Chapter 2

Literature Review

In this chapter, the detailed review of previous works corresponding to the scopes and objectives of the present thesis has been presented. The whole literature review is divided into three parts: (1) Studies on various Authenticated Key Agreement (AKA) protocols for secure peer-to-peer and group communications, (2) Studies on the different types of Digital Signature (DS) schemes and their problems, (3) Studies on various existing one-factor remote user mutual authentication schemes and their drawbacks.

2.1 Literature Review for Authenticated Key Agreement Protocols

With the rapid development of the wireless telecommunication system, the user of portable mobile devices (e.g., Cellular phone, PDA, Notebook PC, Laptop, etc.) can carry out mobile services anytime and anywhere. Further, the flexibility and the mobility of wireless mobile networks, and the portability of hand-held mobile devices attract mobile users for peer-to-peer communication through the mobile networks. Recently, the secure and reliable group communication also becomes a significant concern for mobile networks due to the increase demand of the group-oriented applications such as teleconferences, interactive multi-user games, collaborative workspaces, dis-
tance learning, etc. However, the security and the privacy protection for peer-to-peer and group communications are two major issues when the communication media is an open network. To meet these security goals simultaneously, Two-party Authenticated Key Agreement (2PAKA) protocols for peer-to-peer communication and Authenticated Group Key Agreement (AGKA) protocols for group communication have been used, which are shortly reviewed here.

2.1.1 Two-party Authenticated Key Agreement Protocols

The authenticated key agreement protocols (AKA) become popular in recent years with the great attention for secure and reliable communication in many wireless mobile network applications such as mobile IP registration [1, 2], authentication protocol [4, 5], wireless mobile ad hoc networks [9], IP Multimedia Subsystem (IMS) [67], etc.

In general, two types of AKA protocols can be found: authenticated group key agreement (AGKA) protocol [2, 6, 7] and two-party authenticated key agreement (2PAKA) protocol [14, 15, 16, 45, 54, 55, 56, 57, 58, 59, 68, 69, 70, 71, 72, 73]. In any 2PAKA protocol, a secure and common session is established between two communicating users and the users can securely exchange the messages encrypted by the session key over any insecure and hostile network. In the open literature, the password-based authenticated key exchange (PAKE) protocol [46, 47, 48, 49, 50, 51, 52, 53] can also be found, which allows two communicating users to generate a session key over an open network. However, high computation cost and numerous communication rounds of these protocols, where a secret or a password is shared between a pair of users or with a trusted server prior to communication, makes unsuitable for the environments where the low-power mobile device is used.

In 2002, Hsieh et al. [74] proposed an enhancement of the Saednia’s protocol [75], where the reduction of the computational cost and the improvement of security aspects were made. However, Tseng et al. [76] demonstrated that Hsieh’s protocol cannot resist the key-compromise impersonation (K-CI) attack and thus proposed an
improved protocol to protect the same. Subsequently, Hölbl and Welzer [77] proposed an improvement of Hsieh’s protocol [74] and Tseng’s protocol [78] with much reduction in computation and communication cost. Later on, Zhang et al. [79] pointed out that the improved protocol is vulnerable to the impersonation attack (IA). Although Smart [55] proposed an ID-based two-party authenticated key agreement (ID-2PAKA) protocol using Boneh and Franklin’s IBE scheme [80], Chen and Kudla [54], and Shim [68] independently proved that the perfect forward secrecy (PFS) cannot be achieved in Smart’s protocol. Furthermore, Shim proposed an efficient ID-2PAKA protocol to remove the security pitfalls of Smart’s protocol but, Sun and Hsieh [45] demonstrated that Shim’s protocol [68] is susceptible to the man-in-the-middle attack (MIMA). An efficient ID-2PAKA using bilinear pairings was proposed by Ryu et al. [69] with minimum computation and communication costs. Also Ryu et al.’s protocol achieves better efficiency as it reduces the on-line pairing computation cost to zero, Boyd and Choo [81] showed that Ryu et al.’s protocol does not satisfy the K-CI resilience property. Recently, Wang et al. [81] identified a weakness in Ryu et al.’s protocol, called reflection attack (RA) and proposed an improved protocol to remove the weakness found. An ID-2PAKA protocol was proposed by McCullagh and Barreto [56], which has been analyzed by Xie [71], and Choo et al. [82] and pointed out that the protocol does not have the K-CI resilience property. Although they proposed an improvement of McCullagh and Barreto’s protocol, it still vulnerable to K-CI attack as mentioned by Li et al. [72].

In 2005, Sui et al. [48] proposed an ECC-based PAKA (password-based two-party authenticated key agreement) protocol, which offers PKG’s forward security (PKG-FS) and it was included in third generation partnership project (3GPP2) specifications to improve the security of authenticated key distribution protocol useful for wireless communications. However, Lu et al. [46] shows that the protocol is vulnerable to off-line password guessing attack (OPGA), and then proposed an improvement of the protocol in [48]. Unfortunately, Chang et al. [47] proves that Lu et al.’s protocol is
not secure against the parallel guessing attack (PGA) and then proposed a modified protocol to remove the security flaws of [46]. However, Lo et al. [49] demonstrated that Chang et al.’s protocol [47] lacks to provide mutual authentication property. Lo et al. also proposed an improved PAKA protocol using Elliptic Curve Cryptography (ECC) [83, 84] and claimed that the protocol could resist various attacks. In 2010, Pu [50] independently demonstrated that Lu et al.’s protocol cannot resist off-line password guessing attack. Recently, Youn et al. [51] discovered some security weaknesses of Guo et al.’s protocol [52] and proposed an efficient protocol.

### 2.1.2 Authenticated Group Key Agreement Protocols

This section provides an ample literature survey related to the AGKA protocol for group communication in imbalanced mobile networks. In 2004, Bresson et al. [85] proposed a group key agreement (GKA) protocol with two rounds for imbalanced mobile networks based on public key infrastructure (PKI) [86] and ElGamal encryption scheme [23] with Shamir’s secret sharing technique [87]. In 2005, Nam et al. [88] pointed out that Bresson’s protocol [85] is a group key distribution (GKD) protocol rather than a GKA protocol and does not meet the perfect forward security (PFS), implicit key authentication and known-key security properties of the agreed session key. In [17], the authors proposed an improved two round GKA protocol that can overcome the security patches of [85]. Furthermore, they transform their two round GKA protocol to a three round AGKA protocol by means of Katz-Yung scalable complier [89], which is well suited for a mobile network and provably secure under the Decisional Diffie-Hellman (DDH) assumption [90]. However, Tseng [18] pointed out that Nam et al.’s protocol [17] is not a real GKA protocol as it does not achieve the security requirement of no key control, because the group key can be determined by the powerful node alone rather than all mobile nodes. In order to cope with the security loopholes of [17], Tseng [91] also proposed a provably secure contributory GKA protocol based on DDH assumption for mobile networks. Unfortunately, Lee et al. [19] demonstrated that the
Tseng’s GKA protocol is a non-authenticated GKA protocol that cannot ensure the validity of the transmitted messages. Further, they proposed a bilinear pairing-based non-authenticated GKA protocol, and then extended it to an AGKA protocol and claimed that both of the proposed protocols were intended to provide provable security under the Bilinear Computational Diffie-Hellman (BCDH) assumption [34].

In 2011, Cheng et al. [20] and Tsai [21] independently analyzed Lee et al.’s AGKA protocol and pointed out the vulnerability against impersonation attack such that any non-group member can masquerade as a legal mobile node to determine the contributory group key. Simultaneously, Cheng et al. proposed an improved AGKA protocol using bilinear pairing [34], and its security relies on the hardness assumption of ECDLP [12] and BCDH [34] assumptions in the Manulis et al.’s model [92]. In [20], the static private key and ephemeral key are combined using hash function in order to resist the ephemeral key compromise attack/known session-specific temporary information attack (KSSTIA) [12, 93, 94], which has not been considered in [19, 21]. Further, Yuan et al. [93] shows that Lee’s protocol is vulnerable to the key off-set attack/key replicating attack (KOA/KRA) [95], which is a variant of the man-in-the-middle attack. According to Black-Wilson et al. [95], in KOA/KRA attack, an active adversary can intercept, modify and delete the messages exchanged between entities, and can force them to accept the same session key, which is not actually the one the entities want to agreed on. They also pointed out that any authenticated key agreement protocol, which does not contain asymmetry in the session key formation, is vulnerable to this attack. In 2011, based on ECDLP and BCDH assumptions, Tsai [21] proposed an efficient AGKA protocol for mobile networks using bilinear pairings and Zhang et al.’s short signature scheme [24], where the signature scheme is proven to be secure against adaptive chosen-message attack in the random oracle model [41].

The KSSTIA attack as described in [94, 96, 97] states that if the session ephemeral secrets are leaked to an adversary accidentally, the secrecy of the established session key should not be compromised. In [12, 92], the authors argued that the security con-
2.2 Literature Review for Digital Signature Schemes

When messages are exchanged over any public channel, the digital signature is one of the most fundamental tools used for achieving message integrity, authenticity and non-repudiation. One of the variations of digital signature is partially blind signature (PBS) that allows a signer to explicitly include the common information (e.g., expiration date, collateral conditions, etc.) into the blind signature. In PBS, a signer blindly signs a message submitted by a user without disclosing the original message and the corresponding signature. In banking sector, PBS scheme is used for online e-cash system design that helps a customer to withdraw money from a bank and then he can spend it to a merchant for purchasing some goods. In this section, we discussed some earlier works and their shortcomings related to digital signature and PBS schemes.

2.2.1 Certificateless Digital Signature Schemes

Al-Riyami and Paterson [38] first establish the notion of certificateless digital signature (CL-DS) scheme in 2003, later on, Huang et al. [98] demonstrated that the scheme is susceptible against public key replacement attack, and they proposed a new CL-DS scheme as a remedy. After the pioneer work of Al-Riyami and Paterson, many CL-DS schemes [99, 100, 101, 102, 103, 104, 105, 106, 107] have been proposed in recent years. In 2006, Zhang et al. [99] constructs a more efficient security model over the model presented in [98]. Huang et al. [100] independently defines three types of adversaries, called normal adversary, strong adversary and super adversary according to their attack
2.2 Literature Review for Digital Signature Schemes

powers. They also revisited the security models of CL-DS schemes and proposed two schemes, which were proven to be secure in the random oracle model [41, 42] against all potential adversaries. In 2004, Yum and Lee [101] also proposed a new CL-DS model and claimed strong security against all adversaries, however, Hu et al. [108] shows that the security assumptions adopted in [101] are insufficient to protect the key replacement attack by an outsider. Subsequently, Hu et al. proposed a modernized scheme and its security was established in a new and simplified model.

In 2005, Gorantla and Saxena [102] designed a pairing-based CL-DS scheme, which, according to their claim, can provide the desirable security and computation efficiencies, later on, Cao et al. [109] illustrated the vulnerability of the scheme against the public key replacement attack. In 2004, Yap et al. [103] proposed a pairing-based CL-DS scheme based on the intractability of the CDH assumption in the random oracle model. The scheme is computationally efficient since the signing phase is free from costly bilinear pairing operation and the verification phase requires two pairing computation. However, Zhang and Feng [110] analyzed that the public key replacement attack could be mounted in Yap et al.’s scheme. To cope with the problem of [103], Hu et al. proposed an improved CL-DS scheme. In 2007, Choi et al. [104] constructs an efficient CL-DS scheme using elliptic curve bilinear pairing and then analyzed its security in the random oracle model based on the CDH and mICDH (Modified Inverse CDH) assumptions. Recently, two CL-DS schemes were proposed in [105, 106] and the authors claimed that the schemes were intended to provide the strong security in the random oracle model against adaptive chosen message and identity adversaries. Unfortunately, the works [111, 112] show that the former scheme is insecure against universal forgeries under known message attack; whereas no attack yet has been found in the latter scheme.

2.2.2 Partially Blind Signature Schemes

In 1983, Chaum [27] firstly introduced the notion of blind signature scheme and since then several blind signature schemes have been proposed using traditional PKI or
2.2 Literature Review for Digital Signature Schemes

Shamir’s IBC scheme [8]. Some of them with their shortcomings are discussed here. In 2011, Eslami and Talebi [113] proposed an untraceable off-line e-cash system using RSA-based blind signature under the assumptions that the discrete logarithm problem (DLP) and integer factorization problem (IFP) are intractable in a large cyclic group of prime order. Their scheme can exchange the old e-cash into new ones by adopting a mechanism called exchange protocol that can greatly reduce the bank’s database. Also, their scheme employed ElGamal signature [23] to prevent the double-spending of e-cash. Chow et al. [114] first presented an identity-based partially blind signature scheme (ID-PBS) based on bilinear parings and MTP function. Their scheme possesses the property of simplifying the certificate management as compared with other PKI-based partially blind signature (PBS) schemes. However, Chow et al.’s scheme involves expensive computations for its implementation. In 2000, Abe and Okamoto [26] gave formal proof of security for their schemes. Also Fan and Lei [115] and Zhang et al. [116] proposed a PBS scheme based on quadratic residues problem and a pairing-based PBS scheme, respectively.

Recently, Huang and Chang [117] proposed a new efficient PBS scheme based on DLP and Chinese Remainder Theorem (CRT). They claimed that their scheme is secure and efficient. However, Zhang and Chen [118] show that the scheme cannot achieve the partial blindness property of a partial blind signature scheme, because a malicious user can prepare a forged blind factor and remove the original blind factor from the signer’s signature to obtain a forged signature. In 2008, Hu and Huang [119] proposed an efficient ID-PBS using bilinear pairings. They claimed that the scheme is provably secure in the random oracle model [41, 42]. However, Tseng et al. [120] show that Hu and Huang’s scheme suffers from forgery attacks. In 2007, Chen et al. [121] first proposed an ID-based restrictive partially blind signature from bilinear pairings. Their scheme incorporates the advantages of partially blind signatures and the restrictive blind signature. However, Hu and Huang [119] show that Chen et al.’s scheme has a security weakness due to lacking of restrictiveness property, and also
2.2 Literature Review for Digital Signature Schemes

the prevention of *double-spending of e-cash* has not been satisfied. Lin et al. \cite{122} proposed a provably secure self-certified PBS scheme and claimed that the scheme is secured in their proposed security model. However, Zhang and Gao \cite{123} analyzed that Lin et al.’s scheme is insecure, because anyone can produce a forged signature on any message in the name of any other user, i.e., the scheme doesn’t achieve *non-repudiation* property.

There are different types of electronic payment systems such as (1) online credit card payment \cite{124, 125}, (2) smartcard-based electronic payment \cite{126}, (3) electronic cheque (e-cheque) \cite{127, 128}, (4) e-cash system \cite{28, 113, 129}, etc. Nowadays e-cash system becomes more and more popular, because it can ensure the privacy of customers, risk of customer identity theft and customer fraud in various electronic transactions \cite{31}. However, the efficient implementation of an e-cash system is still an important issue in e-commerce research area. To design an efficient e-cash system, Chaum \cite{27} firstly proposed the concept of blind signature scheme that allows a user to obtain a signature from the signer without revealing anything about the message to the signer and the signature obtained. The e-cash system can be categorized into two types, which are online e-cash system \cite{28, 30, 129, 130, 131, 132, 133, 134} and off-line e-cash system \cite{32, 33, 113, 132, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145}.

The anonymity of the customer is of great importance in e-cash \cite{129, 134}, so the blind signature \cite{146, 147}, which hides customer identity, can play an important role in this application. For e-cash system, anonymity ensures that the bank and the merchant cannot trace the customer from the e-cash spent previously. Although the blind signature achieves the property of *blindness, anonymity, verifiability* and *unforgeability*, it cannot be applicable fully in e-cash system for real-life applications as many other limitations can be found in e-cash system. Some of them are given now. The bank must have different private and public key pairs for different face values of e-cash provided by the customers. For this, the customers and the merchants must always carry a list of bank’s public keys in their electronic wallet. Also, the bank
normally keeps a database to store information about all e-cashes that were previously spent to identify the double-spending. Thus, the size of bank’s database would become huge over time. In addition, the blindness property of the blind signature is undesirable in a simple e-cash system, because the expiration date, time and face value of e-cash cannot be incorporated in blind signature.

2.3 Literature Review for Remote User Mutual Authentication Schemes

The remote user mutual authentication system provides the availability of the resources to the authenticate users only. In this system, the remote server and the user are authenticated by each other so that any unauthorized access by an illegal user is protected. After mutual authentication, a common secret session key is established between the server and the user, which would be user for subsequent communication to achieve the message confidentiality. In the open literature, different types of remote user mutual authentication schemes are available and in this section, we provide a literature survey on some of the one-factor password-based and identity-based remote user mutual authentication schemes.

2.3.1 Password-based Remote User Mutual Authentication Schemes

In 1981, Lamport [148] suggested a hashed-based password authentication scheme that mutually authenticates the client and the remote server successfully. Although it is immune from server’s data eavesdropping and impersonation attack, the scheme is vulnerable to reply attack, suffers from high hash computation cost and password resetting problem, which makes it inefficient for practical use. Peyravian and Zunic [61] proposed encryption-less password authentication and password change schemes
2.3 Literature Review for Remote User Mutual Authentication Schemes

using only collision-resistant one-way hash function (OWHF), which is simple and straightforward for implementation as it employs only cryptographic hash function. Later on, Lee et al. [149] showed that the scheme [61] suffers from off-line password guessing attack (OPGA) and then proposed an improved version of the Peyravian and Zunic’s scheme but, Ku et al. [150] demonstrated that Lee et al.’s scheme has some security flaws such as denial of service (DoS) attack, stolen-verifier attack and OPGA. In 2004, Yoon et al. [151] proposed an improvement of Lee et al.’s scheme but, it has been analyzed by Ku et al. [150] that Yoon et al.’s scheme is still vulnerable to OPGA, stolen-verifier attack and their scheme does not provide forward secrecy (FS). Again, Hwang and Yeh [62] mentioned that Peyravian and Zunic’s scheme also vulnerable to OPGA, server spoofing attack and data eavesdropping attack, and proposed some improvements using public key cryptosystem. Hwang and Yeh’s scheme can achieve mutual authentication and renovates the security problems present in Peyravian and Zunic’s scheme but, Ku et al. [152] showed that the scheme cannot prevent the replay attack. Later on, it has been made known by Lin and Hwang [60] that Hwang and Yeh’s scheme suffers from DoS attack and does not provide perfect forward secrecy (PFS), and proposed an improved scheme that can accomplish mutual authentication and generate a secret key between the client and the remote server.

Again in 2006, Peyravian and Jeffries [153] enhanced Peyravian and Zunic’s scheme; however, Shim [154] claimed that Peyravian and Jeffries’s scheme suffers from offline password guessing attack and denial of service attack. In 2006, Chang et al. [155] proposed a new password authentication scheme based on the symmetric key cryptosystem. However, the distribution of the symmetric key was a burden on the client side as the symmetric key exchange is an immense challenge over the unreliable networks. Recently, Zhu et al.’s scheme [63] claimed that Hwang and Yah’s scheme still susceptible to replay attack, DoS attack, stolen-verifier attack and impersonation attack and then, proposed an enhanced scheme based on public key encryption/decryption with timestamp and salting technique to eliminate the weaknesses of Hwang and Yeh’s
2.3 Literature Review for Remote User Mutual Authentication Schemes

scheme. Zhu et al.’s scheme used a hardware component, called trusted platform module (TMP) [156], which safely stores the salt file in the hard disk of the client’s machine. However, Zhu et al.’s scheme has the serious clock synchronization problem due to timestamp, and the TPM puts a burden on the client.

Recently, several password-based remote user authentication schemes based on smartcard [157, 158, 159, 160, 161, 162, 163, 164] have been implemented for logging into the remote server. These schemes can provide mutual authentication between the client and the server over insecure networks, where the client is authenticated by the remote server using an easy-memorable password without maintaining a password-verifier table and vice versa. But most of them are vulnerable to off-line password guessing attack [164, 165, 166, 167], impersonation attack [160, 164, 167, 168], DoS attack [164, 165, 167], parallel session attack [166], replay attack [165], etc. Except these attacks, the existing smartcard-based schemes are vulnerable to stolen/lost smartcard attack [169] as some sensitive verifying token and secret values stored in the smartcard can be extracted by monitoring their timing information, power consumption [167] and reverse engineering techniques mentioned by Kocher et al. [170] and Messerges et al. [171]. Therefore, if an adversary steals a smartcard of a legitimate client, he can use it to produce a fabricated login message, and then impersonate as a legal client.

2.3.2 ID-based Remote User Mutual Authentication Schemes

In traditional remote login schemes, the remote server has to maintain users’ secrets to a verifier table, which is used to verify the legitimacy of the users. Some of the verifier-based mutual authentication schemes are [60, 61, 148, 149, 151, 153], etc. that are susceptible to the risk of modifying the verifier-table and vulnerable to some of the attacks such as stolen-verifier attack [150, 172], OPGA [149, 150, 154, 172], DoS attack [150, 154], etc. In recent years, researchers are directed to the smartcard-based remote user mutual authentication scheme to provide the adequate security. Static login identity-based authentication scheme [173, 174, 175] with smartcard is one of
the most convenient methods for remote user authentication. However, in several applications (e.g., digital library, online e-voting, pay-TV, etc.), a transaction with static login-identity discloses some personal information about the user. An outsider may intercept the user’s login message and try to manipulate with other parameters to forge the user’s login identity, which is known as identity-theft attack [174].

In addition, static login identity-based scheme has high risks of vulnerability against off-line password guessing attack [164, 165, 174], denial of service attack [164, 165, 176], forgery attack [164, 165, 176, 177], etc. For these reasons dynamic identity-based remote user login scheme with smartcard [174, 178, 179, 180] is comprehensively accepted. In dynamic identity-based remote login with smartcard, user’s identity is changed during each transaction and since the remote server does not keep the verifier table, so the risk of modification and hacking of verifier-table, etc. are avoided, and thus, the protection against forgery attack is possible. We have studied several dynamic identity-based schemes and found that most of them are vulnerable to the off-line password guessing attack [181], impersonation attack [181, 182], denial of service attack [181], and observing power consumption [170] and physically exposing [171] the chip as well to extract the data stored on smartcard.