Chapter 13
Provable Security for Public Key Cryptosystems:
How to Prove that the Cryptosystem is Secure

Syed Taqi Ali
National Institute of Technology Kurukshetra, India

ABSTRACT

In the early years after the invention of public key cryptography by Diffie and Hellman in 1976, the design and evaluation of public key cryptosystems has been done merely in ad-hoc manner based on trial and error. The public key cryptosystem said to be secure as long as there is no successful cryptanalytic attack on it. But due to various successful attacks on the cryptosystems after development, the cryptographic community understood that this ad-hoc approach might not be good enough. The paradigm of provable security is an attempt to get rid of ad hoc design. The goals of provable security are to define appropriate models of security on the one hand, and to develop cryptographic designs that can be proven to be secure within the defined models on the other. There are two general approaches for structuring the security proof. One is reductionist approach and other is game-based approach. In these approaches, the security proofs reduce a well known problem (such as discrete logarithm, RSA) to an attack against a proposed cryptosystem. With this approach, the security of public key cryptosystem can be proved formally under the various models viz. random oracle model, generic group model and standard model. In this chapter, we will briefly explain these approaches along with the security proofs of well known public key cryptosystems under the appropriate model.

DOI: 10.4018/978-1-7998-1763-5.ch013

INTRODUCTION

In the early years after the invention of public key cryptography by Diffie and Hellman in 1976 (Diffie & Hellman, 1976), design and evaluation of public key cryptosystems has been done merely in an ad-hoc manner. That is the fact that the cryptosystem which withstood cryptanalytic attacks for several years is considered to be a secure cryptosystem. But there are many cryptosystems which have been broken after long time of their design. For example, Chor-Rivest cryptosystem (Chor & Rivest, 1985), (Lenstra, 1991), based on the knapsack problem, took more than 10 years to break totally (Vaudenay, 1998), whereas, before this attack it was believed that it is strongly secure. Due to various similar successful attacks on the cryptosystems, the cryptographic community understood that the lack of attacks at some time should never be considered as a security validation and demands the mathematical proof which guarantees the security of cryptosystems.

Provable Security

The paradigm of "provable" security is an attempt to solve this issue. The first public key encryption scheme which provides the mathematical proof of security was proposed by Rabin (Rabin, 1979) in 1979. Later, idea of provable security was introduced in the work of Goldwasser and Micali (Goldwasser, & Micali, 1984) in 1984. Rabin (Rabin, 1979) formally relates the difficulty of breaking the scheme (in some security model) to the difficulty of factoring an integer (a product of two large primes). The basic goals of provable security are, to define appropriate models of security on the one hand and to develop a cryptographic designs that can be proven to be secure within defined model on the other.

The formal security model consists of two definitions; firstly, it must specify how a polynomial-time adversary can interact with legitimate users of a cryptosystem and secondly, it must state what adversary should achieve in order to "break" the cryptosystem. For example, in encryption schemes as an adversary achievement - we define either to recover the message from ciphertext or to distinguish two ciphertexts whether they belong to same plaintext or to correctly map a ciphertext with the appropriate plaintext among the two given, etc.. And, as an adversarial interaction - we define that either adversary can get the decryption of any ciphertext of her choice or can only get the decryption of predefined ciphertexts or cannot get any decryption facility, etc.. Similarly, for digital signature schemes, we have such security models. The strength of the cryptosystem depends on how strong the security model is, under which it is proven secure. Detailed security models of public key encryption and digital signature schemes are discussed in subsequent sections.

Often, building a cryptographic scheme requires some particular atomic primitive(s). In order to prove the security of the scheme, one needs to provide the polynomial-time reduction procedure, which shows that the only way to break the scheme is to break the underlying atomic primitive(s). In other words, they must mathematically relate the security of the cryptosystem to the security of the atomic primitive(s) (such as one-way function or permutation or any hard problem on which scheme is built). Now a days cryptographic schemes are developed based on some well-studied problem(s) (such as integer factorization, discrete logarithm problem or any NP problem) and they provide *reductionist procedure* as a security proof to link the security of the scheme with the underlying well-studied problem. Eventually, if there exists some adversary who can break the proposed scheme then one can use that adversary with