A Survey on Certificateless Encryption Techniques

Fahad T. Bin Muhaya
Management Information Systems Department, College of Business Administration
Prince Muqrin Chair for IT Security (PMC), King Saud University, Riyadh, Kingdom of Saudi Arabia
E-mail addresses: fmuhaya@ksu.edu.sa

Abstract— Certificateless public key encryption is an advanced version of identity-based and public key encryption techniques. It eliminates the inherent key escrow and other key management issues in both techniques, e.g., it does not need any public key infrastructure or digital certificates. This paper presents a survey of the certificateless public key encryption schemes that have been proposed to improve efficiency and security. We examine the construction, infrastructure, and security models to compare published schemes and their security levels. Analyses and comparisons show that many of the different schemes are based on public key infrastructures and/or are identity based. Analyses and comparison results also show that some schemes have correct generally inclusive security concepts, while others are comparatively insecure and inefficient.

I. INTRODUCTION

The revolutionary public key or asymmetric system was proposed by Rivest, Shamir, and Adleman (called the RSA algorithm) in 1978 [1] and released in 2000. It uses two distinct separate keys, public and private, with a mathematical relationship to each other. A public key is used to encrypt the data and is widely distributed, while a private key is used to decrypt the data and is kept secret. The security is based on the assumption that no one can get one key from the other. The public and private keys are generated with attention and care to make them secure. The concept of using public and private keys ensures that a sender can securely send a message to the receiver without exchanging a shared secret key. This is possible because of using the public-private keys, instead of a single secret key. However, these systems have some drawbacks, like the need for the sender to have the correct public key to encrypt data for the receiver. Thus, a public key infrastructure (PKI) is required to manage and distribute public keys as shown in Figure 1. In such systems, a public key is bound to the respective unique user ID. Trusted third party tools are used to bind the users to unique public keys through an appropriate registration process for the users. The use of an additional third party application makes the public key cryptography expensive and inefficient. To overcome the problems and issues of PKI management systems, many ID-based cryptography systems have been proposed. In such systems, a connection is created between the user and a public key using a unique digital ID that is a combination of text characters. In this way, an ID-based system removes the PKI third party application by creating a link between the public key and digital ID for the user. However, this creates the problem of generating and managing the private keys for users. Again, the system needs a third party application for private key management to generate them secretly and distribute them to users.

To overcome the PKI and ID-based cryptography key management issues, a new certificateless public key cryptography scheme was proposed by Al-Riyami [2]. It did not need public key distribution. Certificateless public key cryptography merges the key management concepts of both the ID-based and PKI key management techniques. In this technique, to encrypt data, a user gets a public key using a secret value and partial public key. Similarly, to decrypt the data, the user gets a private key using a secret value and partial private key. The Key Generation Center (KGC) generates these partial public and private keys for the user. Thus, in a certificateless cryptography scheme, there is no need for any third party key management application like the PKI and ID-based techniques. In this case, a user can find a public key from the public directory. One time validation is needed, after which the user can change and update the public key according to his needs. The whole process is depicted in Figure 2.

This paper presents a survey of some of the known certificateless public key encryption schemes that have been published since the first proposal by Al-Riyami and Paterson. We survey the existing schemes to better determine their reality and applicability.
II. OVERVIEW OF CERTIFICATELESS PUBLIC KEY ENCRYPTION SCHEMES

The objective of a certificateless public key encryption scheme is to provide a system where users can securely share information using publicly available information. This scheme eliminates the need for the certificate used in PKI and ID-based encryption schemes. The basic infrastructure of the scheme is based on three entities: the sender, receiver, and KGC as shown in Figure 3. In the following subsection, brief descriptions of some well-known schemes are provided for a basic understanding of certificateless public key encryption schemes.

A. Al-Riyami and Paterson Certificateless public key encryption scheme

In 2003, the first formulation, basic notations, and terminologies of a certificateless public key encryption scheme were introduced by Al-Riyami and Paterson, which was constructed using elliptic curve pairings. The proposed Al-Riyami and Paterson certificateless public key encryption scheme formulation is given below:

- **Initialization setup:** The initialization and startup process is done at the KGC system. It takes the security parameter as input and generates a master private key and public key for the user.

- **Partial private key extraction:** The extraction process is also executed by the KGC system, but only once for each user. It takes the master public and private keys, with the user ID, as inputs and generates a partial private key.

- **Secret value:** The secret value setup process is executed at the user end. It takes the master public key and user ID as inputs and generates a secret value for the user.

- **Private Key:** The one time private key generation process takes the master public key and partial private key, along with the secret value of the user, as inputs to generate the private key for the user. This process is executed by the user.

- **Public Key:** The one time public key generation process takes the master public key and secret value of the user as inputs to generate a public key for the user, after which the public key is distributed to encrypt the data. This process is executed by the user.

- **Encryption:** This process uses the master public key, user ID, and public key to encrypt the message into unreadable form.

- **Decryption:** This process uses the master public key and private key to decrypt the encrypted text back to its original form.


![Figure 3. Al-Riyami and Paterson encryption scheme](image)

B. Baek, Safavi-Naini and Susilo Certificateless public key encryption scheme

In 2005, Baek, Safavi-Naini, and Susilo proposed a new and modified formulation of the scheme by Al-Riyami and Paterson with an improved architecture that did not use elliptic curve pairings [3]. This system can be seen in Figure 4. In their scheme, the receiver needs a partial private key before publishing the public key. The proposed Baek, Safavi-Naini, and Susilo certificateless public key encryption scheme formulation is given below:

- **Initialization setup:** The initialization setup process is done at the KGC system. It takes the security parameter as input and generates a master private key and public key for the users. This is the same as the Al-Riyami and Paterson setup process.

- **Partial private key extraction:** This process is also the same as the Al-Riyami and Paterson extraction process and is executed by the KGC system once for each user. It takes the master public and private keys, along with the user ID, as inputs and generates a partial private key.

- **Key Generation:** This process is different from that of Al-Riyami and Paterson. It takes the partial private key and identity of the user as inputs and generates a pair of public and private keys for users.

- **Encryption:** This process is also the same as the Al-Riyami and Paterson encryption process. It uses the master public key, user ID, and public key to encrypt the message into an unreadable form.

- **Decryption:** This process is different from the Al-Riyami and Paterson decryption process. It uses the master public key and receiver private key to decrypt the encrypted text back to its original form. It does not require the partial private key.

![Figure 4. Baek, Safavi-Naini and Susilo encryption scheme](image)
III. COMPARISONS AND ANALYSIS OF CERTIFICATELESS PUBLIC KEY ENCRYPTION SCHEMES

This section provides comparisons and an analysis survey of the existing literature about certificateless public key encryption schemes. The results of the comparative analysis survey of the certificateless public key encryption schemes are given in Table 1.

In 2003, the first certificateless public key encryption scheme was introduced by Al-Riyami and Paterson [2]-[4]. In their paper, Al-Riyami and Paterson presented the concept of concrete certificateless public key cryptography. They proposed certificateless public key encryption, signature, and key exchange schemes that were constructed using elliptic curve pairings. The scheme was proven using a fully adaptive adversarial model. In 2005, Al-Riyami and Paterson again proposed a new certificateless public key encryption scheme [5] and proved that its security and efficiency were much better than those of the original scheme. They applied techniques similar to those of Fujisaki and Okamoto [6] to prove the security of the scheme. In 2006, Libert and Quisquater [7] proved that the generic compositions of Al-Riyami and Paterson were insecure against chosen cipher text attacks in a relaxed security model. They proposed a better method to achieve a generic construction and fixed the problem by applying the certificateless Fujisaki and Okamoto transform method. In the same year, Zhang and Feng [8] proposed some fine tuning for the certificateless public key encryption scheme of Al-Riyami and Paterson and proved that the old version was insecure. Zhang and Feng also proposed a solution for the problem, but it resembled the scheme of Cheng and Comley [9] without having proven security.

In these schemes, random oracle models or weak security models were used to prove the efficiency and security. They lacked security proofs that used strong security models without random oracle models for the proposed certificateless public key encryption schemes. The first certificateless public key encryption scheme to have demonstrably secure in strong security models was proposed by Dent, Libert, and Paterson [10]. They included two generic constructions of certificateless encryption schemes and proved the security in strong security models without using random oracles models. They also included concrete constructions of Waters identity-based [11] and hierarchical identity-based encryption schemes [12]. After some time, researchers started thinking that they could merge public key and identity-based encryption techniques for better security, reliability, and efficiency in certificateless public key encryption schemes. The idea was to use a public key for encryption (as used in public key encryption) and a private key for decryption, with a combination of two private keys, one from public key encryption and the other from identity-based encryption. The concept of using both public key and identity-based encryption in certificateless public key encryption was first implemented by Al-Riyami and Paterson in [5] and by Yum and Lee in [13]-[14]. They proposed different schemes by applying different combinations of public key and identity-based encryption techniques. In the first proposal, they applied both techniques sequentially. First, the original message is encrypted using public key encryption, after which the output is again encrypted using identity-based encryption. In the second proposal, they again applied both techniques sequentially, but this time the original message was encrypted using identity-based encryption first. In the third proposal, both techniques were applied in parallel by dividing the original message into two messages.

In 2006, Libert et al. [15] and Galindo et al. [16] proved that these schemes were insecure. Libert et al. proved that the first proposal for generic compositions was insecure against chosen cipher text attacks in a relaxed security model. The second proposal was insecure in a strong security model. While, in the third proposal, the message could be decrypted using two oracle queries. Galindo et al. proved that the second proposal was insecure on a weak security model. In 2008, Dent [17] proved that these schemes have more serious issues, in which an attacker can re-encrypt the message using a public key and submit it again in a new encrypted form. In [18], Bentahar et al. proposed a different method that was similar to that of Cramer et al. [19] by extending the key encapsulation mechanisms (KEM) concept for ID-based and certificateless encryption using data encapsulation mechanisms (DEM), which results in more secure encryption schemes for weak type models. In this scheme, KEM generates symmetric key K and performs a key encapsulation operation, after which DEM encrypts a message using symmetric key K. In addition, they proposed generic constructions of ID-based and certificateless encryption based on a KEM and DEM combination, which proved secure on a random oracle model.

<table>
<thead>
<tr>
<th>Proposed</th>
<th>Construction</th>
<th>Security Analysis</th>
<th>Broken By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Al-Riyami [4]</td>
<td>Generic Construction</td>
<td>For one scheme weak type models are used but for other schemes no proof is given</td>
<td>Libert et al. [15], Galindo et al. [16] and Dent et al. [10]</td>
</tr>
<tr>
<td>Yum–Lee [13]</td>
<td>Generic Construction</td>
<td>Weak type model is used.</td>
<td>Libert et al. [15] and Galindo et al. [16]</td>
</tr>
<tr>
<td>Al-Riyami and Paterson [2]</td>
<td>Concrete Construction</td>
<td>Random Oracle Model is used</td>
<td>--</td>
</tr>
<tr>
<td>Al-Riyami and Paterson [5]</td>
<td>Concrete Construction</td>
<td>Random Oracle Model is used</td>
<td>Zhang et al. [8] and Libert et al. [15]</td>
</tr>
<tr>
<td>Back–Safavi-Naini–Susilo [3]</td>
<td>Concrete Construction</td>
<td>Random Oracle Model is used</td>
<td>--</td>
</tr>
<tr>
<td>Bentahar et al. [18]</td>
<td>Generic Construction</td>
<td>Random Oracle Model is used</td>
<td>--</td>
</tr>
<tr>
<td>Cheng–Comley [9]</td>
<td>Concrete Construction</td>
<td>Random Oracle Model is used</td>
<td>--</td>
</tr>
<tr>
<td>Libert–Quisquater [7]</td>
<td>Generic and Concrete Construction</td>
<td>Strong Type models are used</td>
<td>--</td>
</tr>
<tr>
<td>Huang–Wong [20]</td>
<td>Generic Construction</td>
<td>Weak Type models are used</td>
<td>--</td>
</tr>
<tr>
<td>Yum–Lee [14]</td>
<td>Generic Construction</td>
<td>Weak Type models are used</td>
<td>Galindo et al. [16]</td>
</tr>
</tbody>
</table>
In 2007, Huang and Wong [20] proposed a generic certificateless KEM scheme based on public key encryption ID-based KEM and message authentication code, in the standard model. They proved the security of the scheme against malicious-but-passive KGC attacks without using a random oracle model. Secondly, they proposed a certificateless tag-based KEM scheme based on the concept proposed in Abe et al. [21]. They also showed the construction of a hybrid certificateless encryption scheme by applying Abe et al.’s transformation to a certificateless tag-based KEM and one time DEM. The schemes were less efficient but comparable to the certificateless KEM scheme of Bentahar et al., in which only random oracle models were used to prove the security. In 2007, Dent et al. [22] proposed certificateless encryption schemes in the standard model and proved the secure against strong adversaries without using random oracle models. The proposed scheme was based on a combination of certificateless encryption schemes, public key encryption schemes, and the extended version of Naor et al. [23] and Sahai [24] for non-interactive zero-knowledge proofs. In [25], Hwang et al. showed that the schemes of Liu et al. [26] and Dent et al. were insecure and required random oracle models to prove their security. Then, they proposed an improved and secure scheme against a malicious KGC attack in the standard model.

CONCLUSION

This paper presented a survey of certificateless public key encryption schemes, which are advanced version of identity-based and public key encryption techniques, used to overcome and eliminate key management issues. The paper investigated the issues and problems related to the construction, infrastructure, and security models for certificateless public key encryption schemes. Comparative analyses showed that some of the proposed schemes were based on public key infrastructures, identity-based techniques, or both techniques. Some schemes have a correct generally inclusive concept of security, while others are comparatively insecure and inefficient. In the early stages of development for certificateless public key encryption schemes, mostly random oracle or weak security models were used to prove the security and efficiency. In the development of new schemes, strong security models are used and tested without using random oracle models. However, many questions remain unanswered that need to be answered relate to security, models, efficiency, and implication. Thus, we conclude that more research and development is needed in this area.

ACKNOWLEDGMENTS

I would like to thank the anonymous reviewers for their valuable comments. This work is supported by NPST Program 09-INF851-02, by King Saud University.

REFERENCES


