A fresh Two-party Authentication Key Exchange Protocol for Mobile Environment

H.B. Yang, J.H.Chen, Y.Y.Zhang
School of Mathematics and Statistics, Wuhan University, Wuhan, China

ABSTRACT: Mobile environment has been used in large area range of network. In order to communicate securely, a number of schemes also have been proposed. The typical protocol which is two-party authentication key exchange (2PAKE) protocol is based on elliptic curve cryptosystem (ECC) in public networks. In this paper, we propose a two-party authentication key exchange protocol. Our protocol is indeed safer and meets the needs. It achieves efficiency in computational cost. Hence, the proposed protocol has a great contribution to the area of mobile environment.
KEYWORD: Mobile environment; 2PAKE; Elliptic curve cryptosystem; Mutual authentication.

1 INSTRUCTIONS

Key exchange protocol plays an important role in cryptosystem, by which two sides who communicate with each other over an open network can obtain a common session key to keep the communication secret. Both two communication entities make full use of the received messages to compute a secret session key. In 1976, Diffie and Hellman [1] put forward a first key exchange protocol, which cannot make authentication of two communication entities possible. On account of lacking mutual authentication, two parties are subject to the man-in the-middle attack. Since then, some two-party authentication key exchange (2PAKE) protocols are proposed [2-4, 7-10].

Two authentication key exchange protocols furnish mutual authentication of two entities and are suitable for application in public channel. On the basis of new cryptographic techniques, 2PAKE protocols can be divided into three classes. (1) A public-key-based key exchange protocol authenticates each other and builds a common session key by means of public-key technology of cryptography. However, it takes much time to verify the process for certificates in a public-key cryptosystem. (2) A two-party password-based authentication key exchange (2PAKE) protocol allows two sides to have a share in a common password so as to obtain a secret session key. But it is unfit for large area wide range of communication environment to share a secret password for building the common session key. (3) An ID-based key exchange protocol utilizes some user's information (identity, e-mail or social security number) as its public key.

Miller [5] and Koblitz [6] propose the concept of ECC. Yang et al. [11] proposed 2PAKE on basis of ECC [12] to increasing the level of security. In 2009, Yoon et al. [13] pointed out that Yang et al.'s protocol cannot furnish forward secrecy and be subject to impersonation attacks. Compared with Yoon et al.'s scheme, He et al.'s scheme [14] is more fit and efficient in mobile environment. This is because Yoon et al.'s protocol cannot furnish prefect forward secrecy. However, He et al.'s protocol doesn't surmount weakness. A legal party cannot confirm whether or not private key of the user is correct. Based on the above protocols, Chou et al. propose an ID-based authenticated scheme [15]. However, their protocol cannot resist impersonation attacks. In this paper, we proposed new protocol can resist impersonation attack, public key problem, unknown key share attack, mutual authentication, forward secrecy and deniable authentication attack. Meanwhile, we show that our protocol is efficient.

The remainder of this paper is organized as follows. Section 2 describes some preliminaries. We propose our protocol in Section 3. The security analysis of the proposed protocol is presented in Section 4. Comparisons are given in Section 5.

2 PRELIMINARIES

2.1 *Notation*

In this subsection, we first introduce some notations used in this paper as follows:

Fq : A finite field;

G : The cyclic additive group composed of the points on E/ Fq ;

P : A based point with the order n over E ;

E : An elliptic curve defined on finite field Fq with an order n;

$H_1(\bullet), H_2(\bullet)$: Two secure hash functions;

ID_i : The identity of user i ;

d_i / U_i : Private/public key pair of participant i , where $U_i = d_i P$;

d_S / U_S : Private/public key pair of the sever, where $U_S = d_S P$;

SK_i : The private key of entity i ;

2.2 *Discrete logarithms problem*

Definition 1: Discrete logarithms problem (DLP) is described as follow: Let P be a based point in G and generate a point $Q \in G$ at random. It is difficult-to-handle to find k so that $Q = kP$.

2.3 *Background for the elliptic curve group*

An elliptic curve E / Fq is defined by a formula mathematical expression:

$$y^2 = x^3 + ax + b, \quad a, b \in F\ q$$

The coefficients a and b meet:

$$4a^3 + 27b^2 \neq 0$$

A group includes point O (infinity) and the points on E / Fq :

$$G = \{(m,n) : m, n \in Fq, E(m,n) = 0\} \cup \{O\}$$

We know the order of a cyclic additive group G is a big number n . The point $\oplus$ meets the follow conditions:

Let l be a line passing through P and Q (tangent line to E / Fq if $P = Q$), and R be another point of intersection of E / Fq with l . Let l be a line passing through O *and* R . Then, $P \oplus Q$ is the point so that $l^{'}$ intersects E / Fq at O, R and $P \oplus Q$. Scalar multiplication kP is calculated as follows:

$$kP = P \oplus P ... \oplus P. \ (k \text{ times})$$

3 THE PROPOSED AUTHENTICATION SCHEME

We propose a two-party authenticated key exchange (2PAKE) on basis of ECC. Both the user A and the server S build key agreement. Our scheme includes two phases: initialization and authenticated key agreement. The procedure is described at detail as follow.

3.1 *Initialization*

Our scheme includes two phases: initialization and authenticated key agreement. The procedure is described at detail as follow.

On the basis of ECC, the server generates some important parameters E / Fq, P , $H_1(\bullet), H_2(\bullet)$, d_S / U_S and d_U / U_U . Then user keeps the private key d_U secret and the server publishes the parameters $\{E / Fq,\ P,\ H_1(\bullet), H_2(\bullet),\ U_S,\ U_U\}$. We propose a two-party authenticated key exchange (2PAKE) on basis of ECC. Both the user A and the server S build key agreement.

3.2 *Key Agreement*

In order to achieve key agreement, two sides go on communicating and authenticating each other. Note that they use the real identity to perform the authentication procedure. Fig. 1 shows the steps of the authentication procedure as follow:

Step 1: The user $A \rightarrow$ Server: The user A chooses a random number r_A and a value $a \in_R Zq$, then computes $R_A = r_A$ and $w_A = aH_1(d_A, T_A) \bmod q$, where T_A is current timestamp.

Step 2: After that, the user A sends the server an authentication message (i.e., $\{ID_A, w_A, R_A, Auth_A, T_A\}$), where $Auth_A$ is equal to $H_1(ID_A, H_1(T_A, a), R_A)$.

Step 3: The server verifies the user A : Upon receipt of the authentication message (i.e., $\{ID_A, w_A, R_A, Auth_A, T_A\}$), the server compute $a^{'}$ via $a^{'} = w_A \bullet H_1^{-1}(d_A^{'}, T_A) \bmod q$. Then the server checks whether or not $Auth_A$ is equal to $H_1(ID_A, H_1(T_A, a^{'}), R_A)$. If the result is not equal, the server aborts this session.

Step 4: The server chooses a random value r_S at random and computes $R_S = r_S P$ and $SK_S = r_S R_A$.

Step 5: The server $\rightarrow$ the user A : Then the server computes $Auth_A = H_2(ID_A, H_1(T_A, a^{'}), R_S)$ sends

back the authentication reply message ($\{Auth_{SA}, R_S\}$).

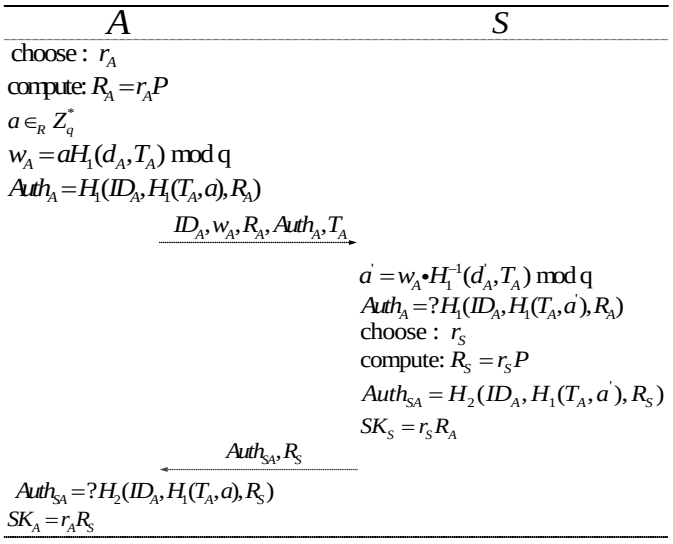

Fig 1. Key agreement phase

Step 6: The user A verifies the server: Upon receiving the message, the user calculates $H_2(ID_A, H_1(T_A, a), R_S)$ and confirms if $Auth_{SA}$ is equal to $H_2\left(ID_A, H_1\left(T_A, a'\right), R_S\right)$. If the value is equal, the user computes the session key $SK_S = r_S R_A$.

4 SECURITY ANALYSIS

In order to ensure that the proposed 2PAKE protocol is secure, we must consider several important security properties, such as impersonation attack, mutual authentication, deniable authentication attack and forward secrecy.

4.1 *Resist the Impersonation Attack*

If an attack C would like to dress up a legal user A to deceive the server S, he or she has to send the valid message $w_A = aH_1(d_A, T_A) \bmod q$ to server S. However, on account of the message a_A as the user A's private key, the attack hasn't the ability to obtain $H_1(d_A, T_A)$. At the same time, the value $a \in_R Zq$ is generated at random. Moreover, both $H_1(d_A, T_A)$ and a are different each time in communication process. It is hard to calculate the message $H_1(d_A, T_A)$ and a from the user A. Thus, the attack cannot succeed to perform Impersonation Attack.

4.2 *Resist the Deniable Authentication Attack.*

In our protocol, the reason why a third party cannot authenticate the messages from the trusted server is that the third party cannot compute the message $Auth_{SA}$. Even if the third party can compute the session key $SK_A = r_A R_S$, he cannot confirm whether or not the server sends the message R_S. Hence, our scheme can resist the Deniable Authentication Attack.

4.3 *Provide Mutual Authentication*

Mutual authentication is that two sides between a user A and a trust server S can authenticate each other within a protocol. In our scheme, the server can authenticate the legal user by means of checking whether or not $Auth_A$ is equal to $H_1(ID_A, H_1(T_A, a), R_A)$. If the legal user can obtain the message from the server, he or she can also authenticate the server by means of checking whether or not $Auth_{SA}$ is equal to $H_2(ID_A, H_1(T_A, a), R_S)$. Therefore, our scheme can make two sides to authenticate each other possible. So our protocol can also resist Unknown Key Share Attack.

4.4 *Resist the Public Key Problem*

We know that the new user keeps the private key secret and publishes the public key Q_{ID_U}. But it is hard to use the user's public key and the server's public key to deduce a secret value for an attack C.

The message $Auth_U$ which no one can succeed to compute except himself cannot be deduced. However, the attack cannot also dress up as any legal user and communicate with server because they cannot obtain the session key.

4.5 *Provide Forward Secrecy*

Forward Secrecy means that the compromise of both the legal user and the trusted server's long-term private keys of the participating parties would not affect the security of the previous session keys [18]. Our scheme satisfies Forward Secrecy via computing $SK_A = r_A R_S$ and $SK_S = r_S R_A$ as the common secret session key. If the legal user's private key is compromised, the attack hasn't the ability to compute r_A or r_S from R_A and R_S. On basis of the DLP, our protocol can provide Forward Secrecy.

5 COMPARISON

Table 1 shows that it takes more less computations cost than the others. Hence, our protocol is suitable for the application environment.

From the Table 2, we know that our protocol has many important secure properties. Compared with previous works, our scheme is provided with some based security requirements: impersonation attack, mutual authentication, deniable authentication attack and forward secrecy.

Table 1 Computational costs comparisons

	U's computational costs	*S*'s computational costs
[11]	$4T_{SM}+2T_{SA}+4T_H$	$4T_{SM}+2T_{SA}+4T_H$
[19]	$3T_{SM}+2T_{SA}+5T_H$	$3T_{SM}+2T_{SA}+6T_H$
[13]	$4T_{SM}+2T_{SA}+4T_H$	$4T_{SM}+2T_{SA}+4T_H$
[15]	$3T_{SM}+3T_H$	$3T_{SM}+5T_H$
Our scheme	$2T_{SM}+T_{NM}+2T_H$	$2T_{SM}+T_{NM}+2T_H$

T_{SM}: the time for computing one scalar multiplication
T_{SA}: the time for computing one scalar addition
T_{NM}: the time for computing one nomal multiplication
T_H: the time for computing one secure hash function

Table 2 Security comparisons

	[11]	[19]	[13]	[15]	Our scheme
Unknown Key Share Rsistance	YES	YES	YES	NO	YES
Replay attack Rsistance	YES	YES	YES	YES	YES
Forward Secrecy	NO	NO	NO	YES	YES
Impersonation attack Resistence	NO	YES	YES	NO	YES
Deniable Authentication Rsistance	YES	YES	YES	NO	YES

6 CONCLUSIONS

In this paper, we presented a fresh two-party authentication key exchange protocol for mobile environment. Their schemes are subject to some attacks. Moreover, we proposed a fresh 2PAKE protocol which overcomes the drawbacks. We demonstrate that our scheme satisfies impersonation attack resistance, forward secrecy, the deniable authentication and mutual authentication.

REFERENCES

[1] Diffie W, Hellman M (1976) New directions in cryptography. *IEEE Trans Inf Theory* IT-22(6): 644-654. doi: 10.1109/TIT.1976.1055638

[2] Bellovin S.M, Merrit M (1992) Encrypted key exchange: password-based protocols secure against dictionary attacks. In: *Proceedings of IEEE Symposium on Research in Security and Privacy*, Oakland, CA, 72-84

[3] Bellare M, Rogaway P (1993) Entity authentication and key distribution. In: *Advances in Cryptology-Crypto*'93, 232-249

[4] Bellar M, Pointcheval D (2000) Authenticated key exchange secure against dictionary attacks. In: *Advances in Cryptology-Eurocrypt*'00, 232-249.

[5] Miller VS (1986) Use of elliptic curves in cryptography. In: *Proc of advances in cryptology-CRYPTO*, vol 85, pp 417-426

[6] Koblitz N (1987) Elliptic curve cryptosystem. *Math Comput* 48: 203-209

[7] Vergados D, & Stergiou G (2007) An authentication scheme for ad-hoc networks using threshold secret sharing. *Wireless Personal Communications*, 43(4), 1767-1780

[8] Tchepnda C, Moustata H, Labiod H, & Bourdon G (2009) On analyzing the potential of a layer-2 muti-hop authentication and credential delivery scheme for vehicular communication. *Wireless Personal Communications*, 51(1), 31-52

[9] Phan R, Wu J, Ouafi K, & Stinson D (2011) Privacy analysis of forward and backward untraceable RFID authentication schemes. *Wireless Personal Communications*, 61(1), 69-81

[10] He D, Chen J, & Hu J (2011) Further improvement of Juang et al.'s password-authenticated key agreement scheme using smart cards. *Kuwait Journal of Science & Engineering*, 38(2A), 55-68

[11] Yang JH, Chang CC (2009) An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. *Comput Secur* 28: 138-143. doi: 10.1016/j.cose.2008.11.008

[12] Hankerson D, Menezes A, Vanstone S (2004) Guide to elliptic curve cryptography. Springer, New York

[13] Yoon E, Yoo KY (2009) Robust ID-based remote mutual authentication with key agreement protocol for mobile devices on ECC. In: *Proc of 2009 international conference on computional science and engineering*, pp 633-640. doi: 10.1109/CSE.2009.363

[14] He D, Chen J, Hu J (2011) An ID-based client authentication with key agreement protocol for client-server environment on ECC with provable security. *Inf Fusion* 13:223-230. doi: 10.1016/j.inffus.2011.01.001

[15] Chou CH, Tsai KY, Lu CF (2013) Two ID-based authenticated schemes with key agreement for mobile environments. *J Supercomput*, 66:973-988. DOI: 10.1007/s11227-013-0962-3

[16] Kaliski B Jr (2001) An unknown key-share attack on the MQV key agreement protocol. *ACM Trans Inf Syst Secur* 4:275-288. doi: 10.1145/501978.501981

[17] Fagen L, Tsuyoshi T (2013) Cryptanalysis and Improvement of Robust Deniable Authentication Protocol. *Wireless Pers Commun*, 69:1391-1398. doi: 10.1007/s11277-012-0640-4

[18] He D, Chen Y, Chen J (2013) An Id-Based Three-Party Authenticated Key exchange Protocol Using Elliptic Curve Cryptography for Mobile-Commerce Environments. *Arab J Sci Eng*, 38:2055-2061. doi: 10.1007/s13369-013-0575-4

[19] Yoon E, Choi S, Yoo K (2012) A secure and efficiency ID-based authenticated key agreement scheme based on elliptic curve cryptosystem for mobile devices. *Int J Innov Comput Inf Control* 8(4):2637-2653