Identity-based Remote Authentication and Key Agreement Protocol with Anonymity

ZHANG Jianjun
College of Engineering and Design
Hunan Normal University
Changsha, China
jianjun998@163.com

WU Qiwu
Department of Information Engineering
Armed Police Engineering University
Xi'an, China
ustb520@163.com

***Abstract*—Most of the existing identity-based remote authentications with key agreement schemes are not designed for protecting user's privacy. If the users' identity is sent with plaintext in the authentication with key agreement scheme, the attackers can track the users' action trajectory. This paper presents an identity-based remote authentication and key agreement with anonymity. The objective is to protect the user's privacy. The problem is addressed through the user's identity is sent with ciphertext in the authentication with key agreement scheme. Theoretical analysis shows that our proposed scheme achieves good security properties.**

Keywords- anonymity; key agreement; authentication; replay attacks; key control

I. INTRODUCTION

With the rapid development of communications technology, particularly intelligent mobile terminals widespread (such as Smartphone, tablets, etc), mobile terminals are convenient to people's lives. Many works, such as remote office, electronic trading, can be done through mobile terminals. But information technology brings convenience to people at the same time; the security problem is getting people's attention [1]. Such as electronic transactions over an insecure channel, the Remote User authentication is problem that needs to be solved. The mutual authentication of users and servers can guarantee the authenticity and fairness of transactions [2].

Information technology also plans an important role in the war, so solider mobile terminals are bound to be widely used. Soldiers' identity information must be kept secret, because disclosure of the identity information might expose soldiers to the previous track and position [3]. So protect the privacy of the entity is also a problem needed to be addressed. Meanwhile, a major feature of mobile terminals is resource-constrained, and how to reduce security costs is an important issue faced by scholars.

At present, in order to achieve these security goals, scholars have made unremitting efforts. Traditional cryptography can also achieve mutual authentication between entities [4], but these security solutions need model index calculating which are requiring significant computing resources, and not suitable of mobile terminals [2]. Cryptography scheme based on elliptic curve has a huge advantage of computing speed and key length [5]. This cryptography scheme has been widely using in Wireless Sensor Networks [6], mobile communication [7], Mobile Ad Hoc Networks [8], and satellite communication [9]. However, as other public-key cryptography scheme, entities need public key certificates to verify the authenticity of public keys, and additional computing costs are needed.

In 1985, Shamir [10] proposed public-key cryptosystem based on identity, in which the users select the public identity (such as phone numbers, IP addresses, email address, and so on) as a public key. Identity-based cryptography requires a trusted third party, that is, key generation center, and the user's private keys are generated based on the users' identity information. When a user needs to communicate with other users, only the user's identity is needed without certificate management and certificate validation.

Choie and others [11] used bilinear pairings to construct authentication and key agreement protocol, which has good security features and less communication overhead. But bilinear operation with respect to multiplication, the calculation is expensive, difficult to use in mobile terminal. By using bilinear pairings and elliptic curve cryptosystem, Jia and others [12] designed a user authentication scheme, which support serve for user authentication, and does not support user for serve authentication. Tian and others [13] designed an authentication key exchange protocol for sensor network by using elliptic curve cryptosystem. But the scheme requires a key certification center to manage public key certificates. When user need to verify the certificates of other users, more computing resource is required.

Identity-based cryptography scheme is widely used in remote authentication and key agreement protocol. Only for remote users, Yang and others [11] designed a identity-based remote authentication and key agreement protocol with elliptic curve cryptosystem. The protocol has good safety performance and efficiency. However, in the process of authentication and key agreement, the user's identity information is transmitted in plaintext, revealing the user's privacy, especially in military and intelligence application, in which an attacker could track a user's action path. For this issue, an identity-based remote authentication and key agreement protocol with anonymity is proposed, in which user's privacy is protected.

In the remainder of this paper, the following information is presented: In Section Ⅱ, the background is described. Then, in Section Ⅲ, the proposed protocol, identity-based remote authentication and key agreement protocol with anonymity, is presented in detail, followed by the performance analysis in Section Ⅳ. In Section Ⅴ, the paper describes the application environment, and concludes with some suggestions for future work.

II. BACKGROUD

In the 1980 of the 20th century, Miller [15] and Koblitz [16] proposed separately the elliptic curve cryptosystem, which gets a wide range of applications.

Define [15-16]: set p is a primer, and $p>3$. In the finite field Z_p , an elliptic curve equation is defined as follow: E: $y^2=x^3+ax+b \pmod p$, $4a3+27b\neq 0$. A point and an infinite point θ compose a cycling plus group $G=\{(x, y): x, y \in F_p$, $E(x, y) = 0\} \cup \{ \theta \}$. Set $g \in G$, the discrete logarithm problem, which is satisfied by the cycling group generated form g, is unsolved. we choose secretly α, and calculate $\beta=\alpha g$. The public key is $pk = \{p, \beta, g\}$, and the private key is $sk = \{ \alpha \}$. If we want to encrypt the plaintext m, we randomly choose $k \in Z_{p-1}$. The encryption algorithm is defined as: $e_{pk}=(m, k) =(kg, m+k\beta)$, and the decryption algorithm is defined as: $d_{sk}=(kg, m+k\beta) = m+k\beta-\alpha g$.

The elliptic curve encryption scheme has some significant advantages as follow:

1) Under the same security strength, the length of key is short. Especially, in the finite field Fp, the security strength of elliptic curve encryption scheme is equal to the strength with 1024 bits model. So this encryption scheme is very suitable for users with limit memory space.

2) It's easy to construct. We can construct some elliptic curves in a same finite field Fp, so this scheme provides greater security guarantee.

3) Its calculating speed is very fast, because a group algebraic operation on an elliptic curve can be converted into more than 15 times multiplication over a finite field.

Because of these advantages above, elliptic curve cryptography is suitable for wireless secure communications, and widely used in deep space secure communications, satellite secure communications and smart card systems.

III. IDENTITY-BASED REMOTE AUTHENTICATION AND KEY AGREEMENT PROTOCOL WITH ANONYMITY

A. Protocol Description

This section provides details on the identity-based remote authentication and key agreement protocol with anonymity. The protocol has three stages: the initialization of the system, user registration and authentication and key agreement. The protocol is suitable for user-server environment, and shown in Fig. 1.

B. System Initialization

The system initialization is offline. Firstly, the server S selects an elliptic curve equation E, and a base point g over a cycling plus group G with $ord(g) = n$, and $n \approx 2^{160}$ to ensure the security of the system. The server S selects a random number q_s as the private key, and calculates the public key $pk=q_s g$. The server S selects 4 secure one-way functions: $h_1( ): \{0,1\} \rightarrow G$; $h_2( ): \{0,1\} \rightarrow Z^*_p$; $h_3( ): \{0,1\} \rightarrow \{0,1\}^L$; $h_4( ): \{0,1\} \rightarrow Z^*_p$, with $G= (g)$. The server S secretly store the private key q_s, and publish the public key { E, g, pk, $h_1( )$, $h_2( )$, $h_3( )$, $h_4( )$}.

C. User Registration

User registration is offline. If a user wants to join the network, and receive services provided by the network, the user U should send ID_U (such as a network address, telephone number, email address, and so on) to the server. The server S calculates the user U's authentication key = $q_s h_1(ID) \in G$, and sends S_{IDU} to the user U through the secure channel. The user U receives S_{ID_U}, and check if S_{ID_U} is equal to $q_s g$. If S_{IDU} is equal to $q_s g$, the user U secretly store S_{ID_U}.

D. Authentication and Key Agreement

- The phase of authentication and key agreement is offline. The user U randomly selects a point g_U with $g_U=(x_U, y_U) \in G$, and $r_U \in Z^*_p$. The user calculates $\overline{R} = (x_U \cdot g, y_U= r_U pk)$ and $k_1=h_3(r_U \cdot g \| N_u)$, encrypts $C_{US}=ENC(k_1, ID_U \| N_u)$, and calculates $n_U=h_2(N_U)$, $m_U= g_U+ n_U \cdot S_{ID_U}$, and $R= x_U \cdot g$. Here N_U is a random number, and in this paper, $ENC(k, x)$ means that x is encrypted by the symmetric key k. Finally, the user U sends { m_U, $\overline{R}$, N_U, C_{US}, y_U } to the server.
- After the server S receives { m_U, $\overline{R}$, N_U, C_{US}, y_U }, it calculates $k_1= h_3(sk^{-1} y_U \| N_u)$, decrypts C_{US}, gets ID_U, checks N_U, calculates $h_{1ID_U} = h_1(ID_U)$, $n_U= h_2(N_U)$, and $\overline{R}' = m_U- q_S \cdot n_U \cdot h_{1ID_U} = (x'_U, y'_U)$. If $\overline{R} = x'_U \cdot g$, the server confirms that the user is a valid user. Otherwise, the protocol is terminated.
- The server S randomly selects a point g_S with $g_S=(x_S, y_S) \in G$, and a random number N_S. Then, the server S

calculates $n_S=h_2(N_S)$, $m_S= g_S+ n_S \cdot S_{IDS}$, $\overline{R} = x_S \cdot g$, session key $k= h_4(m_S, m_U, x_S)$, and $m_k= (k+x_S) \cdot g$. Finally, the server sends { m_S, m_k, N_S } to the user U.

- After the user U receives { m_S, m_k, N_S }, it calculates $h_{1IDU} = h_1(ID_U)$, $n_S= h_2(N_S)$, $\overline{R}' = m_U - \cdot n_U \cdot S_{IDU} = (x'_S, y'_S)$, $k'= h_4(m_S, m_U, x'_S)$, and $M'_k= (k'+x'_S) \cdot g$. If $M'_k = m_k$, the user confirms that the server is real. Otherwise, the protocol is terminated.

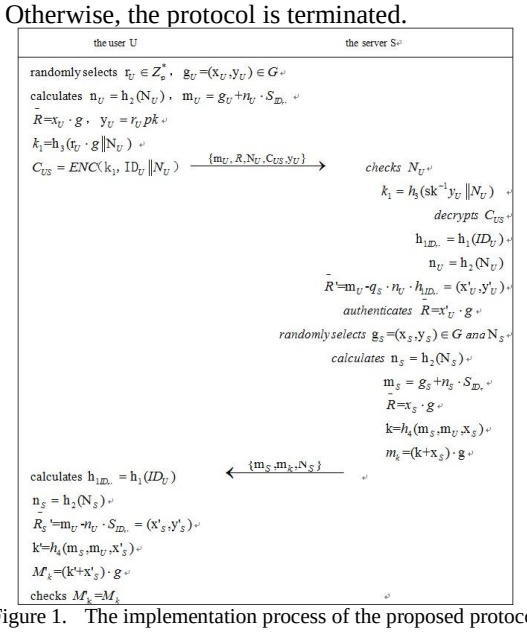

Figure 1. The implementation process of the proposed protocol

IV. DISCUSSION

The security of the proposed protocol depends on the difficulty of elliptic curve discrete logarithm. For remote users, whose terminal is usually on battery power, limited resources, how to save the computing resource is a problem to be solved in the process of authentication and key negotiation. In the identity-based authentication and key agreement protocol, the server and the user does on need to verity each other's certificates, eliminating the cumbersome management of certificates and certificates validation cost. Meanwhile, less computing cost is achieved compared to the authentication scheme based on bilinear pairings, because only point multiplication of elliptic curves is needed. As described in section Ⅲ, mutual authentication and key agreement are implemented between the user and the server.

A. *Anonymity*

In the proposed protocol, the identity information ID_U of user ***U*** is transmitted in ciphertext ENC(k_1, $ID_U \| N_U$), so an attacker cannot get any user identity information, and the user's privacy is protected, which is particularly important for military scenario.

B. *Against replay attacks*

In the process of user and server interaction, the random number N_U or N_S is used in the information { m_U, $\overline{R}$, N_U, C_{US}, y_U} and it's transmission, and the server and the user check the refresh of the random number each time to effectively against replay attacks.

Performance comparison is shown in TABLE Ⅰ. The bilinear operation and certificate operation require more computing resources, so the protocol designed by us is better than [12] and [13] in computing cost. Compared to [14], the anonymity of identity and user privacy protecting are achieved by using only one additional symmetric encryption or decryption. So the protocol designed by us is suitable for mobile environment, in which user privacy protecting is needed.

TABLE I. PERFORMANCE COMPARISON WITH OTHER PROTOCOLS

Performance	**Protocols**			
	protocol in [12]	***protocol in [13]***	***protocol in [14]***	***the proposed protocol***
mutual authentication	No	Yes	Yes	Yes
key agreement	No	Yes	Yes	Yes
anonymity	No	No	No	Yes
certificate costc	Yes	Yes	No	No
number of communication rounds	2	4	2	2
computing cost	4PM[a]+PA[b]	3PM+PA+SD[c]	3PM+2PA	3PM+2PA+SD

a. PM-Elliptic Curve Point Multiplication;

b. PA-Elliptic Curve Point Increase;

c. SD-Symmetric Encryption or Decryption.

V. CONCLUSION

In this paper, an identity-based remote authentication and key agreement protocol with anonymity is proposed. In the process of authentication and key agreement, the identity information of user is transmitted in chipertext, so the user privacy protecting is achieved. Meanwhile, the session key generating depends on the user parameter and the server parameter, so the key control problem is resolved. Theoretical analysis shows that the protocol designed by us has good security.

ACKNOWLEDGMENT

This paper was supported by National Natural Science Foundation of China (No. 61003250), Research Program of Hunan (No.2012GK3120) , and Scientific Research Fund of Hunan Provincial Education Department (No. 10C0944).

REFERENCES

[1] XU Ming-song, LI Xie-hua, CAO Ji-hong, and GAO Chun-ming, "Security-enhanced wireless authentication and key agreement protocol", Computer Engineering, vol. 37(7), pp.116-118, 2011.

[2] He D., J. Chen, Hu J., "Au 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, 2012.

[3] Su R., Cao Z, "An efficient anonymous authentication mechanism for delay tolerant network", Computers & Electrical Engineering, vol. 36(3), pp.435-441, 2010.

[4] ElGamal T, "A public key cryptosystem and a signature protocol based on discrete logarithms" , IEEE Transactions on Information, vol. 31, pp.469-472, 1985.

[5] Koblitz N., Menezes A., Vanstone S., "The state of elliptic curve cryptography. designs, codes and cryptography" ,vol. 19(2-3), pp.173-193, 2000.

[6] Batina L., Mentens N., Sakiyama K, "Low-cost elliptic curve cryptography for wireless sensor networks", ESAS, LNCS vol. 4357, pp.6-17, 2006.

[7] He D, "An efficient remote user authentication and key agreement protocol for mobile-server environment from pairings", Ad Hoc Networks, vol.10, pp.1009-1016, 2012.

[8] Ammayappan K., Negi A., Sastry V, "An ECC-based two-party authenticated key agreement protocol for mobile ad hoc networks", Journal of Computers, vol. 6(11), pp.2408-2416, 2011.

[9] Hong J., Yoon S., Park D. et al, "A new efficient key agreement for VAST satellite communications based on elliptic curve cryptosystem", Information Technology and Control, vol. 40(3), pp. 2008-2016, 2011.

[10] Miller V, Uses of elliptic curves in cryptography, Advances in Cryptology-Crypto'85, LNCS 218. New York: Springer-Verlag, 1986, pp.417-426.

[11] Choie Y., Jeong E., Lee E, "Efficient identity-based authenticated key agreement protocol from pairings" , Applied Mathematics and Computation, vol.162, pp.179-188, 2005.

[12] Jia Z., Zhang Y., Shao H, A remote user authentication scheme using bilinear pairings and ECC, In: proceedings of the sixth international conference on intelligent system design and applications. 2006, pp. 1091-1094.

[13] [13]Tian X., Wong D., Zhu R. "Analysis and improvement of an authenticated key exchange protocol for sensor networks" , IEEE Communications Letters, vol.9(11), pp.970-972, 2005.

[14] Yang J., Chang C, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem", Computers & Security, vol. 28, pp. 138-143, 2009.

[15] Koblitz N, "Elliptic curve cryptosystems", Mathematics of Computation, vol.48, pp.203-209, 1987.

[16] Miller V, Uses of elliptic curves in cryptography, Advances in Cryptology-Crypto'85, LNCS 218. New York: Springer-Verlag, 1986, pp.417-426.