International Journal of Computer Networks and Applications
Volume 2, Issue 2, March – April (2015)

RESEARCH ARTICLE

Public-Key Cryptography Techniques Evaluation

Reham M. Abobeah
Systems and Computers Engineering Department,
Faculty of Engineering, Al-Azhar University, Cairo, Egypt.
eng.reham222@gmail.com

Mohamed M. Ezz
Associate professor ,Systems and Computers Engineering Department,
Faculty of Engineering, Al-Azhar University, Cairo, Egypt.
ezz.mohamed@gmail.com.

Hany M. Harb
Head of Systems and Computers Engineering ,Systems and Computers Engineering Department,
Faculty of Engineering, Al-Azhar University, Cairo, Egypt.
harbhany@yahoo.com.

Abstract – Cryptography techniques play an important role in modern world. The purpose of such techniques is to ensure the contents being unreadable to anyone except for parties who agreed to use some specific scheme. Moreover, current cryptography techniques provide more sophisticated services, such as message integrity, authentication, time stamping, and many others. There are two main approaches for cryptography: private-key cryptography and public-key cryptography (PKC). In this paper we focus on PKC techniques giving a comparison between three main techniques, namely, Public key Infrastructure (PKI), Identity- Based Cryptography (IBC) and Certificate less Public Key Cryptography (CL-PKC). In this research, a brief definition, advantages and disadvantages and analysis of main problem, namely, the revocation problem, are introduced for the three techniques. Also, a variety of available solutions to overcome the revocation problem in each technique are highlighted. Finally, some common applications and schemes for each technique are summarized.

Index Terms – Asymmetric cryptography, PKI, IBC, CL-PKC, Certificate, Key escrow, Revocation.

1. INTRODUCTION

Cryptography can be divided into two main approaches: private-key cryptography (symmetric-key) and public-key cryptography (asymmetric-key). The Symmetric-Key approach was the only type of encryption until the public-key encryption was developed in the 1970s. All traditional schemes are symmetric / private-key encryption algorithms, in which encryption and decryption are performed by a single key. In other words, one shared key is known to both sender and receiver so, encrypting and decrypting messages can be performed by that common key. Although encryption of symmetric key data is relatively easy compared to public key techniques, it has several problems including secret key agreement between different parties. The robustness of symmetric encryption depends on the length of the key used and that key needs to be securely stored and transmitted between parties. This type of cryptography does not provide a non-repudiation mechanism when used in signing the message.

On the other hand, Diffie and Hellman firstly introduced the concept of the second cryptography approach, PKC, in 1976. However, the true beginning is not considered at that time. Admiral Bobby Inman who is the director of the National Security Agency (NSA) claimed that PKC had been discovered in the mid-1960s at NSA. The first documented introduction for these concepts was introduced in 1970, by the security group of Communications-Electronics, the British counterpart to NSA, in a classified report by James Ellis. After developing PKC, a great revolution was added to the history of cryptography. There are two involved keys in PKC approach: a public-key that may be known to anyone and is used to encrypt messages and verify signatures, and a private-key that is owned only by the recipient and is used to decrypt messages and create signatures. This approach is also called asymmetric since the key that is used for encrypting messages or verifying signatures cannot be used for decrypting messages or creating signatures. In fact, the key distribution problem is shifted by PKC approach to the problem of binding the user with its key pair which is the core of PKC security. Fortunately, it is much easier to certify particular binding than to deliver the keys themselves.

PKC approach has many advantages, the primary advantage is the increased security; private keys do not need to be transmitted to anyone so, they are not vulnerable to man in the middle attack, in contrast to the secret-key system. Another major advantage for public-key systems is the ability to achieve non-repudiation cryptography service especially in

RESEARCH ARTICLE

case of digital signatures. Secret key systems authentication requires sharing the secret key and also trusting the third party. Therefore, non-repudiation cannot be guaranteed, since a sender can claim that the shared key was compromised by any one of the parties who shared the secret and hence he will be able to repudiate from the message that is previously authenticated. Authentication via Public-key systems, on the other hand, can guarantee non-repudiation, since each user, only, has the complete responsibility to protect his private key.

On the other hand, the main disadvantage of public key encryption is speed. The methods of secret-key encryption are considered faster than the available methods for Public Key Encryption (PKE). The best solution for the encryption can be achieved by combining the two cryptography approaches in order to get the advantage of both, the high security of public key systems and the high speed of secret key systems [1].

In PKC approach, the sender's private key or the receiver's public key, or both can be used by the sender according to the cryptographic function. There are three categories for using the public-key cryptosystems: encryption/decryption where the message is encrypted with the recipient's public key and decrypted with the recipient's private key, digital signature where the sender uses its private key to sign a message, and key exchange where a session key can be exchanged between two sides of communication with some type of mutual cooperation [1].

In this paper, we focus on the second type of cryptography which is the PKC (asymmetric-key) approach by introducing three public-key techniques namely, PKI, IBC, and CL-PKC. This paper is organized as it follows: Section 2, 3, and 4 highlights PKI, IBC, and CL-PKC techniques respectively, by introducing in each section a brief definition to that technique, its pros and cons, some available solutions to the revocation problem, and some available applications and schemes for that technique. Finally, section 5 compares these three techniques.

2. FIRST TECHNIQUE: PUBLIC KEY INFRASTRUCTURE (PKI)

2.1. Introduction to PKI technique

There are some reasons that lead to the concept of PKI. At first there is a need for some way to enable receiver to find sender's key (may through directory service or delivered as part of a protocol, or along with a signature), and also there is a need to enable receiver to make sure of sender's public key that is really his public key and not for anyone else. In order to bind identities with public keys, certificates are needed and since the sender may leave the company or its private key may become exposed so, there is a need for some way to show that the public key of that sender is no longer valid and cannot be trusted anymore (achieved through revocation mechanism).

PKI is a system that includes digital certificates, Certificate Authorities (CAs), and registration authorities for authenticating and verifying the validity of all entities in an online communication. PKI is able to secure the exchange of encrypted electronic data between all entities over the internet. It can be used for web browsing, email communication, online banking, or lodging tax returns. In other words PKI can be defined as a combination of software, hardware, and people policies that aim to manage digital certificates (create, issue, modify, store and remove digital certificates). The main benefit of PKI is providing a system for distributing and managing digital certificates [2] .

2.2. Some controversial aspects for PKI [3]:

2.2.1. The retrieval of Keys and Certificates is difficult

In order to enable any user to encrypt message for a specific recipient in a traditional PKI, the recipient needs to obtain a certificate and makes it available to the sender (by posting on a repository or transferring it direct). Also for off-line operations, the certificates are required to be obtained in advance in case of available connectivity. Since the large-scale directories have become not available to serve certificate publication process, the interest has directed to approaches that enable the public key encryption without satisfying these preconditions at first.

2.2.2. Additional properties are required for certified key representations

The trusted servers must be available on line and since this is impractical to depend on, certificates are designed. The goal of designing the certificate is to bind a user's public key with its identity in a protected form that could be stored on repositories that may be unprotected or transferred across unsecured channels. The retrieval of certificates requires a repository to be available, but the existence of certificates in signed representations makes it also depends on that repository for the purpose of security.

2.2.3. The Complexity in certificates processing

The integration of PKI technologies with applications that may need to use their services has become difficult since the PKI technologies require both writers and maintainers of these applications to have a specific experience in the security of PKI. For example, X.509 certificates have complex structures that require difficult processing semantics. Some complexity in the certification comes from the need to make a large set of information to be available in a certificate in order to be used in off-line processing without the need to consult other trusted entities. One of the other complex elements in PKI is the revocation mechanisms.

RESEARCH ARTICLE

2.2.4. The cost of Certificates

Certificate usage has many assumptions based on the expensive cost concept for the Certificates so they can only be issued infrequently. There are some enrollment methods that seek to provide a high confidence level for client transactions and implementations that need high-assurance. This may lead to high costs and/or cumbersome enrollment processes. Although this practice may be an important for some different types of technologies, it needs not to be an essential characteristic in using the PKI methods. As well as, in cases when PKI provides unrequired levels of administrative guarantee, certification models are just adapted instead of developing separate infrastructures types in order to bind keys, principals, and attributes.

2.2.5. Privacy is compromised in PKI

Since PKI certificates provide visible, clear and persistent links between keys and identifiers so, the traditional PKI is considered unfriendly regarding to privacy.

2.2.6. Requirement of high security and assurance at CAs

Since any misuse of CA's private key can compromise the whole community so, one of the common practices today is using a password-encrypted form in storing user keys in order to protect them properly.

2.2.7. PKI is subjected to impersonation

In PKI systems, impersonation may exist in a successful way. In other words, the successful attacking on CA will enable an adversary to choose the public-key certificate of any user from that compromised authority and binds any key from its choice to the identity of that user[1].

2.3. Revocation Problem at PKI technique

In any PKI system, private keys for users may be compromised and in order to reduce the damage that may occur, certificates that are associated with these keys should be revoked and all users must be informed in order to stop using these revoked certificates.

Some existing solutions to the revocation problem at PKI

In order to revoke certificates, CAs need to have some mechanism for distributing certificate status information to their users[4]. There are two common mechanisms: certificate revocation lists (CRLs) and on-line certificate status protocols (OCSP). A CRL is a signed data structure that contains a list of revoked certificates. CRL based systems are issuing the updated lists of CRLs regularly in order to enable users to determine the current status of certificates. In an OCSP based systems, before using the information included in any certificate, the relying users send requests to the OCSP server asking for the status of a specific certificate and the server responds with the current status of that certificate. For more details about these common solutions and other available solutions, the reader may refer to[5].

2.4. PKI Applications

PKI is a general purposes technique supported by different number of applications. The following part introduces some of common PKI applications that have been verified by the Dartmouth College's PKI Lab at Dartmouth [6].

2.4.1. Identifying the identity of servers

It is an important for the client to verify the identity of the server before establishing any important communications with it. The PKI server can send its identity certificate to the client in a secure manner by simply using the SSL handshake. This operation can occur when anyone uses HTTPS connection to communicate with the web server. The importance of this application appears in many applications like an online purchasing and banking transactions. Also, Mail servers, VPN appliances and any client server applications that depend on sockets use SSL to identify themselves to their clients.

2.4.2. Providing the required Authentication and Authorization for web applications

Server applications need to authenticate their clients before establishing any important communications with them and that may include transferring sensitive information or doing some actions regarding to their financial transactions. Before establishing HTTPS connection to the client, SSL ask the client to provide its identity certificate to make the web server be able to verify that client. Regarding to authorization, the information that is included in the client certificate is usually sufficient to be used by the application that contains authorization as a part of it. However, the application may need the help of other databases or systems to determine the client authorization.

2.4.3. Signing Forms and Electronic Documents

As mentioned earlier, in PKI technique each user has two keys and a certificate to bind its identity to the public key. Any user in the PKI technique can use its private key to provide digital signatures that cannot be repudiated on forms and electronic documents, and anyone else can verify that digital signatures using the public key of its certificate. PKI digital signatures provide a great savings on time and cost and it also improves security and reliability.

2.4.4. Authentication for VPNs

Some VPN appliances use the client certificates to authenticate users. There are some series like Cisco VPN3000 can use the information contained in that certificates to group its users and give each group its own privilege. So, besides authentication, authorization is also achieved.

RESEARCH ARTICLE

2.4.5. S/MIME Email signing and encryption

Combining PKI technique with S/MIME email provides users the ability to send and receive encrypted emails as well as verifying the identity of senders of these emails. Each user uses its private key to sign his S/MIME email messages and to decrypt the other messages sent to him, whereas the others can use the sender's public key and certificate to verify the signature and to encrypt mails before sending to others. This will prevent the sniffers from reading or modifying the mail contents during the transmission. S/MIME is candidate to be used by organizations, agencies, industries as well as by all users to secure their communications as it is very easy to use.

2.4.6. S/MIME enabled List Server

There is a problem in sending S/MIME email to a list of users as each user has a different public key so, the same email needs to be encrypted by each user's public key in that list. This problem can be solved by using S/MIME enabled list server that contains all certificates and public keys for all users. The list server allows users to easily send S/MIME encrypted mails to a list of users as it follows: the message is sent to the list server encrypted by its public key, then the server receives that message and decrypts it, and finally the server re-encrypts it using public key of each user as it sends the message to each one in the list.

2.4.7. Security in Wireless Network

802.1x standards have an option that able to solve the authentication problem in wireless networks. The option is using PKI technique in the authentication process of users to the wireless network and also to encrypt their data using WPA.

2.4.8. Secure Instant Messaging

AIM is an instant messaging application that was introduced by America Online inc. (AOL) in 1997. It was combined, recently, with PKI capabilities in order to secure the messages and enable its users to authenticate persons in other side of the conversation. PKI provides AIM the option to sign and encrypt its messages and also to authenticate the identity of users before the conversation.

2.5. Some common PKI algorithms

There are many available PKI algorithms, some of them are succeeded to achieve encryption/decryption, digital signature and key exchange applications whereas others can achieve only one or two of them [1]. For example, RSA and Elliptic Curve algorithms can be used in all these applications whereas Diffie-Hellman algorithm can be used only in key exchange application and DSS can be used in digital signature application only.

3. SECOND TECHNIQUE: IDENTITY-BASED CRYPTOGRAPHY (IBC)

3.1. Introduction to IBC technique

In PKI technique and before communications take place, each one must generate encryption and signature key pairs, submit to a Certificate Authority (CA) certificate requests along with proof of identity, and receive certificates that are signed by CA. The certificate can be used by anyone to authenticate one another and exchange encrypted messages. This process can be time-consuming and prone to error, and is especially prohibitive for novice computer users. IBC technique seeks to reduce these impediments by requiring no preparation on the message recipient part. It's worthy to mention that IBC technique provides some advantages over PKI-based approaches without its drawbacks[7].

In 1984, Adi Shamir has introduced the concept of IBC technique. In this model, user's identifier such as phone number, email or IP address is used as a public key that is needed for encryption or signature verification. As a result, this feature reduces complexity of cryptography system by eliminating the need for generating and managing users' certificates. Also, the interaction with unprepared users without the need to communicate with any system components becomes much easier. Regarding to the user's private key, the user needs to authenticate himself to a trusted third party called private key generator (PKG) and after the successful authentication, PKG derives the private key from PKG's master key and user's identity and sends it ,later, to the user over a secure channel [8]. After receiving the private key, the user will be able to sign any message before sending it or decrypt any message sent to him encrypted by his identity. It is worthy to mention that PKG, in IBC technique, is responsible for generating private keys of all users using its master key so, it can easily sign and decrypt all users' messages. At the time when Shamir published the IBC proposal, he introduced an identity-based signature (IBS) scheme based on the RSA function, but he was unable to construct an identity-based encryption (IBE) scheme. IBE scheme was an open problem until 2001 when two independent lines of research (Boneh and Franklin, as well as Cocks) solved that problem and introduced two independent IBE schemes. Since that time, IBC technique has become one of important research topics in the field of cryptography. In addition to academic research, there are also available some commercial product offerings, especially, that are introduced by Voltage Security inc [9].

It is also worthy to mention that Voltage Security is the main commercial player in the field of IBE. It uses IBE as the encryption standard to offer products in order to secure disks and email and provides key management systems. Voltage Security was appeared in 2002 in California and has customers in several industries including Kodak, ING Canada

RESEARCH ARTICLE

and Domino's Pizza. Dan Boneh, who is the co-author of the first practical implementation of IBE, is the co-founded of the Voltage Security.

3.2. Pros and Cons of IBC technique

3.2.1. Some Points that are considered as advantages of IBC [7]:

- There is no need for managing certificates and other PKI components, especially the management of CRL.
- There is no need for any preparations on the part of the recipient to receive an encrypted message.
- Less public information about your enterprise is known by those who do not have a need to know, unlike PKI technique as a great deal of information about your company's infrastructure can be known by each application or person when connecting to an enterprise's certificate database.
- IBC inherent a key escrow feature meaning that PKG knows private keys of all users and it can easily decrypt and sign users' messages easily. Although, this feature is considered as a disadvantage (especially in IBS since in most cases non-repudiation is eliminated), it sometimes enables some other features that are not possible in PKI-based systems where no one can use the private key of each user in signing other than its owner. Some advantages of key escrow feature are:
- Many organizations consider a key escrow feature is an important in order to be able to recover a user's encrypted data in case when its private key is lost.
- This property also can be useful in case when user's privacy is limited, for example, when the user is involved in the crime, its messages should be opened by a court order.
- The designated recipient only in "Chameleon" signatures is able to assert the validity of the signature[10].
- PKG in this model can handle some of cryptographic operations for the user with no client-side installation is required. For example, in case where a company wants to apply a policy whereby all messages of a certain level of sensitivity are automatically encrypted and/or signed. An administrator just needs to specify the policies that are needed to determine the messages that will be signed or encrypted using tools like a keyword search in content of the message content, a regular expression match on the sender or receiver, or a time range with no need for modifying the behavior of email users.

3.2.2. Some points that are considered as disadvantages of IBC [11]:

- Key escrow property that is inherent in all IBC systems since PKG knows the private keys of all users in the system. As it is mentioned earlier, this feature may be considered as an advantage in some cases, so IBC adopters may need to decide whether they need this feature or not.
- Establishing a secure channel between each user and his PKG in order to deliver each private key to the correct user securely.
- IBC technique cannot provide a true non-repudiation since PKG could forge the signature of any user.PKG requires a higher level of assurance and availability than is required for CA in PKI technique as it holds the private keys of all users in IBC system.
- PKG must be available (online) to provide users with their private keys and this may increase its vulnerability to attack whereas CA may be disconnected (offline) from the network, so extra care is required to secure PKG s.
- Compromising the master-key of PKG could be more severe than compromising of CA's private key in conventional PKI.
- In IBC systems, each user needs to authenticate himself to its PKG for obtaining the private key in the same way as when he authenticates himself to CA for obtaining the certificate in PKI technique.
- The use of IBC technique may be restricted to closed, small groups or to applications with limited security requirements for the previous reasons.

It is also worthy to mention that the practical difference between IBC and most PKI systems is that PKI systems can provide un-repudiated digital signature schemes as key escrow feature isn't included in it. However, PKI systems also don't provide a perfect level of non-repudiation as CA is always reported by the compromised key after a time frame. On the other hand, IBC systems can achieve some level of non-repudiation that is always related to the level of trust at PKG, it should not exploit its knowledge of private keys for all users to sign messages or it can sign messages only in case of user's request.

3.3. Revocation Problem at IBC technique

As PKI technique, the identity-based scheme must provide a means to revoke users from the system. IBC technique needs only the PKG's public key and the recipient's identity for encryption, so there is no way to notify senders that a specific identity was revoked.

Some existing solutions to the revocation problem at IBC

1) Boneh and Franklin suggested that users can periodically obtain new private keys in IBC systems. In other words, the user should attach a time period to the string that represents its public key in IBE schemes and send to PKG to obtain the private key that will be valid only during that period and the user should connect again to PKG in order to obtain a new private key for a new period and so on. For example, Bob (receiver) publishes bob@secworld.com||June, 2015 as his public key and so the private key associated with that identity

RESEARCH ARTICLE

will be valid only during June, 2015. In order to revoke a specific user in the identity based system, the PKG is ordered to stop issuing new keys for the identity of that user or according to the example, PKG is instructed to stop issuing new private keys for Bob's e-mail address and as a result, Bob becomes unable to read his email messages [12]. Unfortunately, this solution makes all users to regularly communicate with PKG, authenticate themselves to it and obtain new private keys regardless of whether their keys have been exposed or not. For all these transactions, PKG must be online and also a secure channel between PKG and each user must be established in order to securely deliver the private key to its user. As a result, this may become a bottleneck in systems with large number of users.

2) Alternatively, in order to avoid the need for secure channels and regularly interactions with PKG, it is introduced another solution such that PKG can encrypt the new keys of non-revoked users using their identities and the previous time period, then sends the ciphertexts to these users or can post on line. In this approach, for every key update it is required one key generation and one encryption operation to be performed by PKG for every non-revoked user in the system. This solution is like the previous one since the work required from PKG is linearly increased with the number of users, so it may be unable to scale well when the number of users increase [13].

3) It is also introduced a method to renew the private keys of users periodically without interacting with PKG. In this method, PKG posts key update information publicly which is considered as a more convenient. This solution can be considered cumbersome since each user needs to own a tamper-resistant hardware device [13].

4) There are also available researches for revocation in ID-based system with mediators in both[14], [15]. This solution suggests that there is a special semi-trusted third party called a mediator who has a part of each user's private key so it should help each user to decrypt any ciphertext. The mediator is instructed to stop helping the user when its identity is revoked.

5) Recently, it is introduced a suggestion that is provided by Boldyreva, Goyal and Kumar (BGK) [16]. This technique improved Boneh and Franklin technique and also reduced the amount of work that PKG has to do for key updates to become logarithmic instead of being linear in the number of users as well as keeping the scheme to be efficient for senders and receivers. Their revocable IBE primitive (R-IBE) scheme was built on a binary tree data structure and the idea of Fuzzy Identity-Based Encryption (FIBE) schemes. Unfortunately, the security of R-IBE scheme is proved only in the relaxed selective-ID model wherein adversaries must choose the target identity at the beginning of the attack game since the current FIBE systems are only secure in the selective-ID model. This limitation is left as an open problem although it may reduce the using of this approach.

6) An adaptive-ID secure revocable IBE scheme is introduced, after that, in order to solve the problem that is left open by BGK. The scheme is similar to the efficient revocation mechanism that is introduced in the BGK system while achieving the same security that is defined by Boneh and Franklin where the target identity is chosen by adversaries in the challenge phase [17].

Finally, it is worthy to mention that the solution proposed by Boneh and Franklin [12] remains the most practical user revocation solution in the IBE setting.

3.4. IBC Applications

There are many IBE applications , for example that are introduced in [[12],[18]]:

- Time-based entity revocation. In this application, public key (identity) is concatenated with a specific time period and then send to PKG which produces private key that is valid only during that period and hence the entity is revoked after the aforementioned time period is elapsed.
- Management of user credentials. In this application which is considered an extension to the previous one, messages are encrypted using the public key that is concatenated with a time period and a clearance level such that a receiver will only be able to decrypt the message if on the specified time period he has the appropriate clearance level so, it is very easy to PKG to grant or revoke the credentials of the user.
- Delegations of duties. In this application messages are encrypted using the subject line as the IBE encryption key and the management provides its employees with private keys that are related to their responsibilities such that each employee will be able to decrypt only messages whose subject line falls within its responsibility and he cannot decrypt messages intended for others.
- Using IBE in Email Security. In this application Voltage security Corporation provides a White Paper which shows that IBE introduces a high performance than it is provided by using its counterparts from symmetric and asymmetric key management.
- Using IBE for exchanging sensitive information with no need for downloading any software as it is explained in a white paper that is provided by Voltage security Corporation. It shows that how IBE can be used in order to secure communications through financial services.
- Using IBE for securing Wireless Sensor Networks (WSNs) as well as using it for solving the problem of key distribution in WSNs.

RESEARCH ARTICLE

3.5. Some IBC Schemes

As mentioned earlier, IBE scheme is still an open problem until 2001 when it was independently solved by Boneh and Franklin, and Cocks. They provided two ways through which any IBE scheme can be implemented. Regarding to Boneh and Franklin scheme [12], it presented IBE scheme that based on bilinear maps between groups and used the Weil pairing on elliptic curves as an example of such maps. On the other hand, Cocks used a variant of integer factorization problem to construct his IBE scheme that its security is based on the hardness of the quadratic residuosity problem[19]. This scheme is inefficient since the message is encrypted bit-by-bit and hence the length of the ciphertext becomes long, while it can be suitable for small data packets like a session key.

As an extension to the IBE scheme, the Hierarchical IBE scheme (HIBE) is introduced in[20]. This scheme is provided to solve the problem of heavy workloads on a single PKG in IBE scheme. It suggested that instead of using a single PKG in the system, there is a hierarchy of PKGs such that the PKGs compute private keys to the entities below them only in the hierarchy and hence the users are no longer identified by a single identity, but they will be identified by the identity of each of their ancestors in the hierarchy.

Another extension to the IBE scheme is adding a threshold decryption feature to it [21]. The receiver communicates with the KGC and obtains the private key that related to his identity. He can distribute that key into a number of decryption servers, and after he receives the ciphertext, he forwards to each of the decryption servers to get a decryption share. The receiver will be able to recover the whole plaintext if the number of decryption shares that the receiver holds reaches some threshold.

Regarding to IBS scheme extensions, there are available identity-based blind signature and ring signature schemes[22]. The blind signature is needed in electronic commerce applications and it helps the signer to create a valid signature on a message without seeing it. A ring signature scheme makes the verifier unable to know exactly who signed the message although he may know that one of specific group members signed it. In other words, this scheme provides some of the ambiguity to the signer.

Also there are identity- based signcryption schemes which provide at the same time the property of IBE and IBS, for example the scheme provided at [23]. And as an extension to this work, ID-based Broadcast Signcryption (IBBSC) scheme that enables the broadcaster to sign and encrypt messages before sending to a specific group of users in one logical step, introducing a good solution to the problem of authentication and confidentiality. It is claimed in this paper that ID-based schemes is the best alternative to any broadcast signcryption schemes for wireless content distribution in mobile and portable devices such as cell phones and PDAs for example [24].

4. THIRD TECHNIQUE: CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY (CL-PKC)

4.1. Introduction to CL-PKC technique

In traditional PKI, public key is randomly generated and does not bind to user identity, so it suffers from man-in-the-middle attack. In order to solve this problem, it is required to have a CA third party that binds public key to user's identity and issues a certificate signed by CA's private key for authenticity of user's public key. The disadvantage of this technique is the increasing cost for managing and distributing certificates when the numbers of users increase.

IBC was firstly proposed by Shamir in order to solve the issues of traditional PKI. The public key is an arbitrary string that represents the identity of an entity such as IP address of a network host or an email address of a user. User's private key is generated by PKG using user's identity and PKG's master key. This approach suffers from key-escrow problem because PKG has the information of every user's private key (i.e. decryption and signature can also take place on the server).

In 2003, Al-Riyami and Paterson introduced the concept of CL-PKC technique in order to eliminate the key escrow problem inherent in IBC technique without introducing certificates [25]. CL-PKC technique uses a trusted third party that is called key generating centre (KGC). In contrast to PKG in IBC technique, KGC does not have access to entities' private keys since there are two parts of user's private key that are partial private key and secret value. The Partial private key is generated by KGC using user's identity and KGC's master key while the secret value is generated by the user and it is known only to him. KGC must ensure that the partial private keys are delivered securely to the correct entities. The user then generates the full private key by combining its secret value with the partial private key that he received from KGC and therefore user's private key is not available to KGC. As well as he combines KGC's public parameters with the same secret value in order to generate its public key. After that, user's public key should be available to other users either by placing in a public directory or by sending with messages especially in signing applications. Both public key and user's identity are used to encrypt messages or verify signatures. The use of identity in encryption prevents any other party from decrypting the content even if anyone tries to forge the part of public key. It is noted that CL-PKC system is not identity-based since the public key is no longer computable from an identity (or identifier) alone. Also, the infrastructure needed to support CL-PKC is lightweight when compared to a traditional PKI as there is no need to manage certificates.

RESEARCH ARTICLE

4.2. Pros and Cons of CL-PKC technique

4.2.1. Points that are considered as advantages of CL-PKC:

- CL-PKC is an intermediate model between traditional PKI and IBC. It does not require the use of certificates like PKI and doesn't have the built-in key escrow feature of IBC.
- In contrast to PKG in IBC, KGC in CL-PKC does not have access to entities' private keys. Instead, KGC supplies the entity with a partial private key that is generated from the identifier of that entity and KGC's master key and the entity generates the full private key through combining its secure value with the partial private key from KGC.
- User needs not to have private key before generating public key although both of them need the same user's secret information to produce each of them.
- Compared to IBC, the trust assumptions that are needed for the trusted third party in CL-PKC are much reduced. In IBC, users must trust the PKG not to abuse its knowledge of private keys in performing passive attacks, while in CL-PKC users need only to trust the KGC not to propagate false public keys.
- Any adversary does not know the partial private key of any user, so he will be unable to calculate the full private key of any one. If an adversary tries to replace the public key of any entity by a false key of its choice, he will gain nothing useful without having the correct private key that requires the partial private key and therefore the cooperation with the KGC. As a result, an adversary will not be able to decrypt ciphertexts encrypted under the false public key, or produce signatures that are verified with that false key.
- In contrast to PKI, certificateless scheme does not require expensive infrastructure composed of different kind of authorities, it requires only KGC and Public Parameters Server like that at IBC.

4.2.2. Points that are considered as disadvantages of CL-PKC:

- CL-PKC is not purely identity-based since the public key is no longer computable from an identity (or identifier) alone and both Identifier and public key are required for the encryption.
- As in IBC technique, secure channels are required for delivery of partial private keys to their correct users.
- CL-PKC does not achieve the same security level of traditional PKI since KGC may cheat.

In other words and according to the trust model at [26], CL-PKC schemes achieve trust level 2, whereas traditional PKI reaches to trust level 3. The reason is, when a CA tries to forge a certificate in PKI, it can be identified by the existence of two working certificates for the same user whereas the KGC in CL-PKC will be able to replace public keys of entities without realizing that these keys are invalid.

In order to achieve the trust level 3 for CL-PKC and also strengthen the security against a malicious KGC, CL-PKC introduces an alternative key generation technique that binds the user identifier to its public key. Thus, the corresponding private key for that user will be bound to the public key and if the KGC replaces a public key it will be noticed easily. The existence of two different working public keys for the same identity will identify the KGC as having misbehaved in issuing both corresponding partial private keys. This technique suffers from one drawback that is the public key of the user must be generated before issuing the partial private key by the KGC[25].

4.3. Revocation Problem at CL-PKC technique

As PKI and IBC techniques, the CL-PKC technique also should have an efficient revocation mechanism since private keys may be compromised and become no longer secure for their owners.

Some existing solutions to the revocation problem

1) One solution to the revocation problem in CL-PKC systems is handling that problem in the same way as in Boneh-Franklin IBE systems [12]. In other words, this method is based on attaching a time period to the user's identifier and sending to KGC. After that, KGC authenticates the identity of that user and produces its partial private key that will be valid to use only during that period. This method ensures a limited life for any user's partial private key as well as the full private key. However, this method introduces some disadvantage such that it requires an expensive secret channel between the KGC and each user over which all the newly produced partial private keys are transmitted as well as users need to regularly communicate with KGC for obtaining new partial private keys regardless of whether their keys have been exposed or not, this method is introduced at [27].

2) Another solution to the revocation problem in CLPKC is introduced in mediated certificateless public key encryption (mCL-PKE) scheme [27]. This scheme employs an on-line mediator called SEM (Security Mediator) and it uses two private keys, the first private key is issued by KGC and the second one is issued by the user to remove a key escrow property and in order to generate the corresponding pubic key. In this mechanism, the user's partial private key that is generated by KGC is divided into two pieces, one is delivered to the user while the other is passed to the SEM so, the operations that need the existing of private key such as decrypting or signing the message will need the cooperation between both user and a SEM in order to get the full partial private key. This approach can support instantaneous revocation by instructing the SEM to stop interacting the user. Disadvantages of this solution are: the need for confidential

RESEARCH ARTICLE

channels for all these communications and SEM has to keep large numbers of secret keys which provides more opportunities for attackers to compromise.

3) There are also new and practical approach to the revocation problem in CLPKC that is introduced in [28]. In this approach, KGC generates for each user an initial partial private key that is based on its identity information as well as a time key for each time period. In other words, the full user's private key, in this approach, is made up of three parts: an initial partial private key, a time key and a secret value that is generated by the user. The time key is updated by KGC in every time period and then transmitted to the user over a public channel without any changing in the initial partial private key. In order to revoke a user, KGC just stops issuing new time keys for that user and without a time key the user becomes unable to perform decryption or signing operations. In this approach, there is no secret channel for key update and no mediator, so this scheme is more efficient than previous solutions.

4.4. CL-PKC Applications

CL-PKC is a good choice for low-bandwidth and low-power situations for example in mobile computation scenarios[25] as the infrastructure that is needed to support CL-PKC technique is lightweight when compared to a traditional PKI since there is no need to manage certificates as in IBC technique. In other words and since CL-PKC scheme uses relatively short public and private keys, it is suitable for using in devices with limited resources for instance , mobile phones [29].

Using CL-PKC scheme in decreasing the certificate size and providing a lightweight PKI since the time when a number of signature schemes have succeeded to introduce a very short signatures [25].

Introducing certificateless public key signature schemes (CL-PKS) that can achieve a true non-repudiation since the full private keys are known only to their owners. The first CL-PKS scheme is introduced at [25].

Introducing an email encryption system using certificateless public key encryption scheme (CL-PKE) in [30].

CL-PKE is also considered as an extension of the IBE scheme [12] and according to that it can be applicable to most IBE applications. It is mentioned below some examples of these applications and for more details and other certificateless applications, the reader can refer to [29].

Time-based entity revocation. Like that in IBE schemes, this idea can also be employed in CL-PKE schemes. In this application, public key (identity) is concatenated with a specific time period (expiration date), then send to KGC which issues the partial private key that is based on user's identity coupled with that expiration date. This will enforce the user to refresh his private key every time when time period expired by obtaining the corresponding partial private key, otherwise he will lose his ability to decrypt cipher texts or signing any message.

Management of user credentials and Delegations of duties are the same as ideas that are introduced before in IBE technique.

Cryptographic Work Flows: In this application, the sender can encrypt the message using receiver's public key and its identity coupled with an identifier that the receiver can acquire only after accomplishing some task. This will force the receiver to complete the task, at first, to gain access to that identifier which he can then use to authenticate himself to the KGC to obtain the valid partial private key in order to decrypt the message received.

4.5. Some available CL-PKC Schemes

There are many available CL-PKC schemes, it is introduced in this section some examples for them. There are two available CL-PKE schemes based on pairings: BasicCL-PKE scheme and FullCL-PKE scheme in [25]. Most constructions of CL-PKE schemes are based on using bilinear pairings although pairing is considered as the most expensive operation among other mathematical operations such as addition, multiplication, exponentiation, multiplicative inverse and so on. BasicCL-PKE scheme is defined using seven algorithms and FullCL-PKE scheme is obtained after adding chosen ciphertext security to BasicCL-PKE scheme. A FullCL-PKE scheme is also defined using the same seven algorithms like BasicCL-PKE, but with some modifications in some algorithms that responsible for achieving the chosen ciphertext security.

The encryption scheme can be modified to use biometrics of the user coupled with secrets stored in the mobile devices to encrypt and decrypt messages [29]. This scheme achieves a two-factor authentication that provides a required security for the user since in other encryption schemes the encrypted message and the key needed to decrypt it are stored in the same device and compromising of that device makes it is very easy for the attacker to decrypt the message and destroy all the privacy. By using a two-factor authentication procedure, the user would ensure that the adversary cannot decrypt the messages stored in the device even he has the contents of the device.

Regarding to CL-PKS schemes, it is introduced the first signature scheme in [25]. After that, there are several CL-PKS schemes are introduced recently trying to improve the construction and security of available certificateless signature schemes.

RESEARCH ARTICLE

Public Key Technique	Public/Private key (PU/PR)	Trusted Third Party (TTP)	Certificate	Key escrow problem	Non repudiation	Encryption operation needs	Trust level [26]	TTP assumptions
PKI	PU key is randomly generated and doesn't depend on user's identity (ID). Key pair generation method is different according to the protocol used (ex. RSA, Elliptic curve)	CA	Certificate is needed for each user to bind (ID+PU).	Not exist	can be achieved properly (guaranteed)	Sender should know Receiver's PU and its certificate.	It achieves trust level 3	CA should be trusted not to issue false certificates
IBC	PU: is derived directly from user's ID. PR: is generated by PKG based on PKG's master key and user's ID	PKG	No need for certificate.	Exists (both user and PKG know user's PR)	can't be guaranteed (key escrow problem)	Sender should know Receiver's ID only.	It achieves trust level 1	PKG should be trusted not to use user's PR keys to perform passive attacks
CL-PKC	PU: is derived using user's secret value and KGC's public parameters. User's secret value depends on user's ID and KGC's public parameters. PR: is derived using two parts, secret value from user and partial private key from KGC.	KGC	No need for certificate	Not exist	can be achieved properly (guaranteed)	Sender should know Receiver's PU and its ID.	It achieves trust level 2 and can enhanced to achieve trust level 3	KGC should be trusted not to perform active attacks by replacing public keys with false ones.

Table 1 Comparison between PKI, IBC, AND CL-PKC Techniques

RESEARCH ARTICLE

As an extension to CL-PKS works, for example it is proposed a CL-PKS scheme with fast batch verification [31]which enables a verifier to verify a set of signatures more efficiently than verifying them one by one. This scheme also satisfies Girault's Level-3 security the same security level as in traditional PKI systems while almost of the existing batch verification signatures schemes reach to Girault's Level-1 or Level-2 security only. It is also introduced a Certificateless Partially Blind Signature scheme that is applicable in many applications such as e-cash and e-voting systems as well as it overcome the key escrow problem that is introduced in identity based partially blind signatures [32].

There are also available schemes that can be used in different applications such as the Broadcast signcryption scheme that is introduced in [33]. This scheme enables the broadcaster to sign and encrypt messages before sending to a specific group of users in one logical step, introducing a good solution to the problem of authentication and confidentiality. This scheme is also compared to previous broadcast signcryption schemes and is considered more convenient for devices that have low computational capabilities in any broadcast system.

Finally, there are other certificateless cryptographic primitives and protocols that are available like: Hierarchical schemes, Signcryption schemes, Key Exchange (KE) and Authenticated-Key Exchange (AKE) protocol.

5. CONCLUSION

In this paper, a brief definition, advantages and disadvantages and analysis of the revocation problem were introduced for three of PKC techniques, namely, PKI, IBC, and CL-PKC. Moreover, a variety of available solutions to overcome the revocation problem in each technique are highlighted and some common applications and schemes for each technique are also summarized. Finally, the paper introduced a comparison between these techniques, and it was concluded that CL-PKC technique can be considered as the best choice for using in all current and upcoming applications, as it is an intermediate model between traditional PKI and IBC techniques. The technique achieved the same security level of PKI without requiring certificates that need an exhausting management and it also overcome the key escrow problem inherent in IBC technique that may lead to some security problems in identity based systems, especially in signature schemes.

REFRENCES

[1] W.Stallings, Cryptography and Network Security, 4/E. Pearson Education India, 2006.
[2] A. Jancic and M. J. Warren, "PKI-Advantages and Obstacles.," in AISM, 2004, pp. 104–114.
[3] J. Linn, "An examination of asserted PKI issues and proposed alternatives," 2004.
[4] D. A. Cooper, "A closer look at revocation and key compromise in public key infrastructures," in Proceedings of the 21st National Information Systems Security Conference, 1998, pp. 555–565.
[5] O. Kessler and O. S. Ag, "The Certificate Revocation Framework," no. March, 2000.
[6] "Applications Enabled by PKI." [Online]. Available: http://www.dartmouth.edu/~deploypki/materials/modules/applications/appsmenu.htm#_Toc49051841. [Accessed: 09-Jan-2015].
[7] C. Youngblood, "An Introduction to Identity-Based Cryptography," CSEP 590TU, 2005.
[8] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, "A survey of identity-based cryptography," in Proc. of Australian Unix Users Group Annual Conference, 2004, pp. 95–102.
[9] "voltage security site." [Online]. Available: http://www.voltage.com/. [Accessed: 09-Jan-2015].
[10] G. Ateniese and B. de Medeiros, "Identity-based chameleon hash and applications," in Financial Cryptography, 2004, pp. 164–180.
[11] A. Mariš, "Survey of cryptographic pairing schemes," 2012.
[12] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.
[13] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, Identity-Based hierarchical strongly key-insulated encryption and its application, vol. 3788. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 495–514.
[14] C.-M. Boneh, Dan and Ding, Xuhua and Tsudik, Gene and Wong, "A Method for Fast Revocation of Public Key Certificates and Security Capabilities.," 2001.
[15] B. Libert and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in Proceedings of the twenty-second annual symposium on Principles of distributed computing - PODC '03, 2003, pp. 163–171.
[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security, 2008, pp. 417–426.
[17] D. Vergnaud, "Adaptive-ID Secure Revocable Identity-Based Encryption," pp. 1–13, 2007.
[18] Vertoda, "An Overview of Identity Based Encryption," White Pap., pp. 1–29, 2009.
[19] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, Springer, 2001, pp. 360–363.
[20] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in Advances in Cryptology—EUROCRYPT 2002, 2002, pp. 466–481.
[21] J. Baek and Y. Zheng, "Identity-based threshold decryption," in Public Key Cryptography--PKC 2004, Springer, 2004, pp. 262–276.
[22] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in Advances in cryptology—ASIACRYPT 2002, Springer, 2002, pp. 533–547.
[23] X. Boyen, "Multipurpose identity-based signcryption," in Advances in Cryptology-CRYPTO 2003, Springer, 2003, pp. 383–399.
[24] S. S. D. Selvi, S. S. Vivek, R. Gopalakrishnan, N. N. Karuturi, and C. P. Rangan, "Provably Secure ID-Based Broadcast Signcryption (IBBSC) Scheme.," IACR Cryptol. ePrint Arch., vol. 2008, p. 225, 2008.
[25] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Advances in Cryptology-ASIACRYPT 2003, Springer, 2003, pp. 452–473.
[26] T. K. Mandt, "Certificateless Authenticated Two-Party Key Agreement Protocols, Master's Thesis," 2006.
[27] H. S. Ju, D. Y. Kim, D. H. Lee, J. Lim, and K. Chun, "Efficient Revocation of Security Capability in Certificateless Public Key Cryptography," pp. 453–459, 2005.
[28] Y. Sun, F. Zhang, and L. Shen, "A Revocable Certificateless Signature Scheme," J. Comput., vol. 9, no. 8, pp. 1843–1850, Aug. 2014.
[29] K. Sharad, "Certificateless Encryption Scheme Using Biometric Identity, Master's Thesis," 2012.
[30] Y. Er, W. Yau, S. Tan, and B. Goi, "Email Encryption System Using Certificateless Public Key Encryption Scheme," pp. 179–186, 2012.

RESEARCH ARTICLE

[31] C.-I. Fan, P.-H. Ho, J.-J. Huang, and Y.-F. Tseng, "Secure Certificateless Signature Scheme Supporting Batch Verification.," in AsiaJCIS, 2013, pp. 8–11.
[32] J. Liu, Z. Zhang, R. Sun, and K. S. Kwak, "Certificateless Partially Blind Signature," in Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, 2012, pp. 128–133.
[33] M. Luo, C. Zou, and J. Xu, "Certificateless Broadcast Signcryption with Forward Secrecy," in Computational Intelligence and Security (CIS), 2011 Seventh International Conference on, 2011, pp. 910–914.

Authors

Reham M. Abobeah is a teaching assistant of software engineering, Computer and System Engineering Department, Faculty of Engineering, Al-Azhar University at Cairo. She received his B.Sc degree in electrical engineering from Al-Azhar University in 2011. Her fields of interest include network security, artificial intelligence, machine learning, data mining and operating systems.

Mohamed M. Ezz is a lecturer of software engineering, Computer and System Engineering Department, Faculty of Engineering, Al-Azhar University at Cairo. He received his B.Sc., M.Sc. and Ph.D. degrees in electrical engineering degrees in electrical engineering from Al-Azhar University. His fields of interest include network security, and cryptography.

Hany M. Harb is the professor of software engineering, and head of Computer and System Engineering Department, Faculty of Engineering, Al-Azhar University at Cairo. He received his B.Sc. degree in Computers and Control Engineering from Faculty of Engineering, Ain Shams University, Cairo, Egypt, 1978. He received his M.Sc. in Computers and systems Engineering, Faculty of Engineering, Azhar University, Cairo, Egypt, 1981. He also received M.Sc. degree in Operations Research (MSOR) and Ph.D. degree in Computer Science from Institute of Technology (IIT), Chicago, Illinois, USA in 1987 and 1986 respectively. His fields of interest include artificial intelligence, cloud computing, and distributed systems.