Guo, 25 Oct *Paper Summary Sheet 1*

Paper title and authors; where appeared.

Ch. 10.3 Hybrid Encryption

Katz and Lindell, Introduction to Modern Cryptography

What is the main problem this paper attacks?

The public and private key cryptography has some disadvantages compared each other- private ones need pre-shared secret key, public ones is ineffective.

What solution does the paper propose?

The solution is to combine the public and private key cryptography, take the advantage of each part.

What central idea did the authors use to solve it?

Since the public key cryptography is CPA secure, the sender can send a key under public key cryptography, which used as secret key in private key cryptography to encrypt the message. The result is there is no need for pre-shared secret, and the effectiveness for long enough message is significantly improved.

Why is this paper important?

The hybrid fashion keeps the advantages of both public and private cryptography, at the same time, it is CPA secure, as a result, it largely improve the efficiency for practical use.