Chapter 1

Introduction

Today computer networks and wireless networks have been well developed and become more useful than the earlier days [1, 2, 3], and in order to accomplish the communication efficiently, most of the people use Internet and/or wireless networks and exchange their multimedia information fruitfully [4, 5]. Although IT/ICT dominates nowadays, none of the information and communication technology like Internet is secured. Because the Internet is an open network system deployed and managed by different entities/organizations and no security measure has been adopted neither in its inception nor any such security is provided during its subsequent development and expansion. On the other hand, the wireless communication is inherently more vulnerable [6, 7] than the wired networks as any data packet in wireless system is always exposed and until the data is itself protected using any cryptographic technique [8, 9, 10], it is easily accessible by opponents. Therefore, some cryptographic techniques need to be adopted to achieve security and privacy protection of the important messages communicated over open networks.

In fact, the cryptographic techniques comprise a variety of security mechanisms like information confidentiality, integrity, availability, authentication, etc. including different techniques used in securing the computer communication. As an illustration for the

data confidentiality, the symmetric key and asymmetric key/public key cryptosystems are used, where DES, AES, IDEA, RC4, RC5, etc. and RSA, Rabin, ElGamal, etc. [11, 12] are called symmetric and public key cryptosystems, respectively. In the former case, sender and receiver assume the sharing of a single secret key a priori to be used for message encryption-decryption, and in the latter case, there are two keys known as private key and public key, where a sender uses the receiver's public key for encryption and the receiver decrypts the same using his/her own private key. In addition, the uses of cryptography has been extended in other important areas like non-repudiation, integrity and authentication [11, 12, 13] of the message and message source, where if the proper authentication is not provided, then different attacks like masquerading, repudiation, replay, etc. may occur. In the present work, we develop some cryptographic techniques in three major sub-areas using ECC like (1) Authenticated key agreement protocols, (2) Digital signatures and (3) Remote user mutual authentication schemes and they are briefly described now.

Two secure session key agreement protocols corresponding to two-party and group key (multi-party) communication are developed, where important messages can be securely exchanged by encrypting/decrypting the same using the session key established. The meaning of a session key is that in each session of secure communication, a new secret key is to be always established and used. These protocols are very useful in real-life applications, because if a shared key, a key that is used for many sessions, is exposed by any means to a third party, then the confidentiality of the messages transmitted in all the sessions with the same shard key are lost. On the other hand, if a session key is leaked then the message confidentiality of that session only is lost. Besides, establishing a session key for either peer-to-peer or group communication over unreliable network is a big challenge and involves more risks. Thus, the agreement and use of one-time session key is reasonable and several methods for establishing a session secret key have been proposed [14, 15, 16, 17, 18, 19, 20, 21].

As stated, the authenticity, integrity, non-repudiation of the messages are essential for protecting some common attacks, the current research works have also been carried out in this direction. Although some schemes based on digital signature are available [8, 22, 23, 24, 25], the present works propose two new efficient signature schemes, called certificateless digital signature (CL-DS) and identity-based partially blind digital signature (ID-PBS) based on ECC and pairing-free concept [26, 27, 28]. The signature scheme can be found useful in information and network security applications, where the detection of forgery or tampering of digital documents is the key requirement. As an application, we develop an online e-cash system using the proposed ID-PBS scheme. Note that the e-cash system is very much helpful for anonymous payment in online purchasing useful in e-commerce application [29, 30, 31, 32, 33]. It may be noted that the ID-PBS scheme is a variant of ordinary digital signature, which allows a signer (bank) to sign a message blindly for a user (customer) that explicitly includes some common information agreed between the signer and the user, and the corresponding unblind message and the signature are verified publicly.

The rapid development and use of network and information technologies, in addition to other, attract users also to access the remote server through Internet; however the secure access to remote server becomes a great challenge. Although Internet is accessible worldwide, and if a user wants to access some protected resources residing at remote server, then he needs to authenticate himself as a legitimate user to the remote server before the server allows to get access to the protected resources. However, the remote user authentication is not enough for full security, the server authentication by the user is equally important, known as mutual authentication; otherwise an adversary may impersonate the remote server to cheat the legitimate user. For this purpose, the present work has also investigated to develop two ECC-based remote user mutual authentication schemes using password-based concept and identity-based cryptosystem, respectively, which show efficient performance in remote login operations.

1.1 Objectives and Scopes of the Thesis

The present thesis addresses the design of some useful and fundamental techniques such as self-certified public key cryptosystem-based two-party authenticated and identity-based authenticated group key agreement protocols, certificateless digital signature and identity-based partially blind signature schemes, password-based and identity-based remote user mutual authentication schemes, where an online e-cash system has been developed using the identity-based partially blind signature schemes as an application. However, it can be noted that most of the cryptographic techniques available in the open literature are designed in the above mentioned areas are in support of the certificate authority-based public key cryptosystem/public key infrastructure (CA-PKC/PKI). As a result, they have some limitations: (1) Protocols execute modular exponentiation operation, which is the most time consuming operation known in cryptography, (2) Protocols need a certificate authority (CA) to maintain the public keys and the corresponding certificates of the users and, for a large number of users, CA requires huge storage space and complex certificate management process to keep up and store the public keys and certificates, and (3) Users need to verify the corresponding certificate of others for which extra computations are involved. These problems degrade the overall performance of the system and thus, the CA-PKC-based protocols are not suitable for practical application especially for resource (e.g., energy, storage, computing power, etc.) constrained devices like PDA (Personal digital assistant), Laptop, Mobile phone, Smartcard, etc.

Recently, Elliptic Curve Cryptography (ECC)-based protocol gets huge attention since it is based on additive cyclic finite group (instead of multiplicative group) and it offers same level of security with a less bit key-size. As an instance, a 160-bit ECC secret key has same security level as a 1024-bit RSA secret key [12]. In addition, the ECC-based operations like elliptic curve point addition and scalar point multiplication are much faster than the modular exponentiation. So any ECC-based protocol has

shorter message-length, and needs low computing and communication costs. However, the ECC-based protocols also suffer from some drawbacks like (2) and (3) as mentioned earlier in the PKI based schemes.

Our proposed ECC-based protocols/schemes presented in this thesis are immune from these drawbacks. In order to eliminate these problems, identity-based, self-certified public key-based and certificateless public key-based cryptosystems are used. In identity-based cryptosystem (IBC), which was first proposed by Shamir [8], the public key certificate is not required since the publicly known identity of a user is used as a public key. The corresponding private key of the user is computed by a trusted third party, called Private Key Generator/Key Generation Center (PKG/KGC), which is securely handover to the corresponding user. Similar to RSA, Shamir proposed a smartcard-based digital signature scheme using IBC, however no encryption/decryption scheme was devised until 2001, and Boneh and Franklin [34] first proposed a practical identity-based encryption/decryption (IBE) scheme using ECC and bilinear pairing [35, 36] as an implementation of IBC. In order to the full functionalized of IBE, Boneh and Franklin also introduce a special type of hash function known as map-to-point (MTP) hash function [34] that actually converts a random string of arbitrary length to a point on an elliptic curve.

It can be noted that the IBC/IBE-based protocols are used widely in various applications and same has been used in our most of the works, however it has one drawback called the private key escrow problem. Since PKG generates the private key of the users, it can easily impersonate any user if PKG is not fully trusted, which is known as the private key escrow problem. In 1991, Girault [37] first introduce the concept of self-certified public key cryptosystem (SC-PKC) that seems to be more efficient than PKI and IBC. In this cryptosystem, a trusted third party, called system authority (SA) generates user's public key that does not need a separate certificate for authentication. Because the public key is computed jointly by SA and the user, and the corresponding private key computed by the user is unknown to SA. Thus, the SC-PKC eliminates the

need of public key certificate and the private key escrow problem. On the other hand, Al-Riyami and Paterson [38] proposed a variant of PKC, called certificateless public key cryptography (CL-PKC), which has the abilities to remove the certificate management problem of PKC and private key escrow problem of IBC. Recently, CL-PKC is also applied in developing numerous cryptographic protocols and the present thesis has also incorporated CL-PKC to avoid private key escrow problem. The objectives and scopes as the salient features of the thesis are summarized below.

- **Elimination of Public Key Certificate:** The protocols presented in this thesis are based on SC-PKC, IBC and CL-PKC, thus eliminate the requirement of any Certificate Authority (CA) to store and manage the certificates of the public keys.

- **Bilinear Pairing and Map-to-point Hash Function-free Realization:** The relative computation cost of the bilinear pairing is approximately two to three times more than an elliptic curve scalar point multiplication (ECPM) and the computation cost of MTP hash function is more than an ECPM [14, 15, 39, 40]. In addition, the implementation of bilinear pairing needs a non-singular elliptic curve group with large group-size and MTP is usually implemented as a probabilistic algorithm [16]. The proposed protocols in most of the cases thus implemented without using them or minimally using either of them.

- **Efficiency in Computation and Communication Cost:** Since the proposed ECC-based protocols provide comparable security using smaller key size [12, 15], our protocols require low communication cost and computation cost is also reduced.

- **Security Analysis:** In this thesis, an in-depth security analysis of each and every proposed protocol is given. However, informal security analysis for some of them is provided, where a number of theorems have been presented that show attack resilience of our protocols against varieties of attacks known. Moreover, formal security model called Random Oracle Model [41, 42] for rest of the protocols is given that prove strong security against different types of adversaries.

1.2 Contributions of the Thesis

The main contributions of the thesis are the works carried out in the areas of designing authenticated key agreement protocols, digital signature and remote user mutual authentication schemes. Due to cryptographic advantages of ECC, three core ECC-based cryptosystems like SC-PKC, IBC and CL-PKC are employed in the protocols presented in this thesis. In addition, none of our proposed authenticated key agreement protocols and digital signatures do not apply costly bilinear pairing and probabilistic MTP hash function, however, two ECC-based remote login systems designed based on password and IBC use only bilinear pairing and MTP hash function, respectively. The main research works of the thesis are divided into three major areas, the contribution of each is given below in brief:

Design of Pairing-free Authenticated Session Key Agreement Protocols

- **Two-Party Authenticated Session Key Agreement Protocol:** In the open literature, several 2PAKA protocols [43, 44, 45, 46, 47] using PKI, and/or costly bilinear pairing and probabilistic MTP hash function have been proposed for two-party communications, and especially in resource constrained environments. Also most of the 2PAKA protocols involve comparatively more number of communications round, which make them unsuitable in low-power mobile devices. Furthermore, in password-based 2PAKA protocols [48, 49, 50, 51, 52, 53], a user in advance needs to share a large number of secrets in respect of each member of a group for large scale peer-to-peer communication, which has also high risks of secret leakage to adversaries. In addition, IBC-based 2PAKA protocols [14, 15, 16, 54, 55, 56, 57, 58, 59] have key escrow problem and most of the previous 2PAKA protocols are not well secured, and computation and communication efficient. To mitigate these problems, based on SC-PKC, we designed a 2PAKA protocol with minimal communication round and computation cost. The security analysis against different attacks found

in the open literature has been discussed and satisfactory results have been achieved. Also the comparative results of our protocol with the previous protocols are given.

- **Authenticated Group Key Agreement Protocol:** In imbalanced mobile networks, secure and reliable group communication becomes an important issue due to the increase demand of group-oriented applications. To meet the security and privacy goal in imbalanced mobile networks, an identity-based authenticated group key agreement (ID-AGKA) protocol in ECC have been proposed without bilinear pairing and MTP hash function. The secrecy of the session key relies on the difficulty of solving the OWHF (One-way Hash Function), ECDLP (Elliptic Curve Discrete Logarithm Problem) and CDHP (Computational Diffie-Hellman Problem). The proposed pairing-free ID-AGKA protocol is computation efficient contributory group key agreement protocol that protects various attacks namely *known group key attack*, *key compromise impersonation attack*, *known session-specific temporary information attack*, *impersonation attack*, etc. The proposed protocol is a dynamic group key agreement protocol in which a set of existing users may leave the group or a set of new users can join the existing group at any time. Note that the property of *backward secrecy* of the session key is confirmed in the proposed protocol, which means none of the leaving member can compute any future session key. For joining of user(s), the new member has no ability to compute any of the old session keys, i.e., the *forward secrecy* of the group session key is also satisfied. The proposed protocol is suitable for the application in many imbalanced wireless mobile network areas such as internet stock quotes, audio, music delivery, etc.

Design of Efficient and Secure Pairing-free Digital Signature Schemes

- **Digital Signature Scheme:** Recently, certificateless public key cryptography (CL-PKC) proposed by Al-Riyami and Paterson [38] has received an immense exposure over the CA-PKC/PKI and IBC due to the removal of public key certificate as required in CA-PKC and key escrow problem occurred in IBC. We proposed a

certificateless digital signature (CL-DS) in ECC, which has strong security under the adaptive chosen message and identity attacks against two types of adversaries available in any CL-PKC systems. The proposed CL-DS scheme has ease-of-use implementation facility, computation and communication efficiencies as it is free from two cost-intensive operations, namely bilinear pairing and MTP hash function. The proposed CL-DS scheme is proven to be secured in the random oracle model with the hardness assumption of ECDLP. Therefore, our CL-DS scheme is most suitable than others in low computing and insecure information/network security applications.

- **Partially Blind Signature Scheme:** A provably secure identity-based partially blind signature (ID-PBS) scheme in the random oracle model is proposed without bilinear pairing operation and MTP hash function. The proposed ID-PBS scheme is adaptive chosen and identity attacks resistant with the assumption that ECDLP is intractable in the elliptic curve group by a polynomial-time bounded algorithm. In the thesis, the proposed ID-PBS scheme is applied in efficient implementation of online anonymous e-cash system that provides different security properties such as *unforgeability*, *unlinkability*, *non-deniability* and *prevention of double spending of e-cash*. The proposed e-cash system is found to be suitable in banking application due to its low computation and communication costs, and strong secure property.

Design of Secure and Efficient Remote User Mutual Authentication Schemes

- **Password-based Remote Login Scheme:** The password-based remote user mutual authentication scheme proposed by Lin and Hwang [60] is studied and identified some security flaws. Also some other related schemes proposed by Peyravian and Zunic [61], Hwang and Yeh [62], and Zhu el al. [63] are cryptanalyzed in this thesis and some shortcomings are observed. In this section, an ECC-based improved password authentication scheme to remove these flaws has been presented that simultaneously supports the generation of session key through mutual authentication between the client and remote server. The proposed scheme is compared with a

number of existing schemes in terms of security, computation and communication efficiencies and better results have been found.

- **Identity-based Remote Login Scheme:** Yang and Chang's identity-based remote login scheme [64] and other two improved schemes proposed by Yoon and Yoo [65], and Chen et al. [66] are analyzed and observed some weaknesses. To cope with these security loopholes, we proposed a more efficient and secure dynamic identity-based remote login scheme based on ECC usable for low-power mobile devices. The proposed scheme provides *mutual authentication*, *session key agreement* and *revocation of leaked key with same identity* and *removes clock synchronization problem* and *password verification table*. Compared with other schemes, the proposed scheme is found to be well secured and computation efficient.

1.3 Outline of the Thesis

After briefly presenting the objectives, scopes and contributions of the current thesis, this section describes the organization of the thesis as follows, where the Chapters 4-9 are contributory chapters of the current thesis:

- Chapter 1 provides the introduction of this thesis that contains thesis background, objectives and scopes of the research work, and the main contributions of the thesis.
- Chapter 2 presents through literature review of the selective earlier works related to the authenticated key agreement protocol, digital signature and remote user mutual authentication schemes, and restated their shortcomings available.
- Chapter 3 provides short and snappy theoretical background on ECC, IBC, bilinear pairing, computational problems, OWHF and zero-knowledge protocol. These preliminaries discussed in this chapter can be used as supplement for the remaining part of the thesis.

- Chapter 4 proposes a 2PAKA protocol based on ECC and self-certified public key cryptosystem (SC-PKC). The security analysis of the protocol against different attacks is given and a comparative study in terms of the security, computation and communication costs with other competitive protocols is provided.

- Chapter 5 designs an efficient ID-AGKA protocol using ECC for secure and reliable group communication in imbalanced mobile networks. Here the security performance of the proposed protocol is established based on the infeasibility of OWHF, ECDLP and CDHP. The proposed protocol is also compared in terms of computation and communication overheads with other existing protocols.

- Chapter 6 presents an ECC-based CL-DS scheme without bilinear pairing and MTP hash function. The proposed CL-DS scheme is proven to be provably secure in the random oracle model under the adaptive chosen message and identity attacks based on hardness assumption of ECDLP. In addition, the scheme, from computational point of view, is shown to be more effective than known schemes.

- Chapter 7 proposes a pairing-free ID-PBS scheme using ECC, which is shown to be provably secure in the random oracle model based on the intractability of ECDLP. In this chapter, an online e-cash system for e-banking is also presented as an application of the proposed ID-PBS scheme. It is seen that the proposed e-cash system is computation and communication efficient and satisfies *unforgeability*, *anonymity*, *non-deniability* and *detection of double-spending of e-cash* as well.

- Chapter 8 cryptanalyzes some of the earlier password-based remote user authentication schemes designed by Lin and Hwang [60], Peyravian and Zunic [61], Hwang and Yeh [62], and Zhu el al. [63] and proposes a scheme using ECC. The security analysis and comparison with existing schemes of the proposed scheme in terms of different parameters are given and found improved performance.

- Chapter 9 cryptanlyzes Yang and Chang's identity-based remote login scheme [64] and other schemes like Yoon and Yoo [65], and Chen et al. [66] developed based on [64] and identifies similar types of security loopholes in all of them. Hence, an improved identity-based remote login scheme based on ECC for removing these loopholes and usable for low-power mobile devices is proposed. It is to be noted that the proposed scheme supports low computation cost, mutual authentication, session key agreement and other security features.

- Chapter 10 summarizes and concludes the thesis, and discusses the future research scopes related to the research works presented in this thesis.