Docket #: S06-321

Proxy Identity Based Encryption

Proxy Identity Based Encryption (proxy IBE) is a new encryption scheme that allows a user to send data encrypted with any given public key to a receiving user who decrypts the data with their own private key which is of no relation to the key used for encryption. This is possible through the use of a proxy server that translates a message encoded in one key set into an encrypted form that can be decrypted by another key set. This means that Alice can encrypt data using her public key (or anyone else can use Alice's public key for encryption), but Bob can then decrypt the data using his unrelated private key once the proxy re-encrypts the message. Alice can encrypt all her data and messages with the same key, if she desires, and share them without having to share her secret key. To do this, Alice generates and gives a re-encryption key for her public key to the proxy; the proxy then re-encrypts messages using this re-encryption key so that the message can be decrypted using Bob's secret key. This means that Alice must grant permission for Bob to access the message or data in order for the proxy server to re-encrypt the data into a form that Bob can decrypt. The proxy server cannot decrypt the message because it does not have Bob's private key, so Bob is the only user capable of decrypting the data- yet he cannot do that without the translation task performed by the proxy.

Applications

- Networked storage. Alice can store data encrypted with her public key. If Bob wishes to access her data, she can give permission and the proxy can access her data, then transform it into the encrypted form that Bob can decode using his private key. Yet the proxy server can't decode her data, so she doesn't need to trust the proxy as much as with a normal public key system where Alice would need to give out her private key
- Law enforcement and government agencies can use the networked storage setup to provide secure databases
- Secure e-mail forwarding can be accomplished through these systems

- Outsourced spam filtering in a secure system can be accomplished through proxy IBE (identity based encryption)

Advantages

- No certificate management
- Optimal secret key size (no additional secret keys necessary)
- Optimal encoded message size (the re-encrypted message is as large as the original message)
- No additional algorithms or processes are necessary for the decryption of the re-encrypted message

Patents

- Published Application: 20080170701

Innovators

- Toshihiko Matsuo
- Dan Boneh
- Eu-Jin Goh

Licensing Contact

Imelda Oropeza

Senior Licensing Manager, Physical Sciences

Email