Chapter 11

Securing Public Key Encryption Against Adaptive Chosen Ciphertext Attacks

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

To deal with active attacks in public key encryptions, the notion of security against an adaptive chosen ciphertext attack has been defined by Researchers. If an adversary can inject messages into a network, these messages may be ciphertexts, and the adversary may be able to extract partial information about the corresponding cleartexts through its interaction with parties in the network. The Security against chosen ciphertext attack is defined using an “decryption oracle.” Given an encryption of a message the “ciphertext” we want to guarantee that the adversary cannot obtain any partial information about the message. A method of securing Public Key Cryptosystems using hash functions is described in this chapter.

INTRODUCTION

In this chapter, we define the notion of security against adaptive chosen ciphertext attack for a public key encryption scheme. This security is defined using a decryption oracle. This chapter proposes a method using hash functions to secure public key encryption schemes. This chapter introduces the notion of Semantic Security and discusses modifications to the RSA algorithm to achieve semantic Security.

SECURITY OF PUBLIC KEY ENCRYPTION SCHEMES

Semantic security as defined by Goldwasser and Micali, (1984) captures the intuition that an adversary should not be able to obtain any partial information about a message given its encryption. However, this guarantee of secrecy is only valid when the adversary is completely passive, i.e., can only eavesdrop. Indeed, semantic security offers no guarantee of secrecy at all if an adversary can mount an active attack, i.e., inject messages into a network or otherwise influence the behavior of parties in the network.
To deal with active attacks, Racko and Simon (1991) defined the notion of security against an *adaptive chosen ciphertext attack*. If an adversary can inject messages into a network, these messages may be ciphertexts, and the adversary may be able to extract partial information about the corresponding cleartexts through its interactions with the parties in the network. Racko and Simon’s definition models this type of attack by simply allowing an adversary to obtain decryptions of its choice, i.e., the adversary has access to a “decryption oracle.” However, given an encryption of a message the “ciphertext” we want to guarantee that the adversary cannot obtain any partial information about the message. To achieve this, we have to restrict the adversary’s behavior in some way, otherwise the adversary could simply submit the target ciphertext itself to the decryption oracle. The restriction proposed by Racko and Simon is the weakest possible: the adversary is not allowed to submit the target ciphertext itself to the oracle; however, it may submit any other ciphertext, including ciphertexts that are related to the target ciphertext.

A different notion of security against active attacks, called Non-Malleability, was proposed by Dolev, Dwork, and Naor (1991). Here, the adversary also has access to a decryption Oracle, but his goal is not to obtain partial information about the target ciphertext, but rather, to create another encryption of a different message that is related in some interesting way to the original, encrypted message. For example, for a non-malleable encryption scheme, given an encryption of $n$, it should be infeasible to create an encryption of $n + 1$. It turns out that non-malleability and security against adaptive chosen ciphertext attack are equivalent (Bellare et al., 1998; Dolev et al., 2000).

An encryption scheme secure against adaptive chosen ciphertext attack is a very powerful cryptographic primitive. It is essential in designing protocols that are secure against active adversaries. For example, this primitive is used in protocols for authentication and key exchange (Dwork et al., 1996; Dolev et al., 2000; Shoup, 1999) and in protocols for escrow, certified e-mail, and more general fair exchange (Asokan et al., 2000). It is by now generally recognized in the cryptographic research community that security against adaptive chosen ciphertext attack is the right notion of security for a general-purpose public-key encryption scheme. This is exemplified by the adoption of Bellare and Rogaway’s OAEP scheme (Bellare, M (a practical but only heuristically secure scheme) as the internet encryption standard rsa pkcs#1 version 2, and for use in the set protocol for electronic commerce.

Another motivation for security against adaptive chosen ciphertext attack is Bleichenbacher’s attack (Bleichenbacher, 1998) on the widely-used SSL key establishment protocol, which is based on RSA pkcs#1 version. Bleichenbacher showed how to break this protocol by mounting a specific chosen ciphertext attack (SSL still uses RSA pkcs#1 version 1, but the protocol has been patched so as to avoid bleichenbacher’s attack).

There are also intermediate notions of security, between semantic security and adaptive Chosen Ciphertext security. Naor and Yung (1990) propose an attack model where the adversary has access to the decryption oracle only prior to obtaining the target ciphertext, and the goal of the adversary is to obtain partial information about the encrypted message.

Naor and Yung called this type of attack a *chosen ciphertext attack*; it has also been called a “lunch-time” or “midnight” attack, and also an indifferent chosen ciphertext attack.

**SECURITY AGAINST ADAPTIVE CHOSEN CIPHERTEXT ATTACK**

Security is defined via the following game played by the adversary: First, the encryption scheme’s key generation algorithm is run, with a security parameter as input. Next, the adversary makes arbitrary