Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

On the Security of a Non-Interactive Authenticated Key Agreement over Mobile Communication Networks

Yau, W. C. [1], Yap, W. S. [2], and Chin, J. J. [*3]

[1]*School of Electrical and Computer Engineering, Xiamen University Malaysia, Malaysia*
[2]*Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Malaysia*
[3]*Faculty of Computing and Informatics, Multimedia University, Malaysia*

E-mail: jjchin@mmu.edu.my
[*]*Corresponding author*

Received: 16 Jun 2021
Accepted: 7 October 2021

Abstract

Setting up a common secret key for communications between two parties over insecure mobile communication networks is important for many network applications. Previously, Wu and Lin proposed a non-interactive authenticated key agreement over mobile communication networks with security proofs assuming the Bilinear Diffie-Hellman problem is hard. Wu and Lin scheme is unique as the users do not need to interact at all in sharing a secret key. Besides, their scheme will at least achieve trust level of 2, where the system authority will not know the user secret keys since self-certified cryptography is used. In this paper, we demonstrate that any malicious outsider can break the security of Wu and Lin's scheme by impersonating any one of the party using public key replacement attack. Besides, we show that the system authority can easily recover all the user secret keys which contradicts with the concept of self-certified cryptography. Lastly, if the secret key shared between two parties or one of the party's private key had been compromised, the same two users can no longer communicate in the future since the same secret key will be derived and shared forever. This violates the property of forward secrecy, a property that must be provided for a key agreement scheme.

Keywords: key agreement; security analysis; attacks; communication networks and applications.

1 Introduction

Due to the advancement of Internet, the communications between multiple parties to share confidential data become more frequent. An authenticated key agreement (AKA) protocol [4] enables two parties to authenticate each other as well as securely compute a shared secret key to be used for subsequent operations. Very naturally, the resultant shared secret key can be used for any symmetric key primitives given that symmetric key primitives enjoy higher speed and communication efficiency. To name a few, Digital Video Broadcasting Common Scrambling Algorithm [17] is specified by the European Telecommunication Standards Institute (ETSI), A5/1 stream cipher [3] is used to ensure over-the-air voice privacy in the Global System for Mobile communications (GSM) cellular telephone standard and Cipher-based Message Authentication Code (CMAC) [7] is used on the authentication mechanism of the IPsec Encapsulating Security Payload (ESP) and the Authentication Header (AH) protocols. Another notable example is Hash-based Message Authentication Code (HMAC) [2] that is widely used within the Secure Shell Protocol (SSH) and Transport Layer Security (TLS) to provide the data integrity and ensure the authenticity of a message. Thus, this shows the importance of key generation in providing security services to mobile communication networks and applications.

In 1991, Girault introduced the notion of self-certified cryptography [8] to solve the drawback of conventional public key cryptography and identity-based cryptography [16]. For conventional public key cryptography, the users need to verify the other users' certificates before communicating with them. The public key verification is needed to ensure the public key is genuine avoiding the public key substitution attack [12]. To avoid the usage of the certificate for the conventional public key cryptography, identity-based cryptography aims to achieve implicit certification by generating the user secret key based on the system authority's master private key. However, the system authority must be *fully* trusted since he knows all the user secret keys. The first practical identity-based encryption was realized by Boneh and Franklin [5]. The proposed scheme achieved chosen ciphertext security in the random oracle based on bilinear maps assuming a variant of the computational Diffie-Hellman problem. On the other hand, self-certified cryptography utilizes the advantages of both conventional public key cryptography and identity-based cryptography where it can achieve both implicit certification and that the system authority does not know the users' secret keys. Of course, the main assumption is that the system authority will not generate a fake public key for any users. Thus, the system authority in self-certified cryptography is assumed to be honest but *curious*.

In [19], Wu and Lin proposed a non-interactive authenticated key agreement scheme based on the intractability of the bilinear Diffie-Hellman problem (BDHP). In other word, their proposed scheme is polynomial-time secure assuming that the BDHP is polynomial-time intractable for any probabilistic polynomial-time Turing machine (PPTM) adversary. They also claimed their work in the self-certified model, where no certificate is needed in verifying the user public key and yet the system authority does not know the users' secret keys. The proposed scheme is unique and powerful since the two parties do not need to interact with each other to derive the shared secret key. The more interactions between the two parties, the greater possibilities the information of shared secret key may leak. Wu and Lin emphasized that the public key of the other party does not need to be authenticated in advance since the public key verification is simultaneously combined into the process of generating the shared secret key. The proposed scheme was claimed suitable for the mobile devices with limited computing power and small storage space. Other than providing the security analysis of their scheme, they also showed that their proposed scheme outperformed other cryptographic schemes. For example it is more efficient than the one utilizing a certificateless public key encryption scheme by [10], a specific certificateless key agreement protocol in [11], or the certificateless key agreement with multiple PKGs from [14], and finally an authenticated

certificateless key agreement scheme in [13]. These comparisons were given by the original author to prove the superiority of their scheme in terms of operational costs.

Our contributions. In this paper, we present three main security issues faced by the Wu and Lin proposed non-interactive authenticated key agreement scheme [19]. In an outline, these are:

i) Public key replacement attack: the public key is not authenticated during the key agreement phase and can be easily replaced;

ii) Trust level of the system authority: the system authority can recover all the user secret keys without being detected by users;

iii) Violation of the property of forward secrecy: the shared secret key's derivation is deterministic and remains the same for the same two parties, thus compromise of a long-term private key of a user will affect the secrecy of previous established session keys between these two parties.

We deem our work as important to point out the vulnerabilities of Wu and Lin's construction as their scheme was even recognized and cited by several subsequent works including a high profile conference in 2015 [18, 20]. The security analysis insight provided in this paper can be treated as the future concern in proposing a new authenticated key agreement protocol.

Organization. In Section 2, we prepare the background of bilinear pairing and different attackers in the self-certified model. We then review Wu and Lin's non-interactive authenticated key agreement scheme in Section 3. Subsequently, we show the security flaws in Wu and Lin's scheme in Section 4. Finally, we give some concluding remarks in Section 5.

2 Preliminaries

In this section, we present the notations used throughout the paper and give the description of bilinear pairing and the bilinear Diffie-Hellman problem. Lastly, we also present different attackers in the self-certified model.

2.1 Notations

The following notations are used throughout the paper:

- If G is a set, we denote $z \xleftarrow{\$} G$ as randomly sampling an element from set G.
- We denote (X, Y) as a string composed of two components X and Y that can be individually parsed.
- We use the equals sign to denote assignment, similar to programming languages, where $a = b + c$ would be entail computing the right hand side expression and assigning its result to the left.

- If a string is composed of more than two components, we encapsulate that set of items within $\langle, \rangle$ symbols, e.g. $\langle A, B, C\rangle$ would be a set of items A, B and C.

2.2 Bilinear Pairing

We review the background of bilinear pairing by referring to [19, 5]. Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, \times)$ denote two groups with the same prime order q for some large prime q. Our system makes use of a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ which satisfies the following properties:

i) Bilinearity: We say that a map e is bilinear if $e(aP, bQ) = e(bP, aQ) = e(P, Q)^{ab}$ for any $P, Q \in \mathbb{G}_1$ and any $a, b \in \mathbb{Z}_q^*$.

ii) Non-degeneracy: Since $\mathbb{G}_1, \mathbb{G}_2$ are groups of prime order, thus this implies that $e(P, P)$ is a generator of $\mathbb{G}_2$ if P is a generator of $\mathbb{G}_1$.

iii) Computability: There exists an efficient algorithm to calculate $e(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

2.3 Bilinear Diffie-Hellman Problem

Similarly, we present the bilinear Diffie-Hellman problem by referring to [5]. Notice that the bilinear Diffie-Hellman problem is a variant of the computational Diffie-Hellman problem.

Let $\mathbb{G}_1, \mathbb{G}_2$ be two group of prime order q. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear map and P be a generator of $\mathbb{G}_1$. The bilinear Diffie-Hellman problem in $\langle \mathbb{G}_1, \mathbb{G}_2, e\rangle$ is defined as follows: Given $\langle P, aP, bP, cP\rangle$ for some $a, b, c \in \mathbb{Z}_q^*$, find $W = e(P, P)^{abc} \in \mathbb{G}_2$.

2.4 Adversary's Goals

Different attackers have been considered in the self-certified model, such as the following [8]:

- Malicious Outsider: the outsider may replace any user public keys since no certificates exist in guaranteeing the authenticity of user public key.
- Dishonest Insider: the insider can obtain the user private keys for a number of identifiers; the insider aims to deduce the information of the system authority's master private key by studying the relationship of the user private keys for different users.
- Curious System Authority: the system authority may recover the user private key composed from the user secret key and the system authority's master private key without being detected by the user

The ultimate goal for an attacker (either a malicious outsider or a dishonest insider) is to recover the system authority's master private key. Else, the attacker may hope that he can recover some of the users' private keys. Meanwhile, the curious system authority may hope that he can learn the

user private keys without being detected and subsequently know the shared secret key between any two parties.

In the context of a key agreement scheme, the property of forward secrecy [6, 9] must be fulfilled. Compromise of a long-term private key of any party should not help the attacker in generating the past session keys between two involved parties. This serves to protect the confidentiality of past conversations between two parties. In Park et al. [15] also showed the importance and applications of forward secrecy in mobile communication networks.

3 The Wu-Lin Non-Interactive Authenticated Key Agreement Scheme

In this section, we describe the non-interactive authenticated key agreement protocol by Wu and Lin in [19] with some slight changes in notations to conform to other pairing-based cryptographic schemes. The proposed protocol consists of three following stages: **System Initialization Stage**, **User Registration Stage** and **Authenticated Key Agreement Stage**.

i) **System Initialization Stage.** The system authority (SA) generates groups $(\mathbb{G}_1, +), (\mathbb{G}_2, \times)$ of order q with a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ and selects a generator $G \xleftarrow{\$} \mathbb{G}_1$. Subsequently, the system authority chooses $c \xleftarrow{\$} \mathbb{Z}_q^*$, computes $C = cG$ and a collision resistant hash function $H : \{0,1\}^* \to \mathbb{G}_1$. The public parameters are $\langle \mathbb{G}_1, \mathbb{G}_2, q, e, H, G, C \rangle$ while the master private key is c.

ii) **User Registration Stage.** For each user U_i with identifier ID_i the user performs the following steps to acquire a key pair:

   (a) **Step 1.** U_i chooses $u_i \xleftarrow{\$} \mathbb{Z}_q^*$, computes $R_i = u_i H(ID_i)$ and sends $\langle ID_i, u_i, R_i \rangle$ to the system authority.

   (b) **Step 2.** The sytem authority checks if $R_i = u_i H(ID_i)$ and if correct selects $v_i \xleftarrow{\$} \mathbb{Z}_q^*$ to compute $Y_i = v_i R_i$ and $X_i = cY_i$. It returns (X_i, Y_i) to U_i.

   (c) **Step 3.** U_i checks the correctness as $e(C, Y_i) = e(G, X_i)$ and accepts (Y_i, X_i) as user private/public key pair if the equation holds.

iii) **Authenticated Key Agreement Stage.** When two parties, U_1 and U_2 wishes to generate a shared secret key between them, they do the following:

   (a) **Step 1.** U_1 computes the shared key as $S = e(X_1, Y_2)$.

   (b) **Step 2.** U_2 computes the shared key as $S' = e(Y_1, X_2)$.

The proposed protocol fulfills the property of correctness since $S = S'$:

$$\begin{aligned} S &= e(X_1, Y_2) \\ &= e(cY_1, Y_2) \\ &= e(Y_1, cY_2) \\ &= e(Y_1, X_2) \\ &= S'. \end{aligned}$$

For ease of understanding, Figure 1 illustrates the Wu and Lin non-interactive authenticated key agreement protocol diagrammatically. Security proofs of the proposed protocol is omitted in this paper and interested reader can refer to [19] for more details.

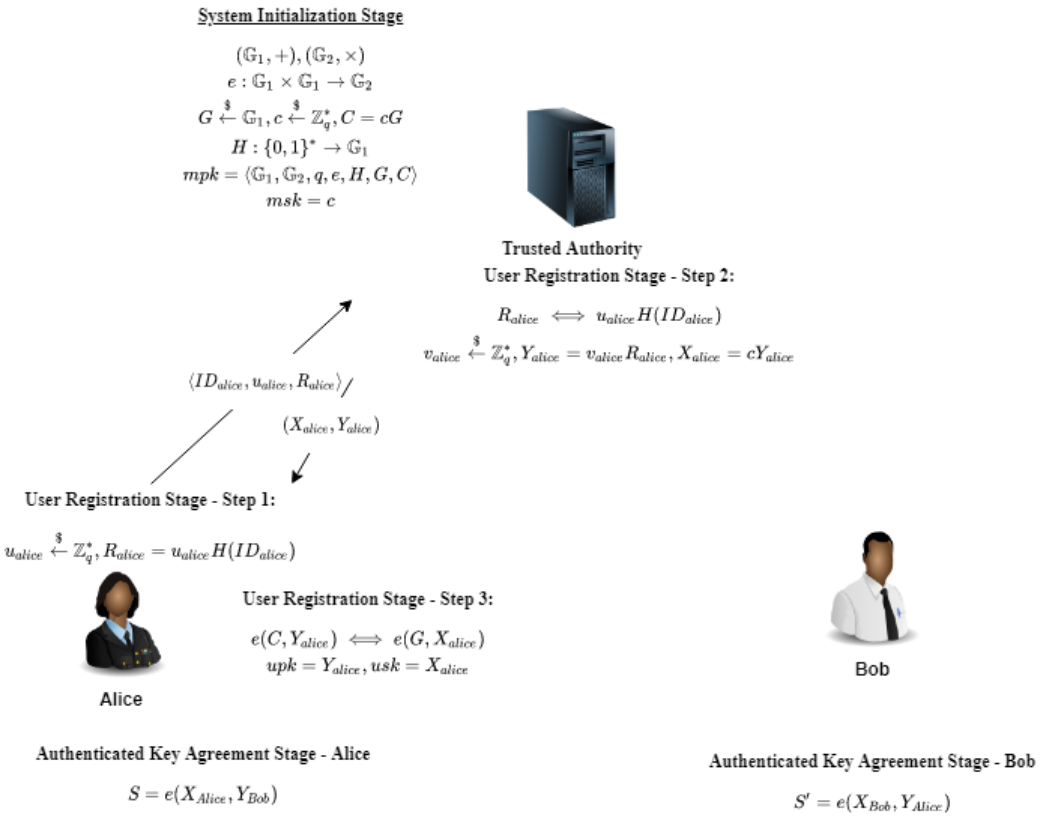

Figure 1: Wu-Lin's non-interactive authenticated key agreement scheme ([19]). The user registration stage for Bob is similar to Alice's and is not depicted.

4 Security Issues with the Wu and Lin's Non-Interactive Authenticated Key Agreement Protocol

In this section, we present our findings, i.e., three security issues with the Wu-Lin non-interactive authenticated key agreement protocol in order of seriousness.

4.1 First Issue: Public Key Replacement Attacks

Self-certified cryptography lies between the conventional public key cryptography and identity-based cryptography. One of the major advantages that is inherited from self-certified cryptography is no certificates are needed to guarantee authenticity of user public keys. This ability had been captured in the security model of self-certified cryptography where the attacker is allowed to replace any user public key with his chosen user public key. Even if the attacker can replace

the user public key, the other part of public key (i.e., the user identifier ID) prevents the attacker from decrypting a ciphertext or forging a signature.

The first attack discovered is that any malicious outsider can easily impersonate any user by launching public key replacement attack since there exists no certificate that binding the public key of a specific user to his identifier ID. The public key replacement attack can be illustrated as follows:

i) A malicious outsider $U_{\mathcal{A}}$ with identifier $ID_{\mathcal{A}}$ chooses $a \xleftarrow{\$} \mathbb{Z}_q^*$ and computes $Y_{\mathcal{A}} = aG$ and $X_{\mathcal{A}} = aC$. $(Y_{\mathcal{A}}, X_{\mathcal{A}})$ serves as $U_{\mathcal{A}}$'s public-private key pair.

ii) Assume that $U_{\mathcal{A}}$ wishes to impersonate user U_1 to share a common secret key with U_2, $U_{\mathcal{A}}$ needs to exchange Y_1 with $Y_{\mathcal{A}}$. This can be done by sending/e-mailing $Y_{\mathcal{A}}$ to U_2 or replacing Y_1 with $Y_{\mathcal{A}}$ stored on the public key directory. In most of the cases, the public key of a sender will be transmitting to the receiver directly by attaching it to emails.

iii) Finally, $U_{\mathcal{A}}$ and U_2 can compute the shared secret key as $S = e(X_{\mathcal{A}}, Y_2)$ and $S = e(X_2, Y_{\mathcal{A}})$ respectively. The correctness can be verified as follows.

$$\begin{aligned} e(X_2, Y_{\mathcal{A}}) &= e(cY_2, aG) \\ &= e(Y_2, acG) \\ &= e(Y_2, aC) \\ &= e(Y_2, X_{\mathcal{A}}) \\ &= e(X_{\mathcal{A}}, Y_2). \end{aligned}$$

This attack works as U_2 cannot distinguish whether the public key belongs to U_1 or $U_{\mathcal{A}}$ since there is no certificate binding Y_1 to U_1. U_2 will be convinced that he is interacting with U_1, instead of $U_{\mathcal{A}}$.

We illustrate the attack diagrammatically in Figure 2.

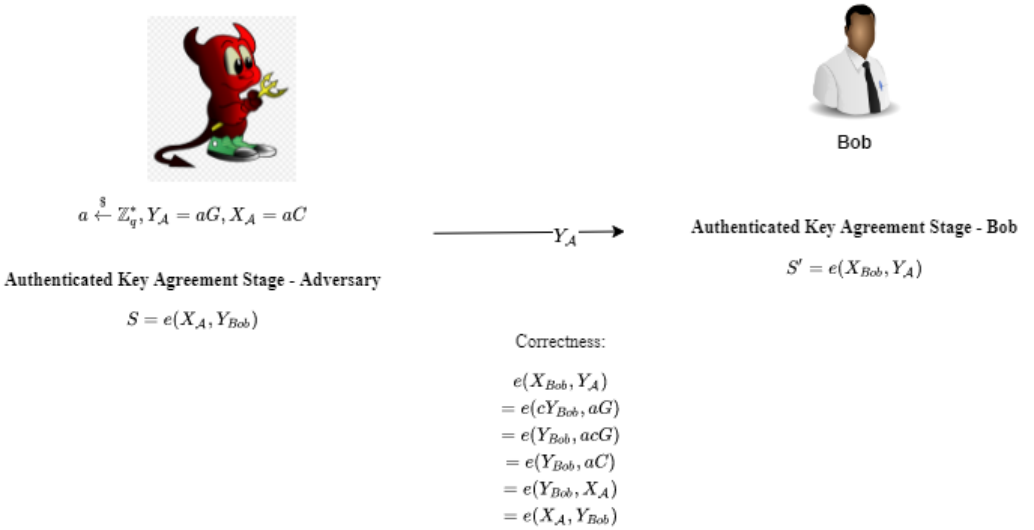

Figure 2: Public key replacement attack on Wu-Lin's protocol.

At the same time, this attack also means the security proofs provided by Wu and Lin (refers to Theorem 3 in [19]) are invalid. The security model given by Wu and Lin is incomplete where public key replacement oracle is not given to the attacker and thus the public key replacement attack cannot be captured in the security proofs. More importantly, Wu and Lin showed that the attacker can break the Bilinear Diffie-Hellman problem if the forgery of shared secret key can be constructed. However, Wu and Lin did not show that the forgery can be constructed using the simulation game in security proofs. Wu and Lin only *assumed* that such forgery can be constructed. Thus, the security proofs provided by Wu and Lin contain flaws.

4.2 Second Issue: Trust Level of System Authority

Wu and Lin claimed their scheme to be self-certified. In the self-certified model proposed by Girault in [8], Girault introduces the concept of trust level of the system authority inspired from the differences between conventional public key cryptography, identity-based cryptography and self-certified cryptography. The trust level of the system authority can be divided into three levels of increasing security order as follows.

- **Level 1.** The system authority generates all user secret keys and can utilize them freely impersonate any user at any time without being detected.
- **Level 2.** The system authority merely certifies a user's secret keys, which are generated by users themselves, but can still impersonate a user by generating false guarantees such as issuing a certificate for a false set of keys that claim to be the user's.
- **Level 3.** The system authority can be detected if attempting impersonation, such as if it attempts to replace a user's secret key in a participation of a protocol with other users. Each user's secret key can be publicly verified to originate from the user.

Obviously, the trust levels of system authority in identity-based cryptography, certain certificateless cryptography schemes and traditional public key infrastructure are of 1, 2 and 3 respectively.

For identity-based cryptography, the user's secret key is generated by the system authority. Therefore the system authority has full access to a user's secret and can impersonate the user at will by only using its identity-string.

For certificateless cryptography, proposed by Al-Riyami and Paterson [1], the trust levels would be 3 if certain binding techniques were used to bind a user's public keys to their identities. Otherwise, it only reaches trust level 2 if public key replacement attacks are successful by the system authority. This allows the system authority to circumvent a user's private keys with their own generated fake public/private key pairs if the binding is not done properly.

Finally, traditional public key infrastructure (PKI) ecosystems and self-certified cryptography achieve trust level 3. In PKI ecosystems, an issued certificate binds a public key to a user, while the secret that is generated by the user remains unknown to the system authority. For self-certified cryptography, this is done implicitly, and similarly the system authority has no knowledge of the user's secret. Changing the certificate would open the system authority up to detection of fraudulent actions.

Figure 3 illustrates the trust levels as depicted in this paragraph.

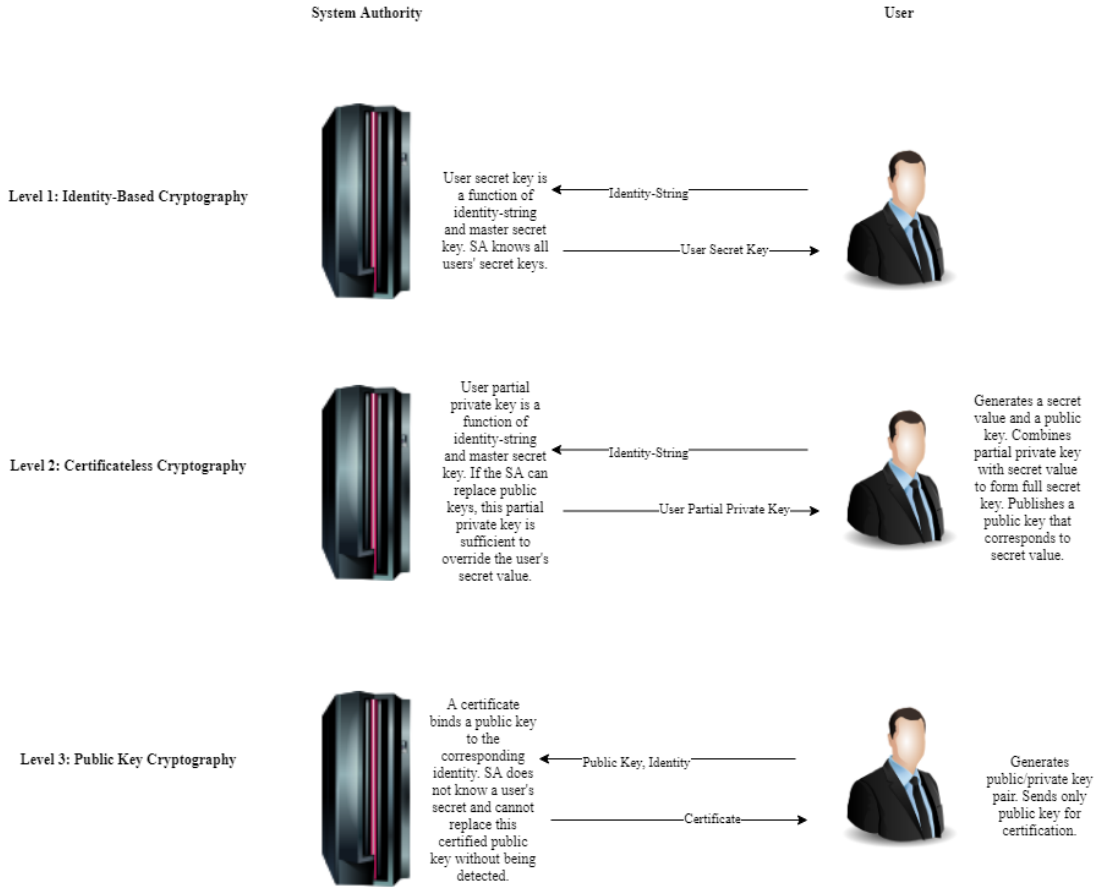

Figure 3: Trust levels for identity-based cryptography, certificateless cryptography (without public key binding) and traditional public key infrastructure as described by Girault [8].

However, it is evident that the Wu-Lin non-interactive authenticated key agreement protocol achieves only trust level of **Level 1**. This is because when a user registers himself in the **User Registration Stage**, the user sends his user secret key u_i as part of the communication to the system authority. The system authority knows the master private key c. Therefore with these 2 pieces of information the system authority can generally impersonate any user who registers themselves with the system authority without being detected.

Even one may modify Wu and Lin scheme by not sending the user secret key u_i to the system authority during the registration state, but this step does not prevent the key escrow problem. In fact, the generation of public-private key pair (i.e., (Y_i, X_i)) is incorrect since the system authority can generate the user public-private key pair as $(Y_{\mathcal{A}} = aG, X_{\mathcal{A}} = aC)$ without relying the user secret key u_i. Moreover, the user can check the correctness as $e(C, Y_i) = e(G, X_i)$ and still be convinced that the public-private key pair is generated using his user secret key and identifier ID_i.

This basically allows a System Authority to impersonate any user of its choice and share its key with whoever it chooses without being detected. Figure 4 depicts a malicious system authority impersonating Alice, Carol and Eve to a user Bob.

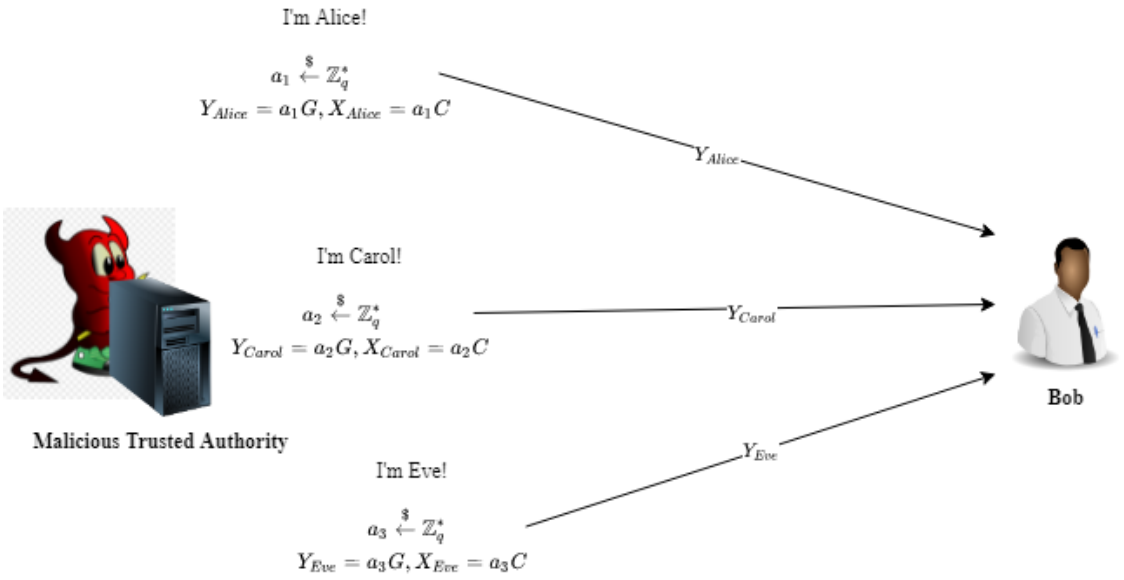

Figure 4: A malicious system authority impersonating Alice, Carol and Eve to a user Bob.

Due to this issue, the Wu and Lin proposed non-interactive authenticated key agreement protocol [19] is on par with identity-based schemes which also achieves trust level of 1 due to its nature architecture. Yet, Wu and Lin scheme is much more complicated than an identity-based scheme as more attacker's abilities must be captured in the security model of self-certified cryptography and thus is more open to possibilities where an attacker can break its security.

4.3 Third Issue: Forward-Secrecy of Shared Secret Key

Forward secrecy is an important property that must be achieved by an authenticated key agreement scheme. This property ensures that a shared secret key derived from users' private keys cannot be compromised even if one of the user's long-term private key is compromised in the future. This will put the confidentiality and integrity of the data communicated in the past and the future at risk.

According to Wu and Lin proposed non-interactive authenticated key agreement protocol, it can be easily seen that the secret keys shared between two parties will be similar for different sessions. This is because the shared secret is derived solely from the public/private key pair which never changes. The critical error made by Wu and Lin is not to involve any randomness in generating the shared secret key between two parties.

This proves to be a problem if a private key X_i of a user has been compromised. For example, if an adversary learns the private key X_1 of the user U_1, all communication prior using the shared secret key S_{12} between U_1 and U_2 will then be fully compromised. If the shared secret was used for encryption, then the adversary can fully decrypt all prior ciphertexts encrypted using S_{12}. If U_1 and U_2 wishes to rectify this problem, both parties will require new private keys (i.e., X_i) reissued.

Figure 5 shows what happens if an adversary manages to steal Alice's private key and is able

to ascertain the shared secret key $S_{Alice,Bob}$ that is shared between Alice and Bob. All messages encrypted using that shared key will then be compromised.

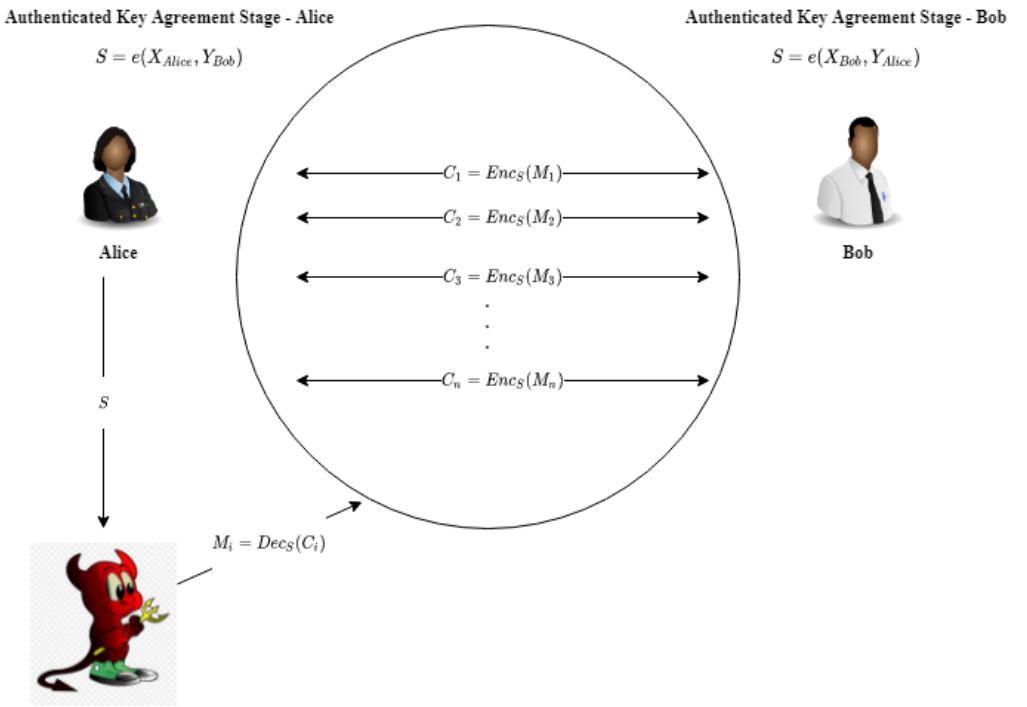

Figure 5: An adversary who manages to obtain Alice's secret can compute her shared key with Bob, and subsequently decrypt all messages that were encrypted using that shared key.

5 Conclusion

We presented three major security issues with the Wu-Lin non-interactive authenticated key agreement protocol which raises quite serious concerns. Until these issues are addressed, it seems that the on-interactive authenticated key agreement protocol is not secure to be deployed as the authors claim it to be. In order to withstand the attacks that we pointed out, the entire Wu and Lin's non-interactive authenticated key agreement protocol must be modified fundamentally. It is obvious that two parties must interact before deriving any shared secret key to fulfill the property of forward secrecy, and thus designing a secure on-interactive authenticated key agreement protocol remains as an open problem. The security analysis insight provided in this paper can be treated as the future concern in proposing a new authenticated key agreement protocol.

Acknowledgement The authors wish to thank the Ministry of Education of Malaysia and TM R&D for supporting this work with the Fundamental Research Grant Scheme (FRGS/1/2019/ICT04/MMU/02/5) and the TM R&D Fund.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] S. S. Al-Riyami & K. G. Paterson (2003). Certificateless public key cryptography. In *Advances in Cryptology - ASIACRYPT 2003*, pp. 452–473. Springer, Berlin, Heidelberg.

[2] M. Bellare, R. Canetti & H. Krawczyk (1996). Keying hash functions for message authentication. In *Advances in Cryptology — CRYPTO '96*, pp. 1–15. Springer, Berlin, Heidelberg.

[3] A. Biryukov, A. Shamir & D. Wagner (2001). Real time cryptanalysis of A5/1 on a PC. In *Fast Software Encryption*, pp. 1–18. Springer, Berlin, Heidelberg.

[4] S. Blake-Wilson & A. Menezes (1999). Authenticated Diffie-Hellman key agreement protocols. In *Selected Areas in Cryptography, SAC'98*, pp. 339–361. Springer, Berlin, Heidelberg.

[5] D. Boneh & M. Franklin (2001). Identity-based encryption from the Weil pairing. In *Advances in Cryptology — CRYPTO '01*, pp. 213–229. Springer, Berlin, Heidelberg.

[6] W. Diffie, P. C. Van Oorschot & M. J. Wiener (1992). Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, *2*, 107–125.

[7] M. Dworkin (2005). *Recommendations for Block Cipher Modes of Operation, Methods and Techniques*. NIST Special Publication 800-38B, United States, US.

[8] M. Girault (1991). Self-certified public keys. In *Advances in Cryptology — EUROCRYPT '91*, pp. 490–497. Springer, Berlin, Heidelberg.

[9] C. G. Günther (1990). An identity-based key-exchange protocol. In *Advances in Cryptology — EUROCRYPT '89*, pp. 29–37. Springer, Berlin, Heidelberg.

[10] M. Hou & Q. Xu (2009). Secure and efficient two-party authenticated key agreement protocol from certificateless public key encryption scheme. In *Fifth International Joint Conference on INC, IMS and IDC*, pp. 894–897. IEEE, Seoul.

[11] T. K. Mandt & C. H. Tan (2007). Certificateless authenticated two-party key agreement protocols. In *Advances in Computer Science - ASIAN 2006*, pp. 37–44. Springer, Berlin, Heidelberg.

[12] M. Michels & P. Hornster (1996). On the risk of disruption in several multiparty signature schemes. In *Advances in Cryptology — ASIACRYPT '96*, pp. 334–345. Springer, Berlin, Heidelberg.

[13] R. Mokhtarnameh, S. B. Ho & N. Muthuvelu (2011). An enhanced certificateless authenticated key agreement protocol. In *13th International Conference on Advanced Communication Technology (ICACT2011)*, pp. 802–806. IEEE, Gangwon.

[14] J. Pan, X. Liu, M. Xie & Q. Liu (2011). Certificateless-based two-party authenticated key agreement protocols in a multiple PKG environment. In *Proceedings of 2011 International Conference on Computer Science and Network Technology*, pp. 2364–2367. IEEE, Harbin.

[15] D. Park, C. Boyd & S.-J. Moon (2000). Forward secrecy and its application to future mobile communications security. In *Public Key Cryptography - PKC 2000*, pp. 433–445. Springer, Berlin, Heidelberg.

[16] A. Shamir (1985). Identity-based cryptosystems and signature schemes. In *Advances in Cryptology - CRYPTO '84*, pp. 47–53. Springer, Berlin, Heidelberg.

[17] L. Simpson, M. Henricksen & W. S. Yap (2009). Improved cryptanalysis of the common scrambling algorithm stream cipher. In *Information Security and Privacy*, pp. 108–121. Springer, Berlin, Heidelberg.

[18] Y. Wei, F. Wei & C. Ma (2014). Certificateless non-interactive key exchange protocol without pairings. In *11th International Conference on Security and Cryptography* (*SECRYPT*), pp. 1–12. IEEE, Vienna.

[19] T.-S. Wu & H.-Y. Lin (2013). Non-interactive authenticated key agreement over the mobile communication network. *Mobile Networks and Applications*, *18*, 594–599.

[20] Y. Zhao & S. S. M. Chow (2015). Privacy preserving collaborative filtering from asymmetric randomized encoding. In *19th International Conference on Financial Cryptography and Data Security*, pp. 459–477. Springer, Berlin, Heidelberg.