Information Fusion 13 (2012) 223–230

Contents lists available at ScienceDirect

Information Fusion

journal homepage: www.elsevier.com/locate/inffus

An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security

He Debiao *, Chen Jianhua, Hu Jin

Mathematics & Statistics School of Wuhan University, Hubei Province, Wuhan 430072, China

ARTICLE INFO

Article history:
Received 27 July 2010
Received in revised form 21 November 2010
Accepted 17 January 2011
Available online 26 January 2011

Keywords:
ID-based
Mutual authentication
Key agreement
Elliptic curve cryptosystem
Perfect forward secrecy
Modular multiplication

ABSTRACT

Recently, lots of remote user authentication schemes are implemented on elliptic curve cryptosystem (ECC) to reduce the computation loads for mobile devices. However, most of those remote user authentication schemes on ECC suffer from different attacks and can not provide provable security. Therefore, we propose an ID-based remote mutual authentication with key agreement scheme on ECC in this paper. The proposed scheme not only provides mutual authentication but also supports a session key agreement between the user and the server. The scheme also provides the known session key security, the perfect forward secrecy, the no key-compromise impersonation, the no unknown key-share and the no key control. Compared with the related works, the proposed scheme is more efficient and practical for mobile devices. We also give a security proof under the random oracle.

1. Introduction

With the rapid development of electronic technology, various mobile devices (e.g., cell phone, PDA, and notebook PC) are produced and people's life is made more convenient. More and more electronic transactions for mobile devices are implemented on Internet or wireless networks. In electronic transactions, remote client authentication in insecure channel is an important issue. For example, when one client wants to login a remote server and access its services, such as on-line shopping and pay-TV, both the client and the server must authenticate the identity with each other for the fair transaction.

Generally, the remote client authentication can be implemented by the traditional public-key cryptography [1,2]. The computation ability and battery capacity of mobile devices are limited, so traditional public-key cryptograph, in which the computation of modular exponentiation is needed, cannot be used in mobile devices. Fortunately, Elliptic curve cryptosystem (ECC) [3,4], compared with other public-key cryptography, has significant advantages like smaller key sizes, faster computations. Thus, ECC-based authentication protocols are more suitable for mobile devices than other cryptosystem. However, like other public-key cryptography, ECC also needs a public key infrastructure (PKI) to maintain the certificates for users' public keys. When the number of users is increased, PKI needs a large storage space to store users' public keys and certificates. In addition, users need additional computations to verify the other's certificate in these protocols

To solve the above problems, Shamir [5] proposed an identity (ID)-based public-key cryptosystem. As compared with the traditional certificate-based public-key systems, the ID-based public key system may simplify the certificate management. However, the disadvantage of the system lies in the fact that the user's private key must be generated by the Key Generator Center (KGC). Because the security of Shamir's system is based on the integer factorization problem, Shamir's system is not easy to be realized in practice. Fortunately, Boneh and Franklin [6] proposed a practical ID-based encryption protocol from the Weil pairing defined on elliptic curves in 2001.

In 2006, Das et al. [7] proposed a pairing-based remote client authentication protocol with smart cards. However, their protocol suffered from a forgery attack [8]. Later on, two improvements [9,10] on Das et al.'s protocol were proposed. In [9], Fang et al. proposed an improvement to overcome the mentioned forgery attack. Nevertheless, Giri and Srivastava [10] proved that the Fang et al.'s improvement is still insecure against another forgery attack (or called off-line attack). However, the Giri and Srivastava's improvement used a public-key encryption algorithm [11] in the smart card. In this case, the ID-based public key encryption requires a time-consuming bilinear pairing operation. Thus, it will add the computational cost of the smart card. In 2008, Tseng et al. [11] presented a provably secure and efficient pairing-based client authentication protocol for wireless clients with smart cards. In 2009, Goriparthi et al. [12] also proposed another efficient protocol based

* Corresponding author. Tel.: +86 015307184927; fax: +86 02787817667.
E-mail address: hedebiao@163.com (H. Debiao).

1566-2535/$ - see front matter Crown Copyright © 2011 Published by Elsevier B.V. All rights reserved.
doi:10.1016/j.inffus.2011.01.001

on Das et al.'s remote client authentication protocol. However, these protocols [7,9,10,12] do not provide mutual authentication and key exchange between the client and the server. Recently, Wu and Tseng [13] present a new client authentication and key exchange protocol using bilinear pairings for mobile client–server environment. As compared with the above client authentication protocols, their protocol provides both mutual authentication and key exchange. However, the relative computation cost of pairing is approximately 20 times higher than that of the scalar multiplication [14], then the above protocols using bilinear pairings are not efficient in mobile client–server environment.

To solve the above problems, several ID-based authentication protocols on ECC are proposed [15–20]. Yang and Chang's [21] show that some of these protocols do not provide the mutual authentication [15,17,20] or the session key agreement [15,16,18,19] between the client and the server. In 2009, Yang and Chang proposed an ID-based remote mutual authentication with key agreement protocol on ECC [21]. Yoon and Yoo [22] found Yang and Chang's protocol is vulnerable to an impersonation attack and does not provide perfect forward secrecy. Nevertheless, Yoon and Yoo's protocol does not provide perfect forward secrecy and fails to achieve forward secrecy. In the schemes [21,22], a special hash function called *MapToPoint* function which is used to map an identity information into a point on elliptic curve is required. However, the hash function is inefficient although there has been much discussion on the construction of such hash algorithm [23]. Therefore, using general cryptographic hash function instead of the *MapToPoint* function can improve the efficiency of authentication protocol.

In this paper, we propose an efficient ID-based remote mutual authentication with key agreement protocol for mobile client–server environment on ECC without the *MapToPoint* function. Compared with the related works, the proposed protocol is more secure, efficient, and more suitable for mobile devices. We also propose a formal proof to show the security strength of the proposed protocol.

2. Preliminaries

2.1. Notations

We first introduce common notations used in this paper as follows:

- p,n: two large prime numbers;
- F_p: a finite field;
- E: an elliptic curve defined on finite field F_p with prime order n;
- G: the group of elliptic curve points on E;
- P: a point on elliptic curve E with order n;
- $H_1(\cdot)$: a secure one-way hash function, where $H_1 : \{0,1\}^* \to Z_n^*$;
- $H_2(\cdot)$: a secure one-way hash function, where $H_2 : \{0,1\}^* \to Z_p^*$;
- $H_3(\cdot)$: a secure one-way hash function, where $H_3 : \{0,1\}^* \to Z_p^*$;
- $MAC_k(m)$: the secure message authentication code of m under the key k;
- C_i: a client;
- S: the server;
- ID_{C_i} : the identity of the client C_i;
- ID_S: the identity of the server S;
- (x,P_S): the server S's private/public key pair, where $P_S = xP$.

2.2. Background of elliptic curve cryptograph

We will just give a simple introduction of the elliptic curve defined on prime field F_p. Let the symbol E/F_p denote an elliptic curve E over a prime finite field F_p, defined by an equation

$$y^2 = x^3 + ax + b, \quad a,b \in F_p \tag{1}$$

and with the discriminant

$$\Delta = 4a^3 + 27b^2 \neq 0. \tag{2}$$

The points on E/F_p together with an extra point O called the point at infinity form a group

$$G = \{(x,y) : x,y \in F_p, E(x,y) = 0\} \cup \{O\}. \tag{3}$$

Let the order of G be n, G be a cyclic additive group under the point addition "+" defined as follows: Let $P,Q \in G$, l be the line containing P and Q (tangent line to E/F_p if $P = Q$), and R, the third point of intersection of l with E/F_p. Let l' be the line connecting R and O. Then P "+" Q is the point such that l' intersects E/F_p at R and O and P "+" Q. Scalar multiplication over E/F_p can be computed as follows:

$$tP = P + P + \cdots + P(t\ times). \tag{4}$$

To prove the security of our proposed protocol, we present two important mathematical problems on elliptic curves.

Computational Diffie-Hellman Assumption (CDHA): Given $P,xP,yP \in G$, it is hard to compute $xyP \in G$.

Collision Attack Assumption 1 (k-CAA1) [24]: For an integer k, and $x \in Z_n^*, P \in G$, given $\left(P, xP, h_0, (h_1, \frac{1}{h_1+x}P), \ldots, \left(h_k, \frac{1}{h_k+x}P\right)\right)$ where $h_i \in Z_n^*$ and distinct for $0 \leqslant i \leqslant k$, it is hard to compute $\frac{1}{h_0+x}P$.

3. Our protocol

In this section, we propose our ID-based client authentication with key agreement protocol for client–server environment on ECC. The proposed protocol is divided into three phases: system initialization phase, client registration phase, and mutual authentication with key agreement phase.

- System initializing phase

In this phase, S generates parameter of the system.

(1) S chooses an elliptic curve equation E.
(2) S selects a base point P with the order n over E.
(3) S selects its master key x and computes public key $P_s = xP$.
(4) The server chooses three secure one-way hash functions $H_1(\cdot)$, $H_2(\cdot)$, $H_3(\cdot)$ and a message authentication code $MAC_k(m)$. The server keeps x in private and publishes $(F_p,E,n,P,P_s,H_1,H_2,H_3,MAC_k(m))$.

- Client registration phase

When a low-power computing client C_i with the identity ID_{C_i} wants to register to the server S, C_i submits its identity ID_{C_i} to S. After S receiving client's identity, S first uses ID_{C_i} to compute $h_{C_i} = H_1(ID_{C_i})$ and then uses the system private key q_S to compute the client's private key $D_{C_i} = \frac{1}{x+h_{C_i}}P \in G$ and then delivers D_{C_i} to C_i. In order to finish the security analysis, we compute the corresponding public key $P_{C_i} = (h_{C_i} + x)P = h_{C_i}P + P_S$.

To deliver the private key D_{C_i} to the client C_i, two approaches may be used, and both of them require to be performed only once. One is off-line approach that the server S stores the identity ID_{C_i}, the private key D_{C_i} into a smart card and returns it to the client C_i. The other one is on-line approach. When the client C_i connects to the server S through Internet, the server S may use the Secure Socket Layer (SSL) channel in the https mode to deliver the private key D_{C_i} to the client C_i.

- Mutual authentication with key agreement phase

In this phase, the client C_i sends a login request message to the server S whenever C_i wants to access some resources upon S. Then the server S verifies the authenticity of the login message