Identity Based Encryption

Ananya Tantia

August 16, 2024

1 Introduction

What is IBE? IBE or Identity Based Encryption is a type of public-key encryption that allows users to generate a public key from a unique identifier, such as an email address or social security number. We use IBE in our everyday lives without even knowing it . For example if you send a message to your friend the application via which you send will encrypt it first based on your friend's unique username then it will send it to your friends computer which will decrypt the message based on a private key that is based on their username which no one except them knows . the decryption and encryption will be in such a way that even though both the keys are different both the messages will be the same.

2 Important mathematical concepts

2.1 Cryptographical Concepts

1. **Key generator** - A key generator is a trusted third party that generates keys for identity-based encryption. in the example the application you use will be the K and will generate several keys based on usernames.
2. **Master public key** - It is public key this is common to all users and is available publicly. it is used to generate public keys and decrypt the message
3. **Master private key** - A private key that is not known to anyone other that the key generator and is used to generate the private keys for each person based on their public keys.
4. **Public key** - It is a cryptographic key that is available to anyone but is intended for only one person.it is used to encrypt messages based on the receiver's public keys. if we take the previous example the receiver's username will be public keys .
5. **Private key**- Is unique to each person and is know only to that person and the key generator. it is used to decrypt the cipher text.

2.2 Methodology of encrypting an decrypting based on IBE

The key generator selects a binary pairing e : such that $e : G_1 * G_2 \to G_T$ where G_1 and G_2 are cyclic groups of prime order p and G_T is another cyclic group of the same prime order p. The Bi-linear map e satisfies the following properties-

- For all $P \in G_1$ and $Q \in G_2$ and $a, b \in Z_p^*$
- $e(a^P, b^Q) = e(a, b)^{PQ}$
- There exist $P \in G_1$ and $Q \in G_2$ such that $e(a, b) \neq 1$
- There exists an efficient algorithm where $e(a, b)$ can be computed efficiently

The key generator chooses a private master key $s \in Z_p^*$ and generates public master key $P_{pub} = sP$ The public parameters are $(G_1, G_2, G_T, e, P, P_{pub}, H_1, H_2)$, where $H_1$and H_2 are cryptographic hash functions.

$$H_1 : \{0,1\}^{\rightarrow G_1}$$

maps an identity ID to a point on the elliptic curve in G_1, and

$$H_2 : G_T ß \{0,1\}^n$$

is used to map elements of G_T to bitstrings.

2.2.1 Key Generation

Given an identity ID:

1. The PKG computes $Q_{ID} = H_1(ID)$, where $Q_{ID} \in G_1$
2. The PKG then computes the private key SK_{ID} for the user as:

$$SK_{ID} = sQ_{ID}$$

where s is the master secret. The private key SK_{ID} is securely transmitted to the user.

Suppose the identity is "alice@gmail.com" the key generator computes $Q_{ID} = H_1$ which maps to a point Q_{ID} on the eliptic curve. If the Q_{ID} = (15,22) and s is 7 then the private key for Alice would be $s.Q_{ID} = (15 \times 7, 22 \times 7)$

2.2.2 Encryption

To encrypt a message M intended for a user with identity ID:

1. The sender computes $Q_{ID} = H_1(ID)$
2. The sender then selects a random $r \in Z_*^p$
3. The ciphertext is computed as (U, V) where:

$$U = rPU = rP$$

$$V = M \oplus H_2(e(Q_{ID}, P_{pub})^r)$$

Here, $e(Q_{ID}, P_{pub})^r$ is an element of G_T and$\oplus$ denotes the XOR operation.

The ciphertext (U,V) is then sent to the recipient.

2.2.3 Decryption

Upon receiving the ciphertext (U, V), the user with identity ID decrypts the message as follows:

1. Compute $e(U, SK_{ID})$where $SK_{ID} = sQ_{ID}$

$$e(U, SK_{ID}) = e(rP, sQ_{ID}) = e(P, Q_{ID})^{rs}$$

2. Recover the message M by computing:

$$M = V \oplus H_2(e(U, SK_{ID}))$$

3. Since $e(U, SK_{ID}) = e(P, Q_{ID})^{rs}$ which is the same value as $e(QID, Ppub)r$ used during encryption, the original message M is successfully recovered.

2.3 Security

The security of IBE is based on the hardness of the Bilinear Diffie-Hellman Problem which can be stated as:

Given $aP, bP, cP \in G_1$ for unknown a, b, cZ_p compute

$$e(P, P)^{abc} \in G_T$$

We can assume that the Bilinear diffie hellman problem is secure because it takes a lot of time to be solved even if someone knows $aP, bP$and cP the big O notation for finding $e(P, P)^{abc}$ is very large.

2.4 Hierarchical Identity-Based Encryption (HIBE)

Hierarchical Identity-Based Encryption (HIBE) extends the concept of IBE to allow for hierarchical identities. For example, in an organization, identities could be structured as "alice@xyz.group.com", with the hierarchy "group.com" $\rightarrow$ "xyz.group.com" $\rightarrow$ "alice@xyz.group.com".

Key Derivation: In HIBE, each level in the hierarchy can derive the private key for its sub-level. If the private key for "xyz.group.com" is known, it can be used to derive the private key for "alice@xyz.goup.com". Mathematically:

- The master secret at each level is used to derive the master secret at the next level.
- The bilinear pairing properties ensure that the security of the keys is maintained across the hierarchy.

2.5 Security Proofs

To formally prove the security of IBE, we can use a reduction approach:

If an adversary can break the IBE scheme, then we can construct an algorithm that solves the BDHP, which is assumed to be hard. In the random oracle model, security proofs involve simulating the hash functions $H_1$and H_2 as random oracles and showing that any successful attack on the IBE scheme would imply a solution to the BDHP, leading to a contradiction.

3 Practical Uses of Identity-Based Encryption (IBE)

Identity-Based Encryption (IBE) offers significant practical advantages in various fields where secure communication and simplified key management are essential. Here are some key applications:

3.1 Email Encryption

IBE is particularly well-suited for email encryption. In traditional public-key systems, users must exchange or access each other's public keys before sending encrypted messages, which can be cumbersome. With IBE, the recipient's email address itself acts as the public key. For instance, if Alice wants to send a confidential email to Bob, she can directly encrypt the email using "bob@xyz.com" as the public key. Bob can then use his private key, generated by a trusted authority (PKG), to decrypt the message. This eliminates the need for a Public Key Infrastructure (PKI) and simplifies the process for users.

3.2 Access Control in Cloud Storage

In cloud storage systems, IBE can be used to control access to encrypted data. For example, a file can be encrypted using the intended recipient's identity, like "alice@xygroup.com". Only the employee with that identity, who possesses the private key for this specific public key , can decrypt and access the file. This ensures that sensitive data remains secure, even if stored in a cloud environment, where the storage provider may not be fully trusted.

3.3 Mobile and IoT Security

The proliferation of mobile devices and the Internet of Things (IoT) creates a need for lightweight and scalable security solutions. IBE can be deployed in these environments to simplify key management and secure communications between devices. For instance, IoT devices can use their unique identifiers (e.g., device serial numbers) as public keys, allowing them to securely exchange data without needing to pre-establish trust or exchange keys manually.

3.4 Secure Messaging Applications

In secure messaging applications, IBE allows users to communicate securely without exchanging keys in advance. A user can encrypt a message using the recipient's username or phone number as the public key. This approach is particularly useful in scenarios where users frequently join and leave the network, as it reduces the overhead associated with key distribution and management.

3.5 Digital Signatures

IBE can also be applied to digital signatures, where a user's identity is used to verify their signature. This simplifies the verification process, as the verifier can use the signer's identity directly to check the authenticity of the message. This application is useful in scenarios such as document signing, where the identity of the signer is crucial. Without digital signatures alice can never be sure if the message was indeed from bob or was from another person pretending to be bob.

3.5.1 How digital signatures work-

1. A pair of public and private keys are generated. The private key is only known to the signer.
2. The message M is then encrypted with the private key and becomes $e(M)$
3. Then the receiver alice decrypts it using the public key which becomes $d(e(M))$ which is M'
4. If M' matches M then alice knows that the message was indeed from bob.
5. M can be recovered by any cyrpto system that would have been decided by them.

3.6 Encryption for Emergency Situations

In certain emergency scenarios, such as disaster recovery, IBE can provide a means for authorized personnel to access critical information using their identities. For example, rescue teams can use predefined identities to decrypt emergency protocols or confidential data, ensuring rapid access without the need for pre-established keys.

4 Implementation Challenges

1. **Efficiency:** The computation of the bilinear pairing e(P,Q) is computationally expensive. Optimizing these computations is critical for practical implementations of IBE.
2. **Key Management:** While IBE simplifies public key management, the secure distribution of private keys from the PKG to users is a critical challenge, especially in environments with limited trust.
3. **Trust in PKG:** The PKG holds the master secret, which gives it the power to generate any user's private key. This creates a single point of trust and potential failure.

5 Future Directions

1. **Pairing-Based Cryptography:** Continued research on efficient pairing computations and alternative pairing-based cryptographic schemes.
2. **Post-Quantum Security:** Investigating the security of IBE in the context of quantum computing, which threatens the hardness assumptions underlying traditional cryptographic schemes.
3. **Decentralized IBE**: Exploring decentralized or distributed approaches to IBE to reduce reliance on a single PKG, enhancing security and trust.

6 Conclusion:

Identity-Based Encryption provides a powerful and flexible alternative to traditional public key infrastructures, offering simplified key management and user-friendly public keys. The mathematical foundation of IBE, rooted in bilinear pairings and the hardness of the Bilinear Diffie-Hellman Problem, ensures both security and efficiency in many cryptographic applications. However, practical challenges, particularly related to trust in the PKG, need to be addressed to realize the full potential of IBE in secure communication and data protection.

7 References

7.1 Citations -

- Chatterjee, Sanjit, and Palash Sarkar. *Identity-based encryption.* Springer Science & Business Media, 2011.
- Rubinstein-Salze, Simon Cryptography , Springer Undergraduate Mathematics Series, 2018