# A Certificateless Authentication Key Agreement Protocol to mitigate MITM and Key-Compromise Impersonation Attacks

Renu Srivastava
IGNOU Study Centre (2777P)
Motilal Nehru National Institute of Technology
Allahabad, India

A.K. Misra
Computer Science &Engineering Department
Motilal Nehru National Institute of Technology
Allahabad, India

## ABSTRACT
To overcome the key escrow issues of the identity based cryptography, Shi Yijuan and Ll Jianhua [11] proposed a new Certificateless Two-party Authentication Key Agreement (CL-2AKA) protocol. In this paper an improved CL-2AKA Protocol has been proposed. The proposed protocol CAKA (Certificateless Authentication Key Agreement Protocol) is based on the algebraic properties of the pairing. The proposed protocol attempts to mitigate the man-in-the middle and Key-compromise impersonation attacks. is found to be more efficient on computation and has more compact cipher text than the existing schemes.

## Keywords
Information Security, Cryptography.

## 1. INTRODUCTION
Protection of data on Internet from any unauthorised usage is an important issue. The techniques used for security of data during transmission in the networks are mostly based on the cryptography, which is an art of secret writing and a method to protect the information from unauthorized usage. Cryptography is either symmetric, which uses the private key or is asymmetric that uses both i.e. the private key and public key. The method to apply the key on the plain text is known as encryption and the method to apply the key on the encrypted data called cipher text for getting the plain text is known as decryption. During transmission of the data, the opponents try to attack in two ways; the first one is human like cracker or hacker and second one is software like worms, viruses etc.

An authentication mechanism prohibits the use of the system (or some resource of the system) by un-authenticated user by verifying the identity of a user before permitting access to the requested resource in any of the following three ways:

- User logins or One-way authentication
- Two-way authentication of communicating entities
- Three-way authentication of communicating entities

Shamir [10] proposed the identity-based public key cryptography (ID-PKC) in 1994, in which the public key of each party is obtained directly from certain aspects of its identity [2, 4, 10]. In 2003 Riyami [8] proposed a new authentication protocol called Certificateless authentication protocol for reducing the certificate provided by the KDC (Key Distribution Centre) due to strong security in place of traditional PKI (Public Key Infrastructure). But, it is possible that the KDC acts as an intruder or opponent because it has the certificates of the sender/initiator and recipient. A single compromise of KDC will make the modes vulnerable over the subscribers of KDC, because the KDC knows the certificates of all the users and they may use it according to the requirement of hacking or any other compromise. Riyami & Paterson [9] also introduced the notion of Certificateless Public Key Cryptography (CL-PKC), which can overcome the key escrow limitation of ID-PKC without introducing certificates and the management overheads. It combines the advantages of the ID-PKC and the PKI.

In 2006, Benoit Libert and Jean-Jacques Quisquater proposed a new key construction for certificateless public key encryption, which is more efficient than the existing ones [5].

Shi Yijuan, LI Jianhua [11] proposed a new Certificateless Two-party Authentication Key Agreement (CL-2AKA) protocol in 2007. Compared with the existing protocol by the Benoit Libert and Jean-Jacques Quisquater [1], this protocol is more efficient and satisfies security attributes. This protocol has been further improved by Xia et al. [14]. A combination of this protocol with the existing certificateless public key encryption and signature schemes yields a complete certificate less public key cryptosystem. The CL-2AKA protocol requires only one time pairing computation and one exponentiation. Thus, the efficiency of the protocol is very high but a problem exists in this protocol in which key replicating attack (one form of the man-in-the-middle attack) and key compromise impersonation attacks are possible. For this reason this protocol is not fully secure. Further, it has been found that this protocol fails to provide implicit key authentication, when there is a man-in-the-middle attack [12, 16]. The CL-2AKA protocol provides implicit key authentication, known session key security, partial forward secrecy, key compromise impersonation resistance, and unknown key share resistance security attributes but it is found that this protocol is not suitable on the security attribute implicit key authentication and key control and is also vulnerable to the key replicating attack[7, 13]. Lippold et al. [3] presented a strongly secure certificateless key agreement

protocol which required ten times pairing computation, and thus efficiency of the protocol reduced considerably. Since the introduction of CL-PKC, many Certificateless Public Key Encryption (CL-PKE) and signature schemes have been proposed but all these certificateless authenticated key agreement protocols were introduced without security analysis.

An active adversary can intercept and properly modify the messages exchanged between two parties, and force two parties to accept the same session key even when two parties really do not want to agree on. The key replicating attack has been analysed in the BR93 security model. Through a detailed study of key replicating attack on the CL-2AKA protocol, it has been demonstrated that the protocol is insecure if the adversary is allowed to reveal non-partner players, who share the same session key and obtain a fresh session key. Trivially this implies the violation of the key establishment security goal.

In order to solve the aforementioned problems, a new Certificateless two party Key Agreement (CL-KA) protocol was proposed in 2010 [5]. The security attributes are analyzed in the eCK security model. This scheme is secure even if key generation centre learns the ephemeral secrets or reveals secret values / replaces public keys but not both. The one-round CL-KA protocol only requires each entity to compute two pairing. Up to now; it turns out to be the most efficient one of all the previously known CL-KA schemes. This protocol has the following properties:

- The protocol is secure only if BDH (Bilinear Diffie-Hellman) and CDH (Computational Diffie-Hellman) assumptions hold.
- The protocol is not certificateless authentication protocol; but it is an alternative of the certificate authentication protocol because it depends on the trusted third party for partial private key.

## 2. SECURITY ANALYSIS

In the new CL-2AKA, the attack and its effect can be described as follows:

The existing problem of man-in-the-middle attack and Key-compromise impersonation attack are defined in the following table:

**Table 1: Existing problem in this protocol**

| Protocol | Pairing | Exponentiation | Security Model | Main Attacks |
|---|---|---|---|---|
| SL[1] | 1 | 1 | No | MA+KCI |

A key replicating attack is fond out in the CL-2AKA protocol during the illustration of an execution of the protocols in the presence of a malicious adversary ***A*** as below.

Let sender A and receiver B wants to agree to a session key for secure communication. Then,

A → B: $<T_A, P_A>$

Where

$T_A = a(H_1(ID_B)P + P_{pub})$

Public Key of A, $P_A = g^x A$

The adversary ***A*** intercepts and deletes the message from A, compute $cT_A$ and $(P_A)^c$ with a random $c \in_R Z_q^*$

($Z_q^*$ is a group with multiplication modulo n and is called the group of units modulo n or the group of primitive classes modulo n.) and sends $<cT_A (P_A)^c>$ to B impersonating A, i.e..

$A_A$ → B: $<cT_A, (P_A)^c>$

B → A: $<T_B, P_B>$

Where $T_B = b(H_1(ID_A)P+P_{pub})$

Public Key of B, $P_B = g^x B$

The adversary ***A*** intercepts and deletes the message from B, compute $cT_B$ and $(P_B)^c$ with a random c selected as above, and sends $<cT_B, (P_B)^c>$ to A impersonating B.

$A_B$ → A: $<cT_B, (P_B)^c>$

A and B compute the session keys $K_A$ and $K_B$ respectively, with

$S_A = x_A D_A$: Private key of A

$S_B = x_B D_B$: Private key of B

A compute: $K_A = e(cT_B, S_A)\cdot(P_B{}^c)^a = g^{cbx}A * g^{acx}B = g(^{bx}A + ^{ax}B)c$

B compute: $K_B = e(cT_A, S_B)\cdot(P_A{}^c)^b = g^{cax}B * g^{cbx} = g(^{bx}B + ^{ax}A)c$

The key replicating attack is as follows:

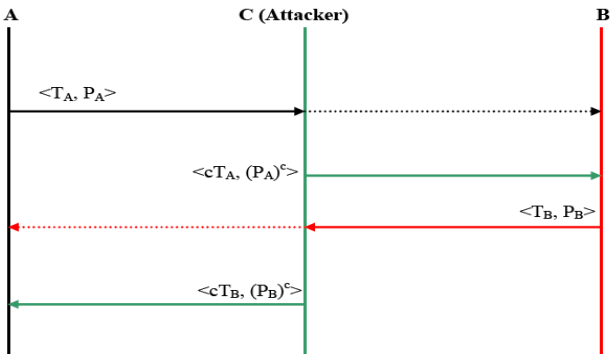


**Figure 1: Replicating Attack (MITM Attack) on New CL-2AKA Protocol**

$K_A = K_B$ i.e. $K_{AB} = K_{AA}$

Attacker → B

B → Attacker : $g(^{bx}A + {}^{ax}B)c$

It is obvious that $K_{AB} = K_{AA}$, this means that A and B compute and accept the same session key $g(^{bx}A + {}^{ax}B)c$ (Actually, A and B should agree on the session key $g^{bx}A + {}^{ax}B$). At last A sends a Reveal query to B, B will return the agreed session key:

$A \rightarrow B$: Reveal

$B \rightarrow A$: $g(^{bx}A + {}^{ax}B)^c$

In the attack sequences shown above, both A and B have accepted the same session key. However, both A and B are non-partners since they do not have matching conversations. In addition, both A and B are uncorrupted since they have not been sent a corrupt query. By sending a Reveal query to either A or B, the malicious adversary ***A*** is able to obtain the session key of a fresh oracle of a non-partner oracle [7]. In order to minimize the short comings of the CK-2AKA protocol, an improved certificate less authentication key agreement protocol named CAKA has been proposed and is described in the section below.

# 3. PROPOSED IMPROVED CL-2AKA PROTOCOL CAKA

In this section an improved certificate less authentication key agreement protocol named CAKA has been proposed. This protocol is based on the principles of CL-2AKA protocol and tries to mitigate the MITM attack and key compromised impersonation attack. This new CAKA protocol is better than the protocol proposed by Liu Wenhao et al. in 2010 because this protocol requires one time pairing computation and exponentiation, which in turn results in very high efficiency of the protocol. This protocol involves three entities, the communicating A (Sender) and B (Receiver) and the Trusted Third Party in which the protocol participants are issued their respective partial private keys. The new CAKA protocol consists of the following:

## 3.1 Bilinear Pairings & Some Assumptions

Let $G_1$ be a cyclic additive group of prime order $q$ and $G_2$ be a cyclic multiplicative group also of prime order $q$. $P$ is a generator of $G_1$. Assume that the discrete logarithm problem (DLP) is hard in both $G_1$ and $G_2$. An admissible pairing $e$ is a bilinear map $e$: $G_1 * G_1 \rightarrow G_2$, which satisfies the following three properties:

- **Bilinear**: for $\forall P,Q \in G$ and , $\forall\ a\ b \in Z_q^*$, we have $e(aP,bQ) = e(P,Q)ab$ ;
- **Non-degenerate**: $e(P,P) \neq 1$.
- **Computable**: If $\forall P$, $Q \in G_1$, one can compute $e(P,Q) \in G_2$ in polynomial time efficiently.

## 3.2 Computational Diffie-Hellman assumption (CDH)

For $g \in G_2$ is the generator of $G_2$, and, $\forall a\ b \in Z_q^*$, given $g^a$ and $g^b$, computing $g^{ab}$ is hard.

## 3.3 Bilinear Inverse Diffie-Hellman assumption (BIDH)

For, $\forall a\ b \in Z_q^*$, $P$ is a generator of $G_1$, given $aP$ and $bP$, computing $e(P,P)^{a-1\ b}$ is hard.

## 3.4 The p-Bilinear Diffie-Hellman Inversion Assumption (p-BDHI):

Given $<P, aP, a^2P, \ldots, a^pP> \in G_1^{p+1}$, computing $e(P, P)^{1/a} \in G_2$ is hard.

## 3.5 Key Agreement

Assume user A and B want to agree to a common session key. To compute this session key, each party computes: A is sending a message to B and B is sending to A by $E_A$ and $E_B$ respectively.

$E_A = (T_A, P_A)$

$E_B = (T_B, P_B)$

$T_A = aP$: Public ephemeral key $aP \in G_1$,

$T_B = bP$: Public ephemeral key $bP \in G_1$ ,

$x_A, x_B$ : Random number chosen by A and B respectively

$P_B = x_BP$ : Public key of B,

$P_A = x_AP$: Public key of A,

$D_B = sQ_B$: Partial Private key of B.

$D_A = sQ_A$: Partial Private key of A

$Y_A = Q_AP_A$

$Y_B = Q_BP_B$

$S_B = x_BD_B$: Private key of B,

$S_A = x_AD_A$: Private key of A

To compute the session key, each user computes.

$K_1 = aT_B = a.bP = b(aP) = b.T_A$,

In this way $K_1 = aT_B = bT_A$

$K_2 = x_AP_B = x_A(x_BP) = x_B(x_AP) = x_B P_A$,

Computation $K_2 = x_AP_B = x_B P_A$,

$K_3 = (S_A, Y_B) = (x_AD_A, Q_BP_B) = (x_AsQ_A, Q_Bx_BP)$

$= (sQ_Bx_B, x_AQ_AP) = (x_BD_B, P_AQ_A) = (S_B, Y_A)$

Computation $K_3 = (S_A, Y_B) = (S_B, Y_A)$

This session key is computed as:

Session Key = H [A, B, $E_{PA,}$ $E_{PB}$, $K_1$, $K_2$, $K_3$ ].

This session key is used for secure communication between both parties.

## 3.6 Architecture

Four way authentications for establishment of session and confirmation to each level for authentication has been proposed in CAKA. The architecture of the protocol is as follows:

The **steps** of Certificateless Authentication Key Agreement protocol are as follows:

- A want to communicate with B. A sends to B the parameter <$T_A$, $P_A$> encrypted with the public key of B, where $P_A$ is public key of A and $T_A$ = aP. (A and B wish to agree on a session key and they each select a private ephemeral key a, b $\in$ $Z_q^*$ and generate the corresponding public ephemeral key aP, bP $\in$ $G_1$ respectively. A then send $T_A$ = aP to B).

(A and B are two parties. Each party has a key pair i. e. a public key and a private key).

- B receives the computational parameter and decrypt with the help of own private key such as $S_B$ and send the parameter <$T_B$, $P_B$> back to A (where $P_B$ is public key of B and $T_B$ = bP $\in$ $G_1$ is public ephemeral key of B) encrypted with the public key of A.

- A send to B, the Message Authentication Key $MAC_k$ ($ID_A$ || $ID_B$ || $T_A$ || $T_B$ || $P_A$ || $P_B$). $MAC_k$ key is known by A and B. This is a shared secret key between A and B.

- Again, B send to A, the Message Authentication Key $MAC_k$ ($ID_B$ || $ID_A$ || $T_B$ || $T_A$ || $P_B$ || $P_A$). This key is used for verified by B to establish a secure session.

Therefore, the session is established between A and B and both is known that the establishment is authenticated. The computation and communication complexity of the certificateless protocols are compared in the table 2, which is based on [5]:

**Table 2: A comparison of Certificateless Authentication protocols**

| Protocol | Pairing | Exponentiation | Security Model | Main Attacks |
|---|---|---|---|---|
| **AP[4]** (2003) | 4 | 1 | No | MA |
| **MT[12]** (2006) | 2 | 1 | No | MA+KCI |
| **WCW[18]** (2006) | 1 | 0 | No | MA+KCI |
| **SL[1]** (2007) | 1 | 1 | No | MA+KCI |
| **Lippold[11]** (2009) | 10 | 5 | eCK | No |
| **Liu[3]** (2010) | 2 | 2 | eCK | No |
| **Our** (2012) | 1 | 1 | No | No |

## 3.7 Advantages of Introducing Hash

The hash function has been used for better security because hash is a one way function.

## 3.8 Security Analysis

Based on [9] the security attributes in the proposed certificateless authentication key agreement protocol are as follows:

### *3.8.1 Implicit Key Authentication*

In the proposed protocol the security attribute implicit key authentication exists because the users are assured that no other users except partners can possibly learn the value of a particular secret key.

### *3.8.2 Known Session Key Security*

Each run of the protocol computes a different session key which depends on the ephemeral private keys a and b.

### *3.8.3 Forward Secrecy*

The adversary has got some messages such as $D_A$ and $D_B$ but he does not compute abP without the knowledge of a and b. Therefore, the proposed protocol can satisfy the security attribute forward secrecy.

### *3.8.4 No Key-compromise Impersonation*

The proposed protocol satisfies key-compromised impersonation (KCI) resilience because if an adversary got $X_{A,}$ $D_A$, b, $D_B$ but not a, $X_B$, it can not compute it.

### *3.8.5 No Unknown Key-share*

The session key SK associated with his elements satisfy both parties has no unknown key-share.

### *3.8.6 Performance Analysis*

This protocol only requires two round communications and each party needs only two pairing operations to perform common session key. This protocol is fully protected to the man-in-the-middle attack (MITM) and Key Compromise Impersonation attack (KCI).

### *3.8.7 One Pairing Computation*

This protocol requires two round communications and each user needs only one pairing computation to perform common session key. Therefore, it is most efficient as compared to Liu Wenhao's new CL-KA protocol in which two pairing operations are required to perform common session key.

### *3.8.8 One Exponentiation*

Public key of a user in the CAKA protocol consists of only one element rather than two elements as in Liu Wenhao's CL-KA protocol.

# 4. CONCLUSION

The proposed CAKA protocol requires each entity to compute one pairing operation and one exponentiation only, which reduces computational burden and provides better security to each party for secure communication. Further, the protocol is secure if BDH and CDH assumptions hold. The verification

of this protocol confirms not only authenticity but it also provides privacy, integrity and confidentiality of data in communication. The protocol is also able to mitigate the MITM and the Key compromised impersonation attacks.

## 5. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of CL-KA, CL-2AKA protocols.

## 6. REFERENCES

[1] B. Libert and J.J. Quisquater, **"On constructing certificateless cryptosystems from identity based encryption",** Public Key Cryptography - PKC 2006, Springer Berlin/Heidelberg, Vol. 3958 of Lecture Notes in Computer Science, 2006, pp. 474-490, doi: 10.1007/11745853_31.

[2] Chen L, Kudla C., **"Identity Based Authenticated Key Agreement from Pairings"**, 2004.

[3] Georg. L., Colin.B, J.M.G..Nieto, **"Stronger Secure Certificateless Key Agreement pairing 2009**", LNCS 5671,pp.206-230,2009, Springer-Verlag Berlin Heidelberg 2009

[4] Joonsang Baek, et. al. **"A Survey of Identity-Based Cryptography"**, 2004.

[5] Liu Wenhao, Xu Chuxiang, Xu Jian., **"Certificateless Two Party Key Agreement Protocol"**, IEEE-2010 International Conference on Multimedia Information Networking and Security, pp 520-525.

[6] Mandt, T.K., **"Certificateless Authenticated Two-Party Key Agreement Protocols"**, Master Thesis, University of Gjovik (2006).

[7] Mengbo Hou and Qiuliang Xu., **"Key Replicating Attack on Certificateless Authenticated Key Agreement Protocol**", IEEE-2009, Asia-Pacific Conference on Information Processing, pp 574-577.

[8] S.S. Al-Riyami and K. Paterson., **"Certificateless Public Key Cryptography"**, In C.S. Laih, editor, Advances in Cryptology - Asiacrypt 2003, volume 2894 of Lecture Notes in Computer Science, pages 452-473. Springer-Verlag, 2003.

[9] S.S. Al-Riyami and K. Paterson., **"CBE from CL-PKE: A Generic Construction and Efficient Schemes"**, In S. Vaudenay, editor, PKC 2005, volume 3386 of Lecture Notes in Computer Science, pages 398-415. Springer-Verlag, Berlin 2005.

[10] Shamir A., **"Identity-Based Cryptosystems and Signature Schemes**", [j]. Lecture Notes in Computer Science,1994, 196: 47-53.

[11] Shi,Y., Li,J., **"Two-Party Authenticated Key Agreement in Cerfiticateless Public Key Cryptography"**, Wuhan University Journal of Natural Sciences, 12(1),071-074 (2007).

[12] Swanson, C, Jao,D., **"A Study of Two-Party Certificateless Authenticated Key Agreement Protocols"**, INDOCRYPT 2009, LNCS 5922,pp.57-71,2009, Springer-Verlag Berlin Heidelberg 2009, 53234.

[13] Swanson, C.M., **"Security in Key Agreement: Two-Party Certificateless Schemes"**, Masters Thesis, University of Waterloo (2009)

[14] Xia,L., Wang,S., Shen,J., Xu,G., **"Breaking and repairing the certificateless key agreement protocol from ASIAN 2006"**, Wuhan University Journal of Natural Science 13(5), 562-566 (2008)

[15] Wang, S., Coa, Z., Wang L., **"Efficient Certificateless Authenticated Key Agreement Protocol form Pairing"**, Wuhan University Journal of Natural Sciences: 11(5), 1278- 1282 (2006).

[16] Zu-hua Shao., **"Efficient authenticated key agreement protocol using self-certified public keys from pairings"**, Wuhan University Journal of Natural Sciences 10(1),267- 270 (2005)