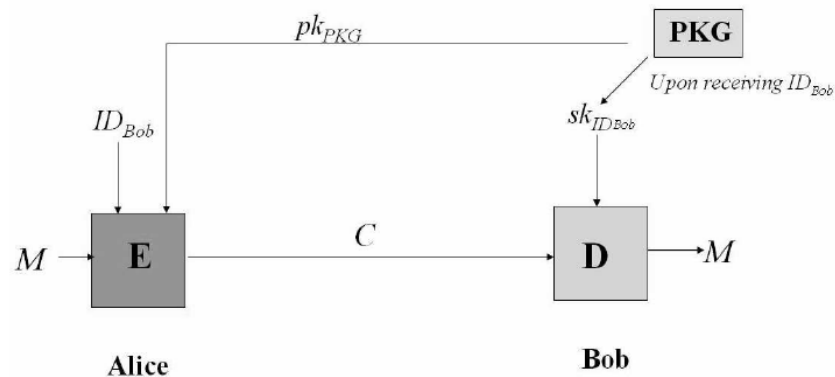


Basic Concepts of Identity-Based Encryption (IBE)

The sender Alice can use the receiver's identifier information which is represented by any string, such as email or IP address to encrypt a message.

The receiver Bob, having obtained a private key associated with his identifier information can decrypt the cipher-text.



Setup

The Trust Authority (PKG) creates its master (private) and public key pair sk_{PKG} and pk_{PKG} respectively. pk_{PKG} is given to all the interested parties and remains as a constant system parameter for a long period.

Private Key Extraction

The receiver Bob authenticates himself to the PKG and obtains a private key $sk_{ID_{Bob}}$ associated with his identity ID_{Bob} .

Encryption

Using Bob's identity ID_{Bob} and the PKG's pk_{PKG} , the sender Alice encrypts her plaintext message M and obtains a cipher-text C .

Decryption

Upon receiving the cipher-text C from Alice, Bob decrypts it using his private key $sk_{ID_{Bob}}$ to recover the plaintext M .

Pitfalls of Identity-Based Encryption (IBE)

Setup

- Every message ever encrypted by a master (private) key sk_{PKG} will be exposed if that key is ever compromised. Essentially, IBE is putting all the security into one single basket. As a singular ultra-high value asset, it becomes economical to attack the master key with brute force attack or social engineering (bribery, espionage, etc). It is unrealistic for anyone to rely on an external Trust Authority company to safeguard all its secrets
- The authenticity of IBE depends on the authenticity of the Trust Authority. There is no practical method for Alice and Bob to authenticate the identity of the Trust Authority without resorting to traditional server PKI certificate via Certificate Authority. In other words, IBE depends upon traditional server PKI certificate and RSA crypto method for its key distribution, which means IBE has higher exposure to risk and is less secure

Compared to Traditional PKI certificate:

- On the contrary, a compromised end-user certificate only exposes messages encrypted with that particular certificate.
- A compromised Certificate Authority certificate does not expose any messages encrypted in the past

Private Key Extraction

- The Trust Authority is subject to denial-of-service attack, which will paralyze all encryption and decryption operations
- Private Key extraction has a very high exposure to man-of-the-middle attack

Compared to Traditional PKI certificate:

- Certificates are stored in a distributed manner. Therefore, it has much smaller risk to man-of-the-middle attack
- Even when a Certificate Authority is subject to denial-of-service attack, encryption and decryption operations can still occur. Only certificate verification is affected.

Encryption

- IBE has a relatively short history, and the underlying crypto-method has not been subjected to widespread scrutiny. It is more likely that certain future advances in pure mathematics could render that crypto-method insecure. On the contrary, 2048-bits RSA encryption has gone through years of peer review
- To support revocation, IBE relies on the recipient's discipline to refrain from using the same ID ID_{Bob} for too long, or using an expired ID. In the long run, it leads to the proliferation of ID's, which will become unmanageable, because it is directory-less

Compared to Traditional PKI certificate:

- Certificates have well-defined expiry date, which prevents expired ID's from being used
- Certificates are being stored and managed properly by directories

Decryption

- IBE only supports a closed community. Different Trust Authorities can not interoperate with each other. Messages encrypted by one Trust Authority cannot be decrypted by another
- Users of IBE is forever locked-down by a Trust Authority

Compared to Traditional PKI certificate:

- Traditional PKI Certificates are Certificate-Authority-agnostic. A certificate published by one vendor can be used anywhere. They are not locked down to a single Certificate Authority

General considerations

- IBE does not support S/MIME

Compared to Traditional PKI certificate:

- S/MIME is a standard technology supported by every major email client, based on traditional PKI certificate

Author: Kai Cheung

Date: May 26, 2011

Version: 1.0

With description of IBE extracted from *A Survey of Identity-Based Cryptography* by Joonsang Baek, Jan Newmarch, Reihaneh Safavi-Naini, and Willy Susilo at the School of Information Technology and Computer Science, University of Wollongong