International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Two-Party Authenticated Key Agreement Protocol in Elliptic Curve Cryptography

Vinod Kumar[1], Adesh Kumari[2]

[1]University of Delhi, Department of Mathematics, Aditi Mahavidyalaya,
Auchandi Road Bawana, New Delhi-110039, India

[2]University of Delhi, Department of Mathematics, Shaheed Rajguru College of Applied Sciences for Women,
Vasundhara Enclave, New Delhi-110096, India

Abstract: ***In this paper, we are taken non singular elliptic curve which is depends on prime finite field. Accomplishment of existing public-key algorithms, comparable to Diffie-Hellman, using elliptic curves. In addition, the paper has been conventional two –party authenticated key agreement protocol in elliptic curve cryptography (ECC).In this protocol, two users communicate to each other and generate secure session key. Furthermore, the paper shows the security analysis of this protocol on a secure communicated channel.***

Keywords: Elliptic Curve Cryptography, Identity based Cryptosystem, Private Key generator Mutual Authentication.

1. Introduction

In current years, a lot of identity-based authentication etiquette have been estimated [2, 4, 7]. Yang and Chang [7] anticipated an identity-based remote user authentication protocol for mobile users based on (ECC).This scheme succeeds to the character of both identity based cryptosystem and elliptic curve. Chen et al. [2] predictable two security defects, namely, insider attack and impersonation attack Yang-Chang's scheme. To remove these security flaws, they proposed a extremely developed code word based authentication method. This scheme is secured to present mutual authentication in ECC- background; Wang et al. [6] demonstrate that Chen et al. scheme is not protected and vulnerable to offline password guessing attack, and key negotiation impersonation attack and also experience from clock synchronization problem. Kang and Zhang [4] proposed dumpy key size identity based authentication method, which wants the computation of bilinear pairing on super singular elliptic curve group via very large element range, wherever the computation cost of the pairing is roughly three times higher than that of elliptic curve (EC) point multiplication. Furthermore, we found that their protocol undertake some security flaws.

In this paper, we proposed "Two-Party Authenticated Key Agreement Protocol in Elliptic Curve Cryptography". In this protocol, two users mutually authenticate each other and establish a session key. The remaining paper is controlled in the following way: 2. Preliminaries, 3.The proposed scheme, 4. Security Analysis, 5. Conclusion.

2. Preliminaries

2.1 ID-Based Cryptosystem

In 1984 Shamir proposed the concept of ID-Based Cryptography (IBC) to remove the authentication, communication, and fortification of public key certificates. IBC user's unique identifier, e.g., rather than a random number, e-mail address, as the user's unlimited key, and the user's corresponding private key is generated based on the user's unhindered key by the system's trusted authority. The system's trusted authority is inimitable and is the characterize of the IBC. It is called Private Key Generator (PKG) conditional on whether or not the final construction generated by a user is known by the authority. In the basic protocol, the session key is kept classified from the authority; consequently the authority is called PKG. In IBC, the user's private key is specific to the user by the use of a confined out-of party channel; it is in fact the user's intrinsic certificate. Yet, intrinsic certificate is known only to the user and the PKG where the certificate strength can be established explicitly, which enables IBC to get purge of the unrestricted key certificate [1].

2.2 Background of Elliptic Curve Cryptography

Let q is the large prime and, E denote an elliptic curve over a prime finite field F_q, defined by an equation $y^2 = x^3 + ax + b$ mod q with $a, b \in F_q$ and $4a^3 + 27b^2$ mod $q \neq 0$. The additive elliptic curve group defined as $G = \{(x, y): x, y \in F_q ; (x, y) \in E\} \cup \{\Theta\}$, where the point Θ is known as point at infinity which act as the identity element in P. The point addition in elliptic curve as: If $P = (x_P, y_P) \in G$ and $Q = (x_Q, y_Q) \in G$, Where $P \neq Q$ then $+Q = (x_i, y_i)$, where $x_i = \mu^2 - x_P - x_Q$ mod q, $y_i = (\mu(x_P - x_Q) - y_P)$ mod q and $\mu = (y_Q - y_P)/(x_Q - x_P)$. The scalar multiplication on the group G is defined like $tP = P + P + P \ldots\ldots + P(t\ times)$. The more details of elliptic curve group are given in [3].

2.3 Computational Problem

Discrete Logarithms Problem (DLP): For given $P, Q \in G$ find $k \in Z_p^*$ such that $P = kQ$, which is hard.

Computational Diffie-Hellman Problem (CDHP): For $a, b \in Z_p^*$ and the g is the generator of G, given(g, ag, bg) , then compute abg is hard to the group G.

3. The Proposed Protocol

3.1 Set Up

Private key generator (PKG) takes a security parameter l, returns security parameter and master key M. for given l PKG takes following steps

- Choose an arbitrary generator $g \in G$.
- Select a master key $M \in Z_q^*$ and public key $PK = Mg$.
- Choose collision free one way hash functions

$$H_1: \{0,1\}^* \to G; H_2: G \times G \to G; H_3: G \times G \to Z_q^*;$$
$$H_4: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \to \{0,1\}^l;$$
$$H_5: \{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^l \to \{0,1\}^l.$$

Publish systems parameters$< F_p, E, G, l, g, PK, H_1, H_2, H_3 >$ and M keep secret.

3.2 Partial-Private Key Extract

Input identity ID_i and system parameters with master key m and output partial private key $P_i = (H_1(ID_i) + M)g$.

3.3. Set-Secret Value

The algorithm takes as inputs an identity ID_i, parameters, secret random value $x_i \in Z_q^*$ and output x_i as the entity security value.

3.4. Set-Private Key

The algorithm takes as inputs an identity ID_i, parameters and secret random value x_i then output entity private key $S_i = x_i P_i$.

3.5. Set-Public Key

The algorithm takes as inputs an identity ID_i, parameters and secret random value x_i and contract the entity public key$PK_i = x_i H_2(P_i \,||S_i)$.

3.6. Mutual Authentication and Session Key Agreement

Assume that users A and B mutual authenticate each other and establish a session keys as:

a) A sends message <HELLO, ID_A> to B.
b) B replies to A with a message "HELLO, ID_B>".
c) On receiving the message A from B. A perform as:
   - Choose a random value $a \in Z_q^*$.
   - Compute $T_A = a[H_1(ID_B) + PK]$.
   - Sends $< T_A, S_A, \tau_1 >$ to B. Where τ_1 is the current date and time of message sending by user A.
d) On receiving message the user B, computes $\tau_2 - \tau_1 \leq \Delta\tau$. Where τ_2 message receiving time of user B and $\Delta\tau$ is the valid time delay in message transmission. If condition is hold then, B takes followings steps as:
   - Choose a random value b $\in Z_q^*$.
   - Compute $T_B = b[H_1(ID_A) + PK]$.
   - Sends $< T_B, S_B, \tau_3 >$ to A. Where τ_3 is the current date and time of message sending by user B.
e) On receiving message the user A, computes $\tau_4 - \tau_3 \leq \Delta\tau$. Where τ_4 message receiving time of user A and $\Delta\tau$ is the valid time delay in message transmission. If condition is hold then, A takes followings steps as:
   - Computes $K_A = H_3(T_B||S_A)PK_A$, session key $SK_A = H_4(ID_A||ID_B||T_A||T_B||S_A||S_B)$ and mutual authentication code $MAC_A = H_5(ID_A||ID_B||K_A||SK_A)$.
   - Sends $< MAC_A, \tau_5 >$ to B. Where τ_5 is the current date and time of message sending by user A.
f) On receiving message the user B, computes $\tau_6 - \tau_5 \leq \Delta\tau$. Where τ_6 message receiving time of user B and $\Delta\tau$ is the valid time delay in message transmission. If condition is hold then, A takes followings steps as:
   - Computes $K_B = H_3(T_A||S_B)PK_B$ and $MAC_B = H_5(ID_B||ID_A||K_B||SK_B)$.
   - Checks $MAC_B =? MAC_A$, if condition hold then, set session key $SK_B = H_4(ID_B||ID_A||T_B||T_A||S_B||S_A)$.

From the explanation of this protocol, A and B agreed session key can be computed as: $SK = SK_A = SK_B$. And, once the session establishes user can store/access his/her data strongly via the public channel.

4. Security Analysis

In this section, the proposed protocol secure against following security attacks:

- **User Privacy:** The proposed method never transmits user private records in plaintext form. The messages $< T_A, S_A, MAC_A >$ and $< T_B, S_B, MAC_B >$ are transmitted in excess of the public channel. Markedly this communication cannot be interpreted straightforwardly to get identity, mail-id, password etc. Hence, the proposed protocols offer user privacy.
- **Replay Attack:** Replay Attack is most ordinary attack in authentication evolution. On the other hand, the common countermeasures are time-stamp and random number mechanism. The proposed method, accept the counter-measure and time-stamp. The communication with message, Mutual authentication phase $A \to B$ and $B \to A$ are with time-stamps. Hence the proposed protocol is sturdy alongside with Replay attack.
- **Mutual Authentication:** Mutual authentication is a major characteristic for a confirmation examine opposing to server spoofing attack. The proposed method provides a mutual authentication for the user A and B by ECC-based private and public key switch over.
- **Man in the Middle Attack:** In the protocol the users authenticate each other without fluent. An adversary can try man in the middle attack by sending the forge message. On the other hand, to authenticate each other users switch over message authentication code (MAC_A) or (MAC_B). To compute (MAC_A) or (MAC_B), knowledge of session keys SK is required. Even though, session key SK is assumed secret and cannot be talented through in public known values.
- **Session Key Agreement:** A session key $SK = SK_A = SK_B$ is recognized between the users. After authentication process, session key is different for different users. Consequently adversary cannot access the session key of fastidious users.
- **Perfect forward Secrecy:** An adversary cannot compute session key because to compute session key $SK = H_4(ID_B||ID_A||T_B||T_A||S_B||S_A) =$

$H_4(ID_A||ID_B||T_A||T_B||S_A||S_B)$.Where to computes T_A, T_B, S_A and S_B with using hash function which assume hash function is secured in ECC.

- **PKG forward Secrecy:** An adversary cannot even compute the user's message authentication code $MAC_A = H_5(ID_A||ID_B||K_A||SK_A)$.or $MAC_B = H_5(ID_B||ID_A||K_B||SK_B)$.To computes K_A, SK_A, K_B and SK_B are equivalent to DLP in ECC and computes MAC_A or MAC_B based on hash function which assume hash function is secured in ECC.

5. Conclusion

In this paper, Two-Party Authenticated Key Agreement Protocol in Elliptic Curve Cryptography. In this protocol, clients authenticate to each other and recognized a secure session key. Also the paper discussed the protection of this protocol which is based on session key agreement, PKG forward secrecy, replay attack, user privacy, man in the middle attack, replay attack and mutual authentication.

Reference

[1] X. Cao, W. Kou and X. Du, "A Pairing-free Identity-based Authenticated Key Agreement Protsocol with Minimal Message Exchanges", Information Sciences, pp. 2895−2903, 180, 2010.
[2] T. H. Chen, H. Yeh and W. K. Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing" 5th FTRA International Conference on Multimedia and Ubiquitous Engineering (MUE), pp. 155-159, 2011.
[3] D. Hankerson, A. J. Menezes and S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer, 2004.
[4] L. Kang and X. Zhang, "Identity-Based Authentication in Cloud Computing Storage Sharing", 2010 International conference on multimedia information network and security, IEEE Computer Society, pp. 851-855, 2010.
[5] Shamir, "Identity-Based Cryptosystems and Signature Schemes", Advances in cryptology, pp. 47-53, 1985.
[6] Wang et al: Comments on an advanced dynamic ID-based authentication scheme for cloud computing. In: Wang, F.L., Lei, J., Gong, Z., Luo, X. (eds.) WISM 2012. LNCS, vol. 7529, pp. 246–253, Springer, Heidelberg 2012.
[7] Yang et al: An ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem. Computers & Security 28(3), pp. 138–143, 2009.

Author Profile

Vinod Kumar received the M.Tech. degree in Computer Science and Data Processing from Indian Institute of Technology Kharagpur, Kharagpur, West Bengal, India in 2013. Also, received M.Phil degrees in Mathematics from Chaudhry Charan Singh University, Meerut,Uttar Pradesh, India in 2011.

Adesh Kumari received the M.Sc degrees in Mathematics in 2009 from Maharshi Dayanand University, Rohtak, Haryana, India.