189, Jan 2015.

[18] M.S. Farash, S.A. Chaudhry, M. Heydari, et al., “A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security,” International Journal of Communication Systems, Jul 2015, DOI:10.1002/dac.3019.

[19] A. C.C. Yao and Y. Zhao, “Privacy-Preserving Authenticated Key-Exchange Over Internet,” IEEE Transactions on Information Forensics and Security, vol. 9, pp. 125-140, Jan 2014 .

[20] S.A. Chaudhry, H. Naqvi, T. Shon, et al., “Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems,” Journal of Medical Systems, vol. 39, pp. 66, Jun 2015.

[21] S.A. Chaudhry, K. Mahmood, H. Naqvi, et al., “An Improved and Secure Biometric Authentication Scheme for Telecare Medicine Information Systems Based on Elliptic Curve Cryptography,” Journal of Medical Systems, vol. 39, pp. 175, Sep 2015.

[22] S.A. Chaudhry, M.S. Farash, H. Naqvi, et al., “A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography,” Electronic Commerce Research, vol.16, pp. 113-139, Mar 2016.