About the Key Escrow Properties of Identity Based Encryption Schemes

Ruxandra OLIMID
Department of Computer Science
University of Bucharest
ROMANIA
ruxandra.olimid@fmi.unibuc.ro

Abstract: IBE (Identity Based Encryption) represents a type of public key encryption that allows a party to encrypt a message using the recipient's identity as public key. The private keys needed for decryption are generated and distributed to each party by a KGC (Key Generation Center). The existence of such an entity in an IBE scheme allows access to the encrypted information for other parties other than the intended recipient by construction: the KGC or any other entity that receives the cryptographic keys from the KGC may perform decryption. A system that permits other parties to have access to the private keys of the users is said to have key escrow abilities. The paper performs a brief analysis of the key escrow properties of IBE schemes and gives a practical example of communication protocol that improves the key escrow capabilities.

Key-Words: Identity Based Encryption, Key Escrow, Lawful Interception

1. Introduction

In a key escrow system, the cryptographic keys are entrusted to a third party (kept in escrow). The benefits of such a system include backup of keys and recovery in case of disaster, delegation of duties, communication monitoring. Of course, in an improperly defined or used system, confidentiality may be lost. Key escrow must satisfy certain condition that diminishes the usage of such abilities in a malicious or unauthorized way. We examine the key escrow properties of IBE (Identity Based Encryption) schemes, a special class of public key schemes that uses the recipient’s identity as public key. The paper is organized as follows: in Section 2 we define IBE and key escrow systems. Section 3 analyzes if the general IBE scheme satisfies the main properties of key escrow. Section 4 gives a more practical example: the usage of Waters IBE [11] system in Han et al. [8] communication protocol [9]. We also analyze how the key escrow properties are improved under this approach. Finally, we conclude in Section 5.

2. Preliminary Notions

This section introduces the preliminary notions: identity based encryption and key escrow.

2.1. Identity Based Encryption

Shamir introduced the concept of IBE in 1984 [10]. More than 15 years later, Boneh and Franklin defined the first secure (in random oracle model) and efficient scheme [5]. In 2003, Canetti et al. proposed a scheme that was proved secure in a weaker security model (the Selective-ID Model) than standard [6]. In 2004, Boneh and Boyen described a scheme that was proved to be fully secure (without the necessity of the random oracle model) [3]. In 2005,
Waters described the first efficient and fully secured IBE [11]. We will use Waters IBE as a part of Han et al. protocol in Section 4.

Gentry and Silverberg extended the IBE notion to hierarchical IBE by in 2002 [7]. Improved constructions were published in the literature in the following years. Some examples include [2], [4]. However, the hierarchical IBE are outside the scope of this paper.

**Definition 1:** *Identity Based Encryption (IBE)* is a type of public key encryption that allows for a party to encrypt a message using the recipient’s identity as public key.

A general method for constructing IBE was given by Bohen and Franklin [5] and consists of 4 steps:

- **Setup** - generates the global parameters and the master key.
  
  Let $k$ be the security parameter, $\mathcal{M}$ the space of plaintext and $\mathcal{C}$ the space of ciphertexts. Then:
  
  $k \rightarrow (\mathcal{M}, \mathcal{C}, \text{params}, \text{master-key})$

- **Key Generation (or Extract)** - uses the master key to generate the users private keys. Each user is unique identified by his identity ID and $d$ is a private key that correspond to the identity ID:
  
  $(\text{params}, \text{master-key}, \text{ID}) \rightarrow d$

  - **Encryption** – a plaintext $M$ is encrypted using the identity of the receiver as public key:
    
    $(M \in \mathcal{M}, \text{params}, \text{ID}) \rightarrow C \in \mathcal{C}$

  - **Decryption** – a ciphertext $C$ is decrypted by the receiver using his private key:
    
    $(C \in \mathcal{C}, \text{params}, \text{ID}, d) \rightarrow M \in \mathcal{M}$

  The scheme must satisfy the consistency constraint:

  $\forall M \in \mathcal{M}: \text{Decrypt}(C, \text{params}, \text{ID}, d) = M$, where $C = \text{Encrypt}(\text{params}, \text{ID}, M)$

A schematic representation of the IBE model is given in Figure 1:

1. The users receive the general parameters from the KGC;
2. A encrypts the message sent to B using B’s identity as public key (his e-mail address for example);
3. B must authenticate to KGC in order to receive his corresponding private key;
4. B receives his private key and is able to perform decryption.

We highlight the fact that B has to authenticate to KGC only once in order to
receive the private key, no matter the number of messages he receives.

2.2. Key Escrow

Definition 2: A key escrow system is a system in which the cryptographic keys are entrusted to a third party (i.e. kept in escrow).

For lawful interception (LI) it is not mandatory for the third party to own the exact private keys of the users. It is however mandatory to benefit of the same features, meaning that it must be able to decrypt the messages encrypted under the users public keys.

The participants in a key escrow system are:

- **The users**
  The users communicate via public channels using encrypted communication. They are aware that it is possible to be under surveillance and may also assume that the LEA illegally intercepts their secured communication.

- **Lawful Enforcement Authority (LEA)**
  It represents the entity that conducts lawful monitoring in accordance with a legitimate warrant.

- **Key Escrow Agency (EA)**
  EA stores the users private keys. As an assumption, it never leaks private keys unless a legitimate warrant is shown.
  In case that a KGC (Key Generation Center) exists in the scheme, then EA and KGC represent the same entity. This is the case for IBE.

- **Lawful Authority (LA)**
  LA approves the lay enforcement action when a warrant is requested. It is assumed that it never issues a warrant in conspiracy with a faulty LEA.

The required steps for the LEA to obtain the private key(s) are (Figure 2):

1. LEA sends an LI approval request to the LA;
2. LA sends the approval/rejection response to the LEA;
3. If LEA receives the approval from the LA, it forwards it to the EA as a Private Key Request;
4. EA sends the corresponding private key(s) to the LEA, based on the approval of the LEA;
5. LEA is now able to monitor the communication of the corresponding users.

3. IBE Key Escrow Properties

IBE provides key escrow capabilities by construction, due to the existence of the KGC: the KGC forwards to the LEA the corresponding private key(s) and therefore, LEA benefit of the same abilities as the original owner of the key.

However, this scenario has some major drawbacks: it cannot limit the duration of the surveillance by the LEA, it cannot restrict the surveillance to the messages sent or received by specific users, etc.

In order to avoid such a behavior, several properties of key escrow should be fulfilled. We give next the most important ones [1], [8] and analyze if IBE can satisfy them by construction. In Section 4 we will
exemplify how this properties can be improved by using the IBE as a part of a communication protocol.

3.1. Warrant bounds

In a key escrow system, it should be possible to limit the duration of the permission for the LEA by the LA. More precise, if the LA invests the LEA to monitor the communication for a precise period of time, the LEA should not be able to decrypt the ciphertext after the warrant period expires.

By default, in an IBE system the warrant bound property is not achieved. If LEA receives the private key of a participant, it will be able to decrypt the messages that he receives for the whole life of its public key or until the master key is changed. Usually, both remains unchanged for a long period of time (the public key is the identity of the user and the change of the master key leads to the change of the private keys of all the users). Therefore, LEA would most probably be able to decrypt ciphertext for longer than it has been authorized to.

However, if used as a part of a communication protocol, an IBE scheme can fulfill this property. The main idea is that KGC gives the LEA a session key that allows the decryption of the messages sent within that session. Once the session expires, the key that LEA possesses becomes useless. We give such an example in the next section.

3.2. Offline EA

The EA should not be needed for the whole surveillance period. Once the LEA gets the private keys from the KGC, it should perform the surveillance without the help of EA.

The property is fully satisfied for IBE schemes. After the LEA is given the necessary private keys, it can perform the decryption by itself.

The only exception appears when a new user joins the group. However, in this case, the EA (KGC) should also be online in order to allow the user to authenticate and send him the corresponding private key.

3.3. Efficiency

The process should not consume a large overhead. Otherwise, the scheme cannot be efficiently used in practice. In case of IBE, once LEA becomes authorized to perform the interception, it should just receive the corresponding private keys.

In case that other properties (as warrant bound for example) are satisfied, a larger overhead is needed.

3.4. Non user participation

The users should not recognize whether they are under surveillance or not. Although they are aware of the possibility of being under surveillance anytime, they should not be able to precisely know if the monitoring can be performed at a given moment.

In case of the trivial usage of IBE, if a user knows he is under surveillance, then he knows he may be under surveillance at any future moment (until his private key is changed).

In case the communication protocol admits the warrant bound property, then the participant knowledge that he may be under surveillance is limited for the warrant period, even if he knows that his messages are intercepted at a precise moment in time.

3.5. Surveillance switching

Lawful monitoring should permit a line of communication between specific users, as well as to monitor the communication that involves a specific user regardless of the partner.

This cannot be achieved in public key cryptosystem: once the LEA gets access to the private key of the user that is under surveillance, it becomes able to decrypt all his messages, regardless of the sender.

More, if LEA should be able to decrypt all the messages that a specific user sends, regardless of the partner, then it must possess all the private keys of the rest of the users.

Therefore, in the trivial case, a LEA must be given all the private keys of the users,
fact that permits it to decrypt any message. This is no longer true when IBE is used in a communication protocol as Han et al’s, as it will be explained in the next section.

3.6. Non directive monitoring

In case of monitoring a specific user, the surveillance should be possible regardless of the direction of the message flow. This property is related to the previous one in the sense that if LEA is able to decrypt the communication of a specific user, then it can monitor the communication of all the users.

As a remark, it may be very difficult for one system to fulfill all of the desired properties. However, using the IBE within a communication protocol improves the usability of the key escrow by satisfying most of the desired properties. An example is the Han et al. communication protocol [8]. We will refer in the next section to their modified protocol that uses the Waters IBE [9].

4. A more practical example

In order to accomplish as many properties of key escrow as possible, IBE are used as a part of communication protocols. Such an example is Han et al. model [5] for the mobile environment that eliminates some of the previously mentioned shortcomings. The protocol uses IBE as the underlying scheme, but generates different session keys. LEA receives the session private key that is authorized for, being able to decrypt only the communication of the corresponding session. In case the period of time that LEA needs to supervise the communication increases, then LEA receives the corresponding session key for each session.

We present next the communication protocol that relies on the Waters IBE, the first fully secured and efficient IBE.

4.1. Waters IBE

Definition 3: Be \( G \) and \( G_1 \) two multiplicative cyclic groups of prime order \( p \) and \( g \) a generator of \( G \). A bilinear map is a map \( e : G \times G \to G_1 \) with the following properties:

1) bilinear: \( \forall u,v \in G \) and \( \forall a,b \in \mathbb{Z} \), we have:
\[ e(u^a,v^b) = e(u,v)^{ab} \]
2) non degenerate: \( e(g,g) \neq 1 \)

\( G \) is a bilinear group if the group action in \( G \) can be computed efficiently and there exists a group \( G_1 \) and an efficient computable bilinear map \( e \) as above.

Waters scheme can be described as follows [11]:

- **Setup:** \( G = \langle g \rangle, \quad G_1, \quad \alpha \in \mathbb{Z}_p \)
  random, \( g_1 = g^\alpha \), \( g_2 \in G \) random, \( U = (u_1)_{i=1}^{n}, u_i \in G \) random, \( u^i \in G \), random. The public parameters are:
  \[ \text{params} = (g^a, g_1, g_2, u^i, U) \]
  and the master secret key \( g_2^a \).

- **Key Generation (Extract):**
  The identity \( ID \) is considered to be a string of \( n \) bits \( ID = v = (v_i)_{i=1}^{n} \). If the identity needs more than \( n \) bits for representation, then a hash function can be applied. Let \( V \) be the set of indexes that correspond to 1 in the bit representation of the identity \( v \):
  \[ V = \{i \mid v_i = 1\} \]
  The KGC selects a random \( r \in \mathbb{Z}_p \) and computes the private key that correspond to the identity \( ID = v \) as:
  \[ d_i = (d_1, d_2) = (g_2^a(u^i \prod_{j \in V} u_j)^r, g^r) \]

- **Encryption:**
  Let \( M \in G_1 \) be the plaintext and a random \( t \in \mathbb{Z}_p \). The encryption is computed as:
  \[ C = (C_1, C_2, C_3) = (e(g_1, g_2)^t M, g^r, u^i(\prod_{j \in V} u_j)^r) \]
• **Decryption:**
Let \( C = (C_1, C_2, C_3) \) be a valid encryption of \( M \) under the public key \( ID = v \). Then:
\[
M = C_1 \frac{e(d_2, C_2)}{e(d_1, C_2)}
\]

4.2. Modified Waters IBE

We slightly modify the Waters IBE in order to permit a private session parameter \( r_A \) that leads to a different private key for each session [11]:

- **Setup:**
  \( G = \langle g \rangle, \ G_1, \ \alpha \in \mathbb{Z}_p \) random, \( g_1 = g^a, \ g_2 \in G \) random, \( U = (u_i)_{1 \leq i \leq n} \) \( u_i \in G \) random, \( u' \in G \), random. The public parameters are:
  \[\text{params} = (g, g_1, g_2, u', U)\]
  and the master secret key \( g_2^\alpha \).

- **(Session) Key Generation:**
  For a given private key, a session private key is computed based on the value \( r_A \in \mathbb{Z}_p \) as:
  \[
d_v' = (d_1, d_2') = (d_1, d_2 g^{r_A}) = (g_2^a (u' \prod_{i \in \mathcal{V}} u_i)^r, (g g^{r_A})^r)
  \]

- **Encryption:**
Let \( M \in G_1 \) be the plaintext and a random \( t \in \mathbb{Z}_p \). The encryption is computed using \( r_A \in \mathbb{Z}_p \) as:
\[
C = (C_1', C_2, C_3) = (C_1 e(g^{-r_A}, C_3), C_2, C_3) = (e(g, g_2)^{t}, e(g^{-r_A}, u' (\prod_{i \in \mathcal{V}} u_i)^{r}) M, g^{t}, u' (\prod_{i \in \mathcal{V}} u_i)^r)
\]

- **Decryption:**
Let \( C = (C_1', C_2, C_3) \) be a valid encryption of \( M \) under the public key \( ID = v \) and session parameter \( r_A \in \mathbb{Z}_p \). Then:
\[
M = C_1' \frac{e(d_2', C_3)}{e(d_1, C_2)}
\]

**Theorem 1:** The modified Waters IBE scheme is consistent.

**Proof.**
\[\forall C = (C_1', C_2, C_3) \in G_1 \) a valid encryption of \( M \) under the public key \( ID = v \) and session parameter \( r_A \in \mathbb{Z}_p \), the owner of

---

**Figure 3. The Han et al. protocol with Waters IBE**
the session private key $d_v$ is able to correctly obtain $M$:

$$M = C_1 \frac{e(d_2, C_3)}{e(d_1, C_2)} =$$

$$= C_1 e(g^{-r_1}, C_3) \frac{e(d_2, g^{r_1}, C_3)}{e(d_1, C_2)} =$$

$$= C_1 e(g^{-r_1}, C_3) \frac{e(d_2, C_1) e(g^{r_1}, C_3)}{e(d_1, C_2)} =$$

$$= C_1 \frac{e(d_2, C_1)}{e(d_1, C_2)} e(g^{-r_1}, C_3) e(g^{r_1}, C_3) = M$$

### 4.3. Waters IBE used in Han et al. communication protocol

Han et al. recently introduced a model for lawful interception based on IBE [8]. It satisfies the requirements and overcomes the potential threats of IBE, in mobile network architecture.

We have considered the same model, with a slightly modification: the usage of Waters IBE as the underlying IBE scheme [9]. Our choice is based on the two advantages of Waters scheme: its efficiency and its proved security in the standard model, without the need of random oracles.

The model requires the existence of a MO (Mobile Operator). The users use the infrastructure of the MO for their encrypted communication. It is also assumed that each user shares a common encryption key with the MO and a signature algorithm so that the MO is able to verify the message authenticity. These assumptions are very probable to meet in practice.

Let A and B be the users that communicate to each other. We use the following notations:

- $ID(A), ID(B)$ - the identity of the user A, respectively B;
- $e_{KA}, e_{KB}$ - the encryption under the common key of the MO and the user A, respectively B;
- $e_{A}, e_{B}$ - the encryption under the identity of A, respectively B using the modified Waters IBE;
- $\text{sig}_A, \text{sig}_B$ - the public verifiable signatures of the users A, respectively B.

Figure 3 shows the modified version of Han et al. protocol using Waters IBE:

1. EA/KGC sends the corresponding private keys to users A and B. Their private keys are computed as in the original Waters scheme. This represents the Pre-process Phase.
2. If LEA wishes to monitor the communication from A and B (and it

![Figure 4. Multiple messages sent from A to B within one session](image-url)
had previously received an acceptance from the LA), it will send two LI (Lawful Interception) requests: one to EA/KGC (in order to receive the needed private key) and one to the MO (in order to receive the encrypted message). This represents the LI Request Phase.

3. When A wants to send a message M to B, he chooses a random $r_A$, signs it as $\text{sig}_A(r_A)$ and sends them to MO together with the ciphertext, obtained from the modified version of the Waters IBE by using the value of $r_A$ and $\text{ID}(B)$. The concatenated message is encrypted under the common key of MO and A.

4. MO decrypts the message, obtains the value of $r_A$ and if it verifies A’s signature on $r_A$, MO re-encrypts the message under the common key with B and sends it to B.

5. B decrypts the ciphertext using the common key that he shares with MO and obtains $e_B(M)$, the encryption of the original message M performed by A using the modified version of Waters under the identity of B and the random number $r_A$. If the signature $\text{sig}_A(r_A)$ verifies, then he decrypts using his private key and obtains the plaintext M.

6. Because MO had previously received the LI request from the LEA, he responds to the request by sending the session value $r_A$ to the EA/KGC and the ciphertext $e_B(M)$ to the LEA.

7. EA/KGC receives the session value $r_A$, computes a private key that corresponds to the identity of B by using the modified scheme and the session value and sends it to the LEA as a response to the previously received LI Request.

As a remark, notice that even though MO knows the value of $r_A$, it is not capable to discover the message M because it does not have access to a corresponding private key.

Han et al. proposed 2 variants of the model (for one-way and two-way communications). We have restricted in Figure 1 to the one-way communication protocol.

A trivial solution to construct the bidirectional communication may consist of using the one-way communication model twice and considering each of the two participants the initiator. In this scenario, each sender selects his own parameter $r_A$ and performs the encryption using this value. Therefore, LEA needs two different keys, one for each direction of communication. Figure 4 illustrates this
scenario, for the communication sent from A to B within one session. In the original Han et al. protocol, a two-way communication is possible without the need of 2 session parameters. In the modified Han et al. protocol this becomes possible if the initiator chooses by himself the value of the session parameter (although this may be a vulnerability of the system). This scenario is presented in Figure 5: A initiate the conversation with B, therefore A chooses the value of the session parameter $r_A$. For the rest of the session, both A and B will use the same value for encryption.

4.4. Analysis of the Lawful Interception Properties

We briefly analyze the improvements achieved by using IBE as a part of the communication protocol. After LEA receives the secret key and the encryption of the message, it is able to successfully decrypt. The main advantage of the protocol is that LEA is not capable to decrypt messages that are not encrypted using $r_A$. Therefore, if A chooses a new value $r_A \neq r_A$, the LEA must obtain a new warrant from the LA in order to receive the corresponding private key and continue the surveillance. Therefore, LEA is only capable to perform monitoring during the session it has been authorized for. So, this approach satisfies the warrant bound property. If B knows he is under surveillance at a given moment, he knows that he may be under surveillance for the rest of the session, but he knows nothing regarding the previous or future sessions. This was not true in case of pure IBE: a user that knows at a given moment in time that he is under surveillance becomes aware that he may be under surveillance at any moment in the future.

Table 1. IBE Key Escrow Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>IBE by Construction</th>
<th>IBE as a part of a Communication Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warrant bound</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Offline EA</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Efficiency</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Non user participation</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Surveillance switching</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Non directive monitoring</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

More, if B is the only user under surveillance, LEA is able to decrypt just the ciphertext sent to B. For example, if A wants to send a message to another user C, A will use a different session key and therefore, it becomes impossible for the LEA to decrypt the message. The same remark remains true for the messages that B sends to other participants. It becomes possible to monitor only the communication between A and B, no matter the sense of the message flow, by giving the LEA only 2 private session keys: the private session key used by A to send messages to B and the private session key used by B in order to encrypt messages for A. In conclusion, the communication protocol also satisfies the surveillance switching and non-directive monitoring. Of course, the drawback is a lower efficiency of the scheme. Table 1 summarizes the properties that an IBE scheme may fulfill by construction or by being used in a communication protocol. The improvement of the key escrow capabilities becomes evident in the latter case.
5. Conclusion

The paper considers the IBE schemes from the perspective of key escrow capabilities. We consider some of the most important properties a lawful interception must fulfill and analyze if an IBE is able to satisfy them by construction. In order to improve the applicability of IBE schemes in lawful interception systems, we consider the example of using them as a part of a communication protocol and highlight the obtained improvements.

Acknowledgment

This paper is supported by the Sectorial Operational Programme Human Resources Development (SOP HRD), financed from the European Social Fund and by the Romanian Government under the contract number SOP HDR/107/1.5/S/82514.

Parts of this paper have been published in the Proceedings of the International Conference on Security for Information Technology and Communications – SECITC 2012.

References


