ON PROVABLE SECURITY OF SOME PUBLIC KEY ENCRYPTION SCHEMES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

TURGUT HANOYMAK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

SEPTEMBER 2012

Approval of the thesis:

ON PROVABLE SECURITY OF SOME PUBLIC KEY ENCRYPTION SCHEMES

submitted by **TURGUT HANOYMAK** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Ersan Akyıldız _____
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak _____
Head of Department, **Cryptography**

Prof. Dr. Ersan Akyıldız _____
Supervisor, **Mathematics Department, METU**

Assist. Prof. Dr. Ali Aydın Selçuk _____
Co-supervisor, **Computer Science Department, Bilkent University**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy _____
Mathematics Department, METU

Prof. Dr. Ersan Akyıldız _____
Mathematics Department, METU

Assist. Prof. Dr. İsmail Hakkı Denizler _____
Mathematics Department, Yüzüncü Yıl University

Assist. Prof. Dr. Ali Aydın Selçuk _____
Computer Science Department, Bilkent University

Dr. Muhiddin Uğuz _____
Mathematics Department, METU

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: TURGUT HANOYMAK

Signature :

ABSTRACT

ON PROVABLE SECURITY OF SOME PUBLIC KEY ENCRYPTION SCHEMES

Hanoymak, Turgut
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ersan Akyıldız
Co-Supervisor : Assist. Prof. Dr. Ali Aydın Selçuk

September 2012, 59 pages

In this thesis, we analyse the security criteria of some public key encryption schemes. In this respect, we present the notion of adversarial goals and adversarial capabilities. We give the definition of provably security by means of several games between the challenger and the adversary in some security models, namely the standard model and the random oracle model. We state the main differences between these two models and observe the advantage of the success probability of the adversary in breaking the cryptographic schemes. We search the ways of making more efficient and provably secure encryption schemes under weak assumptions. In this context, we examine the constructions of some public key encryption schemes such as RSA, ElGamal, Cramer-Shoup, Paillier, Damgard and finally Zheng-Seberry schemes and discuss under which circumstances they satisfy which security notions. Finally, we modify one of the schemes proposed by Zheng-Seberry -which is based on ElGamal signature- by adapting Schnorr signature in order to enhance the efficiency and give a rigorous proof of security in the random oracle model.

Keywords: public key encryption, provable security, standard model, random oracle model

ÖZ

AÇIK ANAHTAR ŞİFRELEME SİSTEMLERİNİN İSPATLANABİLİR GÜVENLİĞİ

Hanoymak, Turgut
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ersan Akyıldız
Ortak Tez Yöneticisi : Yrd. Doç. Dr. Ali Aydın Selçuk

Eylül 2012, 59 sayfa

Bu tezde, bazı açık anahtar şifreleme sistemlerinin güvenlik kriterlerini analiz ediyoruz. Bu anlamda, sistemi kırmaya çalışanın amacını ve bu amaca yönelik kapasitelerini sunuyoruz. Standart modelde ve rastgele kahin modelinde sistem kırıcı ile oynanan çeşitli oyunlar vasıtasıyla ispatlanabilir güvenliğin tanımını veriyoruz. Bu iki model arasındaki esas farkları belirtiyoruz ve kriptografik sistemlere saldıran düşmanın başarı olasılığının avantajını gözlemliyoruz. Zayıf varsayımlar altında verimli, pratikte kullanışlı ve güvenliği ispatlanmış sistemler yapmanın yollarını arıyoruz. Bu amaç doğrultusunda RSA, ElGamal, Cramer-Shoup, Paillier, Damgard ve son olarak Zheng-Seberry açık anahtar şifreleme sistemlerinin yapılarını inceliyoruz ve bu sistemlerin hangi durumlarda hangi güvenlik notasyonlarını sağladıklarını açıklıyoruz. Son olarak, Zheng-Seberry'in önerdiği ElGamal imzasına dayanan sistemi Schnorr imza algoritması kullanarak modifiye ederek daha etkili bir sistem elde ediyoruz ve bu sistemin rastgele kahin modelinde güvenli olduğunu ispatlıyoruz.

Anahtar Kelimeler: açık anahtar şifrelemesi, ispatlanabilir güvenlik, standard model, rastgele kahin modeli

To my lovely Mom and Dad

ACKNOWLEDGMENTS

"Imagination is more important than knowledge."

Albert Einstein

I would like to express my gratitude to all those who supported me in completing this thesis. I would like to express my deepest gratitude to my supervisor Prof. Dr. Ersan Akyıldız for his guidance and insight he provided throughout this research. His ideas and tremendous support had a major influence on this thesis.

I would like to express my sincere gratitude to Assist. Prof. Dr. Ali Aydın Selçuk for his encouragement and many advices with useful discussions.

I would like to thank my dear friend Dr. Murat Ak for his support and helpful conversations.

I am indebted to all the members of the Institute of Applied Mathematics at Middle East Technical University, especially Nejla Erdoğdu, Atilla Bektaş, Canan Çimen, Nurgül Gökgöz, Oğuz Yayla and Bilgi Yılmaz for their lovely friendship and helping me getting positive motivated through my university life.

Last but definitely not least, I would like to send my special thanks to my family, especially my Mom and Dad for all their support over the years. Without their unending love, neither this thesis nor my life would be complete.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

CHAPTER 1

INTRODUCTION

"Better know nothing than half-know many things."

Friedrich Nietzsche

Throughout the last century, especially with the beginning of public key cryptography due to Diffie-Hellman [14], many cryptographic schemes have been proposed and it is significant to note that their security depends on some mathematically hard problems such as the integer factorization problem, RSA problem and knapsack problems. In fact, many people think that a cryptographic algorithm is assumed to be secure if it resists to cryptographic attacks for a long time. However, some schemes may take several years before widely studied in details so it is possible to be broken in the future such as the Chor-Rivest system based on the knapsack problems.

Later, cryptographic researchers are focused on trying to provide provable security for public key cryptographic algorithms in a complexity theory. The idea of provable security was first introduced by Goldwasser-Micali [19] and the notion of semantic security which is also called polynomial indistinguishability was defined. Later, Naor and Yung introduced a more severe security notion called security against non-adaptive chosen ciphertext attacks which is also called lunch time attacks denoted by CCA1 [27]. In this attack model, an adversary is given a decryption oracle and may access *only before* getting the challenge ciphertext. Hence, the ciphertexts queried to the decryption oracle are uncorrelated with the challenge one but they may be related with one another. Rackoff and Simon [34] improved this type of attack model and introduced the strongest notion of security which is called security against adaptive chosen ciphertext attacks denoted by CCA2. In this attack model, the attacker may query the decryption oracle *before and after* getting the challenge ciphertext. So, the ciphertexts

queried to the decryption oracle may related with the challenge ciphertext. They presented cryptosystems whose security proofs are based on noninteractive zero knowledge proof techniques which are horribly inefficient due to the fact that multiple gigabytes of ciphertext may be needed to encrypt a single bit of plaintext. Dolev, Dwork and Naor proposed a notion of non-malleability cryptography [15] meaning that the adversary who observes a ciphertext C of plaintext P, cannot modify it consciously and obtain a valid ciphertext C' of a plaintext P' which is related to P where this relation is known by the adversary. Fujisaki and Okamoto [17] gave a generic construction from a one way trapdoor function which is secure against chosen plaintext attacks to a public key encryption scheme secure against chosen ciphertext attacks. Damgard [11] first initiated efficient and simply constructed public key encryption schemes which are secure against nonadaptive chosen ciphertext attacks based on Diffie-Hellman/ElGamal public key cryptosystems. Zheng and Seberry [39] proposed three immunizing methods to make public key encryption schemes secure against adaptive chosen ciphertext attacks by appending a tag to each ciphertext which is related to the message. These immunizing methods are encrypting using with one way hash function C_{owh}, with universal hash family and with ElGamal digital signature adaptation, C_{sig}. They are different from each other at the point of tag generation. Zheng and Seberry also introduced *sole-samplability* security notion which is especially related to chosen ciphertext attacks. Informally, it means that there is no other way to generate ciphertext y than to pick a message x first and compute $y = E(x)$, i.e., there is no way to generate valid ciphertexts without knowing the underlying plaintexts. They also prove that if a scheme is sole-samplable, then the cryptosystem is semantically secure against adaptively chosen ciphertext attacks if and only if it is semantically secure against chosen plaintext attacks.

Although C_{owh} is efficient and has a simple design, it is shown to be insecure against known plaintext attacks [38] and also the authentication capability fails shown by Lim and Lee [25]. This is because the tags are computed as a function of the message alone whereas this attack cannot be applied to C_{sig}, since the random numbers used to generate a seed are also involved in generating a tag. Lim and Lee also presented another method for attaining security against adaptive chosen ciphertext attacks and this method is useful for an application to group oriented cryptosystems [12]. In this method, the deciphering algorithm first checks that the ciphertext is legitimate and then outputs the matching plaintext only when the check is successful. This is different from Zheng-Seberry method where the deciphering algorithm

first recovers the plaintext and then outputs it only when the checking condition on it is satisfied. To overcome this vulnurability of C_{owh}, and the other immunizating methods, Zheng [40] improved the tag generation methods by adding some randomness to the input of the hash function being used to get ciphertexts and also noted that if Schnorr signature [36] is adapted instead of ElGamal in C_{sig}, a more efficient scheme can be obtained.

In provably security, the security is proved via a reduction method. For this, we first consider a computationally hard underlying mathematical problem P which is well known to be intractable by any probabilistic polynomial time algorithm. Then, we provide a polynomial reduction from this mathematical problem to the problem P' of breaking the cryptosytem. Finally, we decide that if there exists an algorithm A breaking the cryptosystem in polynomial time, then we can build a probabilistic polynomial time algorithm A' which uses A as a subroutine, to get a contradiction. Therefore, we state that the scheme is computationally secure.

Such security proofs in the standard model suffer from efficiency and hence up to date very few practical public key schemes can be proven secure in the standard model. But, Cramer and Shoup [9] proposed such a scheme which is quite practical and is provably secure against adaptive chosen ciphertext attacks under standard intractability assumptions. Because of inefficiency to prove the security in the standard model, researchers tried to provide security proofs of public key encryption schemes in an efficient way. First attempt came from Bellare and Rogaway [4]. They proposed a model, namely the random oracle model as a counterpart to the standard version. In this model, hash functions are considered behaving like truely random functions. Hence, it is reasonable to model a secure hash function as a completely random function in a security analysis. This mostly reduces the process of proving security of cryptographic scheme. By doing so, we know that the output of the hash function is completely random and independently generated values on different inputs. Therefore, adversary can get no advantages about the outputs for any other inputs although he knows the hash values for several different inputs. The RO model gives an opportunity for the designer of the scheme to construct the responses about the outputs in order to prove the security of the scheme, i.e, we may control the attacker's behavior which is imposibble in the real world.

We note that the schemes with security proofs in the random oracle model may not be necessarily secure when the hash function is fixed. Canetti et al. [8] showed that it was possible to

construct an encryption scheme that was provably secure in the random oracle model but insecure when the random oracle was instantiated with any hash function. In the standard model, the attacker knows the description of the hash function and then submits it to the decryption oracle as a ciphertext and the oracle outputs the secret key. So, their scheme is completely artificial.

Baek and Zheng [3] was able to prove that the modified version of C_{owh}, is secure against adaptive chosen ciphertext attacks in the random oracle model under the gap Diffie-Hellman assumption [28].

In this thesis, we focus on one of the three immunizing methods presented by Zheng and Seberry [39], namely C_{sig} and following Zheng's idea, we modify the C_{sig} scheme by adapting the Schnorr signature [36] instead of ElGamal signature [16] and prove that the modified version C_{msig} is provably secure against adaptive chosen ciphertext attacks in the random oracle model under the gap Diffie-Hellman assumption.

This thesis is organized as follows:

In Chapter 2, we review the security notions on public key encryption schemes and discuss security models in terms of adversarial goals and adversarial capabilities. Then we give some probabilistic public key encryption schemes and show that under which assumptions they satisfy which security notions.

In Chapter 3, we discuss the random oracle model and the standard model which are the main tools for security analysis. Then we give game hopping technique. This technique is useful when proving security via a sequence of games such that successive games are indistinguishable from the view of the adversary and this indistinguishability is related to the underlying mathematically hard problems. We mention some concrete security proofs of several public key encryption schemes. We briefly mention about Fujisaki and Okamoto's construction and propose a shortcut in this construction by checking the consistency of the ciphertext using the random value instead of requiring re-encryption and investigate for which probabilistic encryption schemes satisfy this construction.

In chapter 4, we deal with the active attacks and construction methods for public key encryption schemes. These methods are utilized to make the schemes secure against adaptive chosen ciphertext attacks. We also analyse the structure of the schemes and explain which security

notion they satisfy under which circumtances. Finally, we focus on C_{sig} encryption scheme and modify it with Schnorr signature, then we give a rigorous proof of security against chosen ciphertext attacks in the random oracle model.

In chapter 5, we complete the thesis with conclusion part.

CHAPTER 2

SECURITY NOTIONS AND PUBLIC KEY ENCRYPTION SCHEMES IN THE STANDARD MODEL

"Intelligence plus character - that is the goal of true education."

Martin Luther King

In this chapter, we review security models in terms of the adversarial goals and the adversarial capabilities. We define what security actually means to decide whether a scheme is secure. In this respect, we investigate some public key encryption schemes. Finally, we discuss the Cramer-Shoup encryption scheme [9] which is the first efficient and practical scheme proven to be secure against adaptive chosen ciphertext attacks in the standard model.

2.1 Public Key Encryption Scheme

Definition 2.1.1 *A public key encryption scheme is a tuple of probabilistic polynomial time algorithms* $\Pi = (Gen, Enc, Dec)$ *such that:*

1. *The key generation algorithm Gen takes as input the security parameter and outputs a pair of public and secret keys* (pk, sk).

2. *The encryption algorithm Enc takes as input a public key pk and a message m from some underlying plaintext message space. It outputs a ciphertext c, i.e,* $c = Enc_{pk}(m)$.

3. *The decryption algorithm Dec takes as input* (sk, c) *and outputs a message m or* $\perp$. *We denote it by* $m = Dec_{sk}(m)$.

We note that *Enc* may be probabilistic but *Dec* must be deterministic and it is required for any encryption scheme to be valid,

$$Dec_{sk}(Enc_{pk}m) = m$$

is satisfied.

2.1.1 Success Probability of The Adversary

We decide that a cryptographic scheme is secure if the success probability of an adversary trying to break the scheme is small. This notion is achieved by negligible functions.

Definition 2.1.2 *A function* $\epsilon : \mathbb{N} \longrightarrow \mathbb{R}^+ \cup 0$ *is negligible, if for every positive polynomial p, there exists an integer* k_p *such that*

$$\textit{for all } n > k_p, \;\; \textit{we have } \epsilon(n) \; < \frac{1}{p(n)}.$$

In other words, a negligible function approaches zero faster than the inverse of any polynomial. We denote this function by *negl* in the following sections.

2.2 Security Models

In the cryptography literature, there are several adversarial goals and capabilities. When we talk about the security of a cryptographic scheme, we need to define them clearly. As the goal becomes more difficult or as the capabilities are more limited, the security proof becomes easier. First, we review some adversarial goals and capabilities related to them, then give proof techniques of some public key encryption schemes in the standard model.

2.2.1 Adversarial Goals

2.2.1.1 One-Wayness

This is a weak kind of adversarial goal where the purpose of the adversary is to reveal the whole plaintext m of a particular ciphertext c. However, this is an extremely weak notion

of security because revealing almost all of the plaintext is considered to be unsuccessful according to this definition but actually in almost all systems revealing the plaintext partially is considered successful. This goal is defined via a game between the adversary and the challenger as follows:

Game 1 The One Wayness Game: $PubK^{ow}_{A,\Pi}$

1: *Gen* is run to obtain the keys (pk, sk)
2: m is chosen at random from message space
3: The challenge ciphertext $c = Enc_{pk}(m)$
4: Adversary A is given pk and c to produce $m' = A(pk, c)$
5: The output of the game is defined to be 1 if $m^{'} = m$ and $\perp$ otherwise.

A more convincing adversarial goal namely, indistinguishability, which focuses on keeping the entire plaintext information secret, is given below:

2.2.1.2 Indistinguishability

This goal focuses on keeping the entire plaintext information secret and it is the most popular adversarial goal. In this goal, the adversary selects two plaintexts of his choice and sends them to an hypothetical challenger who has the secret key. The challenger randomly selects one of the messages, encrypts it and sends the challenge ciphertext back to the adversary. Here, the goal of the adversary is to find out which of the plaintexts has been selected by the challenger.

Game 2 IND-CPA Game: $PubK^{ind-cpa}_{A,\Pi}$

1: *Gen* is run to obtain public and secret keys (pk, sk).
2: Adversary A is given pk, outputs a pair of messages $(m_0,\ m_1)$ of equal length.
3: A random bit $b \in (0, 1)$ is chosen, the challenge ciphertext $c = Enc_{pk}(m_b)$ is computed and given to A.
4: A outputs a bit $b^{'}$.
5: The output of the game is defined to be 1 if $b^{'} = b$ and 0 otherwise.

Remark 2.2.1 *We note that the encryption algorithm has to be probabilistic although the decryption algorithm is always deterministic. Because, otherwise, the adversary can encrypt*

both plaintexts that he has chosen and compare the resulting ciphertexts to the challenged one which would be a trivial solution.

Remark 2.2.2 *Indistinguishability means that a ciphertext gives semantically no information about the plaintext. In other words, whatever a passive adversary can compute about m given the challenge ciphertext c, he can also compute without c. This is why it is also called semantic security [19].*

Definition 2.2.3 *A public key encryption scheme* $\Pi = (Gen, Enc, Dec)$ *is IND-secure against chosen plaintext attacks if for all probabilistic polynomial time adversaries A, there exists a negligible function such that*

$$Pr[PubK^{cpa}_{A,\Pi} = 1] \leq \frac{1}{2} + negl.$$

2.2.1.3 Malleability

The notion of malleability is introduced by Naor et al. [15]. The goal of the adversary A who observes a ciphertext c of plaintext m, cannot modify it consciously and obtain a valid ciphertext c' of a plaintext m' which is related to m where this relation is known by the adversary.

2.2.2 Adversarial Capabilities and Indistinguishability Games

There are several possible capabilities of an attacker in the public key setting depending on the availability of the decryption oracle which is a hypothetical black box that is presented to the attacker so that it can make decryption queries of its own choice and gets the corresponding plaintexts. This captures the possible real life attacks that consist of attackers that has gained temporary access to the decryption oracle. In this respect, there are three types of decryption oracle access:

- CPA (Chosen Plaintext Attack): if there is no decryption oracle access at all, we call this a chosen plaintext attack.
- CCA1 (Non-adaptive Chosen Ciphertext Attack, or lunchtime attack): Adversary A can access the decrpytion oracle until it sees the ciphertext it needs to break.

- CCA2 (Adaptive Chosen Ciphertext Attack): Adversary A always has access to the decryption oracle but querying the ciphertext it needs to break is prohibited.

Remark 2.2.4 *Security against adaptive chosen ciphertext attacks is the most widely accepted level of security notion.*

We explain them in Game 3 and Game 4.

Game 3 IND-CCA1 Game: $PubK^{cpa}_{A,\Pi}$

1: Gen is run to obtain keys (pk, sk).
2: Adversary A is given pk, as well as oracle access to Dec_{sk} and outputs a pair of messages $(m_0,\ m_1)$ of equal length.
3: A random bit $b \in (0, 1)$ is chosen, and the challenge ciphertext $c = Enc_{pk}(m_b)$ is computed and given to A.
4: A continues to interact with Dec_{sk} before he gets the challenge ciphertext c and later it is not allowed, then this kind of experiment is called CCA-1 or lunch time attacks.
5: The output is defined to be 1 if $b' = b$ and 0 otherwise.

Game 4 IND-CCA2 Game: $PubK^{cpa}_{A,\Pi}$

1: Gen is run to obtain keys (pk, sk).
2: Adversary A is given pk, as well as oracle access to Dec_{sk} and outputs a pair of messages $(m_0,\ m_1)$ of equal length.
3: A random bit $b \in (0, 1)$ is chosen, and the challenge ciphertext $c = Enc_{pk}(m_b)$ is computed and given to A.
4: A continues to have access to Dec_{sk} even after he sees the challenge ciphertext, but may not request a decryption of the challenge ciphertext itself and finally outputs a bit b'.
5: The output is defined to be 1 if $b' = b$ and 0 otherwise.

2.2.3 Computational Security and Reductions

Most of the security proofs in the literature are in the form of a reduction. Typically, a mathematically hard problem M is reduced to breaking the scheme S that is assumed to be provable secure. Existence of such a reduction implies that the problem of breaking the scheme S is as hard as M. This implication stems from the following contraction argument: If there exist

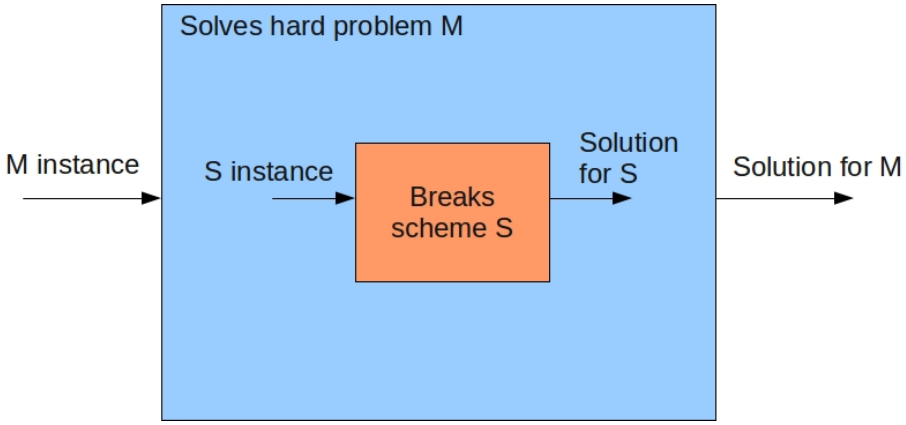

Figure 2.1: The reduction idea to prove security of public key schemes

a polynomial time algorithm A that breaks the scheme S, then due to this reduction, one may construct a polynomial time algorithm B which uses A as a subroutine to solve M which is assumed to be impossible. This is explained in Figure 2.1.

2.3 Security Analysis of Some Public Key Encryption Schemes

Before we review public key encryption schemes, we give some definitions which are utilized throughout this chapter.

Definition 2.3.1 *The set of integers* $\{0,\ 1,\ 2,\ ...,\ N-1\}$ *is defined as the integers mod N and denoted by* $\mathbb{Z}_N$.

Definition 2.3.2 *The multiplicative group of* $\mathbb{Z}_N$ *is*

$$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N \mid gcd(a,\ N) = 1\}$$

2.3.1 The RSA Encryption Scheme

Rivest, Shamir, Adleman proposed this scheme due to the trapdoor one way permutation property of the RSA function [35]. The key generation algorithm produces a large composite number $N = p \cdot q$ where p and p are primes, a public key e and private key d such that $e \cdot d = 1 \bmod \phi(N)$ is satisfied. The encryption of a message m from $\mathbb{Z}_N^*$ is an element of $\mathbb{Z}_N^*$, namely $c = m^e \bmod N$. One finds m using the secret key d by computing $m = c^d \bmod N$.

Definition 2.3.3 (RSA problem) *Let $N = p \cdot q$ where p and p are prime numbers. Let e be an integer relatively prime to $\phi(N)$. The RSA problem states that for a given $y \in \mathbb{Z}_N^*$, compute the e-th root of y, namely x, such that*

$$y = x^e \bmod N.$$

If the factorization of N is known, then the RSA problem can be easily solved.

RSA assumption: Given $N = p \cdot q$, the RSA problem is intractable.

- This encryption scheme is one-way secure due to the RSA problem.
- Since RSA encryption is deterministic, it does not satisfy IND-CPA security notion (i.e, semantic secure). It is because, given the challenge ciphertext c of either m_0 or m_1, the adversary A simply computes $c_0 = m_0^e \bmod N$ and $c_1 = m_1^e \bmod N$ and checks the resulting ciphertexts with the challenge one.
- RSA encryption scheme is vulnerable to a chosen ciphertext attack. If an adversary A gets the challenge ciphertext $c = m^e \bmod N$, he can choose a random element r from $\mathbb{Z}_N^*$ and compute the modified ciphertext as $c^{'} = r^e \cdot c \bmod N$. Since c' is different from the challenge, A asks it to the decryption oracle, gives the decryption $m^{'}$ of this ciphertext, then recovers $m = m^{'} \cdot r^{-1} \bmod N$.
- The scheme is malleable: Let the adversary A gets the challenge ciphertext $c = m^e \bmod N$, then he is able to generate, for example, $c' = 2^e \cdot c$ such that the underlying plaintexts satisfy a relation $m^{'} = 2m$ This holds, because

$$(c^{'})^d = (2^e \cdot m^e)^d = 2^{ed} \cdot m^{ed} = 2 \cdot m \bmod N.$$

Remark 2.3.4 *Bellare and Rogaway [5] proposed a padding scheme named Optimal Asymmetric Encryption Padding which is often used with RSA encryption. It uses two random oracles and achieves IND-CCA security with trapdoor one way permutation under the RSA assumption in the random oracle model.*

2.3.2 Rabin Encryption Scheme

Breaking a cryptographic scheme is not necessarily equivalent to solving the underlying mathematically hard problems. Rabin's scheme is a counter example of it. If we know the fac-

torization of N, then we can convert the RSA function and anybody can not invert it without knowing p and q, i.e, RSA problem is polynomially reduced to factoring. It is conjectured that there is no effective way except factorization to find the e-th roots modulo N. Rabin [33] proposed an encryption function that could be proved to be invertible only by someone who could factor N. This system is similar to RSA, ciptertext c is produced by squaring plaintext m modulo N, i.e,

$$c = m^2 \bmod N$$

where $N = p \cdot q$ and the squaring map is 4-1. So, Rabin finds all four square roots of a ciphertext c.

The most important fact about Rabin encryption scheme is that it is in some sense provably secure in reductionist argument meaning that if someone breaks the scheme and finds the plaintext m from ciphertext c, then he is able to factor N.

- It is the first public key encryption scheme to be proposed with a reductionist security argument.
- Since it is deterministic encryption, it does not satisfy IND-CPA security notion.
- As RSA encryption, it is also vulnerable to chosen ciphertext attacks, namely if an adversary gets m, he is able to factor N.

2.3.3 Goldwasser-Micali Encryption Scheme

Goldwasser and Micali [19] introduced probabilistic encryption and proposed a scheme which was proven secure in the sense of semantic security assuming the intractability of the quadratic residuosity problem which is defined as follows:

Definition 2.3.5 (Quadratic Residues) *Let N be any positive integer and $a \in \mathbb{Z}_N^*$. a is said to be a quadratic residue modulo N if there exists an $x \in \mathbb{Z}_N^*$, such that $x^2 \equiv a \bmod N$ and x is a square root of $a \bmod N$. If no such x exists, then a is called a quadratic nonresidue modulo N. We denote the set of all quadratic residues modulo N by Q_N, and the set of all quadratic nonresidues by $\bar{Q_N}$.*

Definition 2.3.6 (Legendre Symbol) *Let $N = p$ be an odd prime, a is an integer such that $gcd(N, a) = 1$. Then the Legendre symbol is defined to be*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & if \ \ a \in Q_p \\ -1, & if \ \ a \in \bar{Q}_p \end{cases}$$

Lemma 2.3.7 *Let p be an old prime and $a, b \in \mathbb{Z}_p^*$. Then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Definition 2.3.8 (Jacobi symbol) *The Jacobi symbol is an extension of the Legendre symbol for composite $N = p \cdot q$ defined as*

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$

where p, q are prime numbers and $a \in \mathbb{Z}_N^*$.

Remark 2.3.9 *Given a and N (with unknown factorization), it is possible to compute the Jacobi symbol of a in polynomial time.*

Definition 2.3.10 (Quadratic Residuosity Problem: QRP) *Given $N = p \cdot q$ and $a \in \mathbb{Z}_N^*$ with*

$$\left(\frac{a}{N}\right) = 1$$

decide whether a is quadratic residue mod N.

Quadratic Residuosity Assumption: Given $N = p \cdot q$ with unknown factorization, the QRP is intractable.

Remark 2.3.11 *If p, q are known and $N = p \cdot q$, then there exists a polynomial time algorithm to decide whether a is quadratic residue mod N.*

G-M encryption scheme works on bits. To encrypt $m \in (0, 1)$, one first selects a quadratic nonresidue $y \in \mathbb{Z}_N$ satisfying $\left(\frac{y}{N}\right) = 1$. Then choosing a random value $r \in \mathbb{Z}_N^*$ and produces the challenge ciphertext

$$c = y^m r^2 \mod N.$$

The receiver decides the plaintext m is 0 if c is a square, otherwise it must be 1 using the factors of $N = p \cdot q$.

Remark 2.3.12 *Although, G-M encryption scheme is the first probabilistic encryption scheme satisfiying semantic security, efficiency does not hold because of ciphertext expansion.*

2.3.4 ElGamal Encryption Scheme

Before we give the description of the scheme, we recall some mathematically hardness assumptions and relations between them.

Definition 2.3.13 (The Discrete Logarithm Problem: DLP) *Let $\mathbb{G}$ be a finite, multiplicative group of order q with a generator g. The DLP asks x given a group element $h = g^x$.*

The Discrete Logarithm Assumption: The DLP is intractable in the underlying group $\mathbb{G}$. We formally show this via adversarial view as the following: For any polynomial time adversary A, the probability that

$$Pr[x = A(\mathbb{G}, q, g, h) : g^x = h]$$

is negligible.

Definition 2.3.14 (The Computational Diffie-Hellman Problem: CDH) *Let $\mathbb{G}$ be a finite, multiplicative group of order q with a generator g. Given two elements of $\mathbb{G}$, g^x and g^y, it is required to find g^{xy}.*

The Computational Diffie-Hellman Assumption: The CDH problem is intractable in the underlying group $\mathbb{G}$.

Definition 2.3.15 (The Decisional Diffie-Hellman Problem: DDH) *Let $\mathbb{G}$ be a finite, multiplicative group of order q with a generator g. Given three elements of $\mathbb{G}$, (g^x, g^y, g^z), it is asked to find whether $xy = z \mod q$.*

The Decisional Diffie-Hellman Assumption: The DDH problem is computationally hard in the underlying group $\mathbb{G}$.

This assumption can also be represented in terms of probabilities as follows: Let D be a polynomial time algorithm which is designed for deciding whether a three-tuple is a DDH

tuple, and let

$$Pr[D(g^x, g^y, g^{xy}) = 1] - Pr[D(g^x, g^y, g^z) = 1]$$

where x, y, and z are selected randomly from $\mathbb{Z}_q$ is defined as the advantage of D in distinguishing a DDH tuple distribution from a random one. The DDH assumption assumes that this advantage is negligible.

Remark 2.3.16 *The three assumptions are related with each other such that if there exists a polynomial time algorithm A solving DLP with non-negligible probability, then using this algorithm as a subroutine, one can construct an efficient algorithm B for CDH problem and moreover, running B as a subroutine, there exists an algorithm C for DDH problem which solves it in a polynomial amount of time. Hence, we decide that DDH assumption is the strongest one.*

We review the ElGamal encryption scheme [16] whose security is based on the DLP. Let $\mathbb{G}$ be a finite cyclic group of order q with generator g. The secret and the public keys are x and $y = g^x$, respectively. To encrypt $m \in \mathbb{G}$, the sender chooses a random $r \in \mathbb{Z}_q$ and produces the challenge ciphertext

$$c = (c_1, c_2) = (g^r, y^r \cdot m).$$

The receiver gets m by calculating $c_2/{c_1}^x$.

We note that it is hard to find x, given $y = g^x$ under the discrete logarithm assumption but this does not guarantee the security of semantic notion sense. If we work on some groups such as for a prime p, $\mathbb{Z}_p^*$, where DLP holds, then there exists a polynomial time adversary violating the semantic security as follows:

- Adversary selects two messages m_0 and m_1 of equal length such that one of them is quadratic residue and sends them to the challenger.
- Given the challenge ciphertext $c = (c_1, c_2)$ where $c_1 = g^r$ and $c_2 = y^r m_b$, it is easy to distinguish which m is chosen. If c_1 or y are quadratic residues, then at least r or x must be even, hence y^r is also quadratic residue. So, upon receiving c_2, one can determine whether m_b is quadratic residue. If y^r is a not a residue but c_2 is residue, then m_b is

also a non residue. Hence, the semantic security of the scheme fails under the discrete logarithm assumption.

We state a well known theorem about the semantic security of the ElGamal encryption scheme [23].

Theorem 2.3.17 *Under the DDH assumption, ElGamal encryption scheme is semantically secure.*

Proof. The proof is done by using the reductionist argument such that assuming there exists a polynomial time adversary A breaking the scheme, then we can construct a polynomial time algorithm B using A as a subroutine and solve the DDH problem which is a contradiction under the DDH assumption, hence we conclude that this scheme is semantically secure.

The inputs to B is $(\mathbb{G}, q, g_1, g_2, g_3, g_4)$, where $(g_1,\ g_2)$ is the public key. B gives the public key to A and asks to get messages $(m_0,\ m_1)$ of equal length. B selects a bit $b \in (0, 1)$ randomly, produces the challenge ciphertext $c = (g_3,\ g_4 \cdot m_b)$ and runs $A(pk,\ c)$ to obtain b' of a guess for b. Finally, B outputs 1 if and only if $b = b'$. Since the DDH assumption holds in $\mathbb{G}$ and B is a PPT algorithm, we have

$$\left|Pr[B = 1 \mid \text{DDH tuple}] - Pr[B = 1 \mid \text{Random tuple }]\right| \leq \frac{1}{2} + negl.$$

If the input to B is a DDH tuple, then we have

$$Pr[B = 1 \mid \text{DDH tuple}] = Pr[\text{Success of A in breaking the scheme}].$$

When DDH tuple occurs, we have $g_2 = g_1^x,\ g_3 = g_1^r$ and $g_4 = g_1^{xr} = g_2^r$ for some $x, r \in \mathbb{Z}_q$. But this is exactly ElGamal encryption scheme in real life so B outputs 1 if and only if A succeeds in breaking the scheme. To complete the proof, we show that

$$Pr[B = 1 \mid \text{Random tuple}] = \frac{1}{2}$$

is satisfied. In this case, g_4 is uniformly distributed in $\mathbb{G}$ and it is independent of g_1, g_2 or g_3. So the second component given to A is uniformly distributed in $\mathbb{G}$ and independent of m. Thus, A has no information about b, therefore, there is no way other than predicting with probability $\frac{1}{2}$. ■

Remark 2.3.18 *Like RSA and Rabin encryption schemes, ElGamal encryption scheme is also vulnerable to adaptive chosen ciphertext attacks. When adversary A gets the challenge ciphertext* $c = (c_1, c_2)$*, he can modify it by randomly selecting* m' *and getting* $c' = (c_1,\ c_2 \cdot m')$*. Since this is different from the challenge, he can ask it to the decryption oracle and by dividing the returned answer by* m'*, he can get the plaintext* m*.*

Remark 2.3.19 *Damgard proposed [11] a slight modification of ElGgamal encryption scheme by just adding an exponentiation to ciphertexts to provide security against nonadaptive chosen ciphertext attacks. But it is vulnurable to an IND-CCA2 attacker. In 2008, Desmedt and Duong [13] showed that by employing a data encapsulation mechanism to Damgard's ElGamal scheme resulting in hybrid Damgard's ElGamal encryption and is secure against adaptive chosen ciphertext attacks in the standard model.*

2.3.5 Cramer-Shoup Encryption Scheme

We discuss about the Cramer-Shoup public key encryption scheme which is the first efficient scheme proven to be secure against adaptive chosen ciphertext attacks under the DDH assumption in the standard model. It is an extension of the ElGamal encryption scheme. We summarize the proof techniques below, and inform that all the details and reductions can be found in [9, 22].

2.3.5.1 The Modified ElGamal Encryption

In this section, we review the modified ElGamal scheme and show that it is semantically secure under the DDH assumption.

Let $\mathbb{G}$ be a finite, cyclic group of prime order q meaning that every element of $\mathbb{G}$ except the identity is a generator. Let (g_1, g_2) be two generators and (x, y) be the secret keys randomly chosen from $\mathbb{Z}_q$. The public key is $h = g_1^x \cdot g_2^y$. To encrypt $m \in \mathbb{G}$, one randomly chooses $r \in \mathbb{Z}_q$ and performs the challenge ciphertext:

$$c = (u,\ v,\ e) = (g_1^r,\ g_2^r,\ h^r \cdot m).$$

The receiver with secret key $(x,\ y)$ decrypts c as follows:

$$e/u^x \cdot v^y = h^r \cdot m/(g_1^r)^x \cdot (g_2^r)^y = h^r \cdot m/(g_1^x \cdot g_2^y)^r = m.$$

Theorem 2.3.20 *If the DDH assumption is hard in $\mathbb{G}$, then the modified ElGamal scheme is secure against a CPA attacker.*

Proof. We use the reductionist argument such that if there exists a polynomial time attacker A breaking the semantic security of the modified scheme in non-negligible probability, then we can construct a polynomial time algorithm B which is able to break the DDH assumption by distinguishing a DDH tuple from a random one. B is given $(g_1,\ g_2,\ g_3,\ g_4)$ as input.

$x, y \in \mathbb{Z}_q$ are chosen randomly, $h = g_1^x \cdot g_2^y$ is set as the public key and $(g_1,\ g_2,\ h)$ is given to A. A chooses $(m_0,\ m_1)$ of equal length and sends them to B. B selects one of them, namely m_b and produces the challenge ciphertext $(u,\ v,\ e) = (g_3,\ g_4,\ g_3^x \cdot g_4^y \cdot m_b)$ and send back to A. A guesses a bit b' for b. If $b' = b$, then we decide that $(g_1,\ g_2,\ g_3,\ g_4)$ is a DDH tuple, otherwise, random one.

Claim 2.3.21 *If the input to B is a DDH tuple, then A's view is the same as in the real attack game, i.e,*

There exist $\alpha, r \in \mathbb{Z}_q$ such that:

$$(g_1,\ g_2,\ g_3,\ g_4) = (g_1,\ g_1^\alpha,\ g_1^r,\ g_1^{\alpha r} = g_2^r)$$

holds. Hence, the success probability of A in breaking the scheme is directly related to the DDH assumption which is supposed to be intractable.

Claim 2.3.22 *If the input to B is a random tuple, then b is theoretically hidden from the view of A and the scheme becomes a one time pad encryption, hence the success probability is nothing but* $1/2$ *plus negligible probability.*

Assume B gets a random tuple. Then there exists α, β, r which are randomly chosen from $\in \mathbb{Z}_q$ such that the input $(g_1,\ g_2,\ g_3,\ g_4)$ to B becomes $(g_1,\ g_2 = g_1^\alpha,\ g_3 = g_1^r,\ g_4 = g_1^\beta)$. Another saying of this, there exist r, $r' \in \mathbb{Z}_q$ with $r \neq r'$, $g_3 = g_1^r$ and $g_4 = g_2^{r'}$. Given the public key, $(g_1,\ g_2,\ h)$, it is easily seen that there are exactly q possible pairs $(x,\ y)$ that could be chosen by A. Then we have

$$log_{g_1} h = x + \alpha y.$$

We observe that for every $x \in \mathbb{Z}_q$, there is a unique $y \in \mathbb{Z}_q$ satisfying this equation. So, there are exactly q solutions due to the group order. Let us consider $\mu = g_3^x \cdot g_4^y$ where μ is an arbitrary group element. By similar argument, we have

$$log_{g_1}\mu = r \cdot x + r' \cdot \alpha \cdot y.$$

We see that these form a system of linear equations and has a unique solution in (x, y). But μ is an arbitrary group element so each possible value for μ is possible meaning that A can not guess $g_3^x \cdot g_4^y$ with non negligible probability. It seems like a one-time pad encryption. ■

2.3.5.2 The Reduced Cramer-Shoup Encryption

In this section, we review the reduced Cramer-Shoup encryption scheme and show that it is provably secure against non-adaptive chosen ciphertext attacks under the DDH assumption, however, it is insecure against CCA2 attackers.

Let (g_1, g_2) be two generators of the group $\mathbb{G}$ and $(x,\ y,\ a,\ b)$ be the secret key randomly chosen from $\mathbb{Z}_q$. The public key is $(h,\ c) = (g_1^x \cdot g_2^y,\ g_1^a \cdot g_2^b)$. To encrypt $m \in \mathbb{G}$, one randomly chooses $r \in \mathbb{Z}_q$ and performs the challenge ciphertext:

$$c = (u,\ v,\ e,\ w) = (g_1^r,\ g_2^r,\ h^r \cdot m,\ c^r)$$

On receiving the challenge ciphertext $(u,\ v,\ e,\ w)$, there is a checking mechanism and the receiver checks whether $w = u^a \cdot v^b$. If so, output is $e/u^x \cdot v^y$, else $\perp$.

Correctness is satisfied, since

$$w = c^r = (g_1^a \cdot g_2^b)^r = u^a \cdot v^b$$

and

$$e/u^x \cdot v^y = h^r \cdot m/(g_1^r)^x \cdot (g_2^r)^y = h^r \cdot m/(g_1^x \cdot g_2^y)^r = m.$$

Theorem 2.3.23 *Under the DDH assumption, the scheme is IND-CCA1 secure.*

Proof. To prove this, as in the previous section, we use reductionist argument such that if there exists a polynomial time attacker A breaking the semantic security of the reduced Cramer-Shoup scheme with a nonnegligible success probability, then we can construct a polynomial

time algorithm B which is able to break the DDH assumption by distinguishing a DDH tuple from a random one. The important difference is that A has access decryption oracle and is allowed to have polynomially many queries until getting the challenge ciphertext. B is given $(g_1,\ g_2,\ g_3,\ g_4)$ as input which is either a DDH tuple or a random tuple. A chooses $(m_0,\ m_1)$ of equal length and sends them to B. B selects one of them, namely m_b, produces the challenge ciphertext $(g_3,\ g_4,\ g_3^x \cdot g_4^y \cdot m_b,\ g_3^a \cdot g_4^b)$ and sends it to A. Then, A guesses a bit b' for b. Finally, if $b' = b$, then $(g_1,\ g_2,\ g_3,\ g_4)$ is a DDH tuple, otherwise random one.

Claim 2.3.24 *If the input to B is a DDH tuple, then A's view is the same as in the real encryption scheme.*

If $(g_1,\ g_2,\ g_3,\ g_4)$ is a DDH tuple, we can write $g_3 = g_1^r$ and $g_4 = g_2^r$ for a randomly selected $r \in \mathbb{Z}_q$. Hence, the success probability of A in breaking the scheme is directly related to the DDH problem which is supposed to be intractable.

Claim 2.3.25 *If the input to B is a random tuple, then b is theoretically hidden from the view of A and the scheme becomes a one time pad encryption, hence the success probability of A guessing the true b is about* $1/2$ *plus some negligible probability.*

The proof is similar with the modified ElGamal scheme so we omit it and refer [9, 22] for details, however we discuss below why this scheme is not secure against adaptive chosen ciphertext attacks.

On receiving the challenge ciphertext $(g_3,\ g_4,\ g_3^x \cdot g_4^y \cdot m_b,\ g_3^a \cdot g_4^b)$, A computes

$$log_{g_1} w = a \cdot log_{g_1} g_3 + b \cdot log_{g_1} g_4 \tag{2.1}$$

and from the public key c, A learns that

$$log_{g_1} c = a + b \cdot log_{g_1} g_2. \tag{2.2}$$

From (2.1) and (2.2), A theoratically learns (a, b). Then, in particular, makes a query of the form $(g_1^r,\ g_2^{r'},\ e,\ (g_1^r)^a,\ (g_2^{r'})^b)$ and return m, thus we have;

$$log_{g_1} \frac{e}{m} = x \cdot r + y \cdot r' \cdot log_{g_1} g_2 \tag{2.3}$$

from the public key h, A learns that

$$log_{g_1} h = x + y \cdot log_{g_1} g_2. \tag{2.4}$$

Since (2.3) and (2.4) are linearly independent, A can compute the values of (x, y) and finally decrypt the challenge ciphertext. ■

2.3.5.3 The Full Cramer-Shoup Encryption

In the previous section, we analyse the reduced Cramer-Shoup version and briefly show that it satisfies IND-CCA1 security under the DDH assumption but vulnerable against an CCA2 attacker. In order to make the scheme provably secure against adaptive chosen ciphertext attacks in the standard model, a public collision-resistant hash function H which hashes arbitrary length strings to Z_q is used. Briefly, the full Cramer-Shoup encryption scheme is as follows:

Encryption:

- $pk = (g_1,\ g_2,\ h = g_1^x \cdot g_2^y,\ c = g_1^a \cdot g_2^b,\ d = g_1^{a'} \cdot g_2^{b'},\ H)$
- $sk = (x,\ y,\ a,\ b,\ a',\ b')$
- To encrypt m, we choose random $r \in \mathbb{Z}_q$ and set the challenge ciphertext

  $$c = (g_1^r,\ g_2^r,\ h^r \cdot m,\ ((c \cdot d^{\alpha}))^r)$$

  where $\alpha = H(g_1^r,\ g_2^r,\ h^r \cdot m)$.

Decryption:

- To decrypt the challenge ciphertext $c = (u,\ v,\ e,\ w)$, there is a checking mechanism: if $u^{a+\alpha a'} \cdot v^{b+\alpha b'} = w$ where $\alpha = H(u,\ v,\ e)$ then output is valid.
- Output is $e/u^x \cdot v^y$, else $\perp$.

Theorem 2.3.26 *Under the DDH assumption, the Full Cramer-Shoup encryption scheme is secure against adaptive chosen ciphertext attacks in the standard model.*

Proof. Given a PPT algorithm A attacking the scheme with nonnegligible success probability, we construct an adversary B violating the DDH assumption as follows:
B is given $(g_1,\ g_2,\ g_3,\ g_4)$ as an input. The algorithm selects $(x,\ y,\ a,\ b,\ a',\ b')$ from $\mathbb{Z}_q$ and sets $(g_1,\ g_2,\ h = g_1^x \cdot g_2^y,\ c = g_1^a \cdot g_2^b,\ d = g_1^{a'} \cdot g_2^{b'},\ H)$ as the public key. Then it runs A to produce $(m_0,\ m_1)$ of equal length. B selects a bit b and gives the challenge ciphertext $(u,\ v,\ e,\ w) = (g_3,\ g_4,\ g_3^x \cdot g_4^y \cdot m_b,\ g_3^{a+\alpha a'} \cdot g_4^{b+\alpha b'})$. Then A guesses a bit b' for b. Finally, B outputs 1 if and only if $b = b'$. We see from the previous sections that if B is given a DDH tuple, then A's view is the same as in an execution of the real full Cramer-Shoup encryption scheme. Hence, we show that if B is given a random tuple, then the bit b is theoratically hidden from A's view, so A has no information about the bit chosen by B. From the public key, A learns

$$log_{g_1} c = a + b \cdot log_{g_1} g_2$$

and

$$log_{g_1} d = a' + b' \cdot log_{g_1} g_2.$$

We write $g_3 = g_1^r$, $g_4 = g_2^{r\prime}$ and when given the challenge ciphertext, denoted by

$$(g_3,\ g_4,\ e^* = g_3^x \cdot g_4^y \cdot m_b,\ w^* = g_3^{a+\alpha a'} \cdot g_4^{b+\alpha b'}).$$

A learns

$$log_{g_1} w^* = (a + \alpha \cdot a') \cdot r + (b + \alpha \cdot b') \cdot log_{g_1} g_2 \cdot r'.$$

Hence, we have three cases to be considered about the decryption oracle queries. We also note that it is not allowed to query the challenge ciphertext to the oracle.

- if $(u,\ v,\ e) = (u^*,\ v^*,\ e^*)$, and $w \neq w^*$ then the query is always rejected because of the checking mechanism.
- if $(u,\ v,\ e) \neq (u^*,\ v^*,\ e^*)$ but the the hash values are the same, this happens with negligible probability because of the collision resistant property of H.
- if $\alpha' = H(u,\ v,\ e) \neq H(u^*,\ v^*,\ e^*) = \alpha$. Then, with a careful analysis, we have more unknowns than linear equations in these unknowns.

■

CHAPTER 3

SECURITY PROOFS BASED ON THE RANDOM ORACLE MODEL AND GAME HOPPING TECHNIQUE

"Education is the most powerful weapon you can use to change the world."

Nelson Mandela

In this chapter, we discuss the random oracle model- a tool for security analysis of cryptographic schemes- which has been proposed as an alternative to the standard model. Then we give game hopping technique since sometimes security proofs in cryptography may be constructed as sequence of games. We give some concrete illustrations of public key encryption schemes and their security proofs that utilize random oracles and game hopping.

3.1 The Random Oracle Model

The random oracle model was introduced by Bellare and Rogaway [4] as an alternative to the standard counterpart. It is well accepted as a method for proving security of public key encryption because in the standard model, secure schemes require more complex operations whereas in the random oracle model, the use of hash functions usually is sufficient. In this model, hash functions are modeled as random oracles which are not actually possible in the real world however, due to this relaxation, one may construct much more efficient schemes. ROM assumes that there exists a public, randomly chosen function H which is evaluated only by quering an oracle; given x as input, it returns $H(x)$ as an output and it ensures that queries and responses must be consistent meaning that if the same query is asked later in the future then the same answer has to be given.

The main utilization of ROM while analysing cryptographic schemes and their security proofs is that it provides simplicity and enables the design of more efficient schemes than those in the standard model mentioned in the previous sections. In the random oracle model, secure hash functions would share many properties with the random functions and they are modeled truely random functions which is a heuristic argument. However, random oracles are instantiated in the real world with concrete hash functions.

In the ROM, hash functions are modeled as random functions meaning that the outputs are truly random so the knowledge of the outputs for some inputs are useless for the knowledge of the outputs of some other inputs. Hence, it is more convenient to think generating outputs for H on the fly as needed. We assume that the function is defined by input-output table. When x is queried on H, first it is checked to be in the table and if so, then the corresponding y is given as an output otherwise, a random y is chosen, returned as the output and stored in the table in case whenever the same x is queried then the same y is given as an output to keep consistancy. In the real world, however, the on the fly process is impossible.

3.1.1 Security Proofs in the Random Oracle Model

Unlike the security proofs in the standard model, the random oracle model enables different proof techniques mainly because in addition to all parties in the system, adversary is also given access to the RO which means we observe the adversary's behaviour during the attack process. Random oracle proofs are not considered to be rigorous mathematical proofs and indeed it is shown that there exist schemes which can be proven in the random oracle model but completely insecure in real world such as in [8]. Probably, this is why the use of ROM is objected by a number of cryptographers such as Menezes and Koblitz [24]. But this does not make ROM completely useless because at least it guarantees that there are no inherent design flaws and this is certainly better than providing no proof at all.

We stress that, it is still preferable to use a scheme secure in the standard model even if it is slightly less efficient as opposed to the random oracle counterpart.

We emphasize that random oracle is a hypothetical "magic" box that is assumed to have the following two properties:

- It produces truly random outputs.

- For each input, it gives the same output.

The objections on ROM comes from the fact that random oracles do not exist in the real world, and a simulator needs to see the queries of the adversary which is not so realistic. Also it is assumed that the simulator can set the output of the random oracle as it wishes. This is called *programmability* yet it is not realistic, neither.

When proving security of public key encryption schemes in the ROM, we assume there is an efficient polynomial time algorithm A breaking the scheme, then we try to construct a polynomial time algorithm A' which violates the underlying cryptographic hard assumption. This procedure is called ***reduction*** as in the standard version. The random oracle H which is given to the adversary A, must be simulated, i.e, A' sees the queries and answers them as it likes, these answers must be correctly distributed and uniformly random in order not to realise for A whether it is in the real attack game or in a simulated one.

An Important Remark on the Validity of the Random Oracle Model: In the cryptography literature, as we point out there are two major objections about the validity of the random oracle model originating from the usage of hash functions to simulate random oracles:

- Programmability property is not possible in the real world:

  Since in the real world it is impossible to set the output of an hash function to a specific value, this is indeed a sound objection. Because most of the time, a concrete hash function (e.g. SHA-1, SHA-2) is used and the result is immediately set as soon as the input is given. Some sort of programmability would be possible in a highly hypothetical environment where hash families could be used instead of a concrete hash function.

- In the real world, it should be impossible for any other entity to see the hash evaluations that the adversary makes:

  Unlike the previous one, this objection may not be correct [2]. Note that by arguing such an impossibility, one imposes that the hard problem being reduced cannot be broken by the same breaker as the scheme security of which is being proved. To make this point clear, suppose that we are proving the security of a scheme S by reducing a mathematically hard problem P to S. In such a reduction, we need to provide a breaker B_P for P assuming that we have a breaker B_S for S. If we do not allow B_P to see the hash evaluations that B_S makes, this implies the restriction that B_P cannot be designed by

the same entity who designed B_S. However, this is an unnecessary restriction because it must be sufficient to show that if S can be broken so can P, no matter who designs the breaker algorithms B_S and B_P. So, since B_S and B_P can possibly be designed by the same entity (at least we cannot prohibit this), the hash evaluations of B_S should be visible to B_P.

In the next sections, we present the random oracle methodology in details and game hopping technique in order to prove security of the schemes with some public key illustrations.

3.1.1.1 CPA Secure RSA Encryption in the ROM

The first scheme we will discuss is an IND-CPA secure version of RSA based encryption scheme. The scheme is defined by the following three algorithms:

- **Setup**: Let N be an RSA number and e, d is an RSA key pair. Let $H : \mathbb{Z}_N^* \rightarrow \{0,1\}^\ell$ be a hash function.
- **Encrypt**(m): Given a message $m \in \{0,1\}^\ell$, a random $r \in \mathbb{Z}_N^*$ is chosen and m is encrypted as:
$$c = (r^e \bmod N,\ H(r) \oplus m)$$
- **Decrypt**(c): Given a ciphertext $c = (c_1, c_2)$,
$$m = H(c_1^d) \oplus c_2$$

Theorem 3.1.1 *If the RSA problem is hard, then the scheme above is IND-CPA secure in the random oracle model.*

Proof. The proof is given in [23] and proceeds as follows: A reduction from breaking the scheme to solve the RSA problem is presented. Suppose there exists an adversarial algorithm A that can break the scheme. We will construct another algorithm B that solves the RSA problem using A as a subroutine. Algorithm B will simulate an attack game for the successful attacker A given. The steps of B is explained in Algorithm 1.

The core idea of the proof is as follows: If t is not queried, then $H(t)$ is considered to be truly random, hence, c_2 is like a one-time pad encryption. If it is queried, then t must be

Algorithm 1 $B(N, e, y)$

1: Choose $s \in_R \mathbb{Z}_N^*$. Consider $t = y^{1/e}$ which we do not actually know, and due to programmability, let $H(t) = s$.
2: Simulate IND-CPA game for A as follows:
3: Provide the public key (N, e) to A.
4: Maintain table T for random oracle queries, initially empty.
5: Whenever A makes a random oracle query q at FIND stage, check whether q is already queried before. If so, return the same output. Otherwise randomly choose $H(q)$, save $(q, H(q))$ to table T and return $H(q)$ to A.
6: After FIND stage is over A outputs two messages m_0, m_1.
7: Randomly select a bit b and give the challenge ciphertext $c = (c_1, c_2) = (y, s \oplus m_b)$
8: Whenever A makes a random oracle query q at GUESS stage, check whether q is already queried before. If so, return the same output. Otherwise randomly choose $H(q)$, save $(q, H(q))$ to table T and return $H(q)$ to A.
9: After the game is over (A outputs its guess b') search table T to see whether $q^e = y$, if so, output q as the answer otherwise return $\perp$.

the answer we are looking for, i.e. the answer of the RSA problem. So we can argue that Algorithm B solves the RSA problem if A can break the scheme. This contradicts with the RSA assumption, so the scheme is IND-CPA secure. ■

3.1.1.2 Security of Hashed ElGamal Encryption

We look at a similar but slightly more complicated example random oracle proof. The reduction will be similar to that of the previous section but there will be a probabilistic argument. This time, the encryption scheme is as follows:

- **Setup**: Let g be a generator of some prime order group $\mathbb{G}$. Let x be the private key and $h = g^x$ be the public key. Let $H : \mathbb{G} \to \{0,1\}^\ell$ be a hash function.
- **Encrypt**(m): Given a message $m \in \{0,1\}^\ell$, a random $r \in \mathbb{G}$ is chosen and m is encrypted as:

$$c = (g^r,\ H(h^r) \oplus m)$$

- **Decrypt**(c): Given a ciphertext $c = (c_1, c_2)$,

$$m = H(c_1^x) \oplus c_2$$

Theorem 3.1.2 *Under the CDH assumption, the scheme is IND-CPA secure in the random oracle model.*

Proof. In order to prove this theorem, we give a reduction from breaking the scheme to solve the CDH problem [2]. Similar to the previous proof, we assume that we have an adversarial algorithm A that can break the scheme above and construct another algorithm B that solves the CDH problem using A as a subroutine. Algorithm B will be similar to that of the previous proof except that we cannot check the queries whether they correspond directly to the answer of the CDH problem we are looking for. However, we note that when we set the parameters g^x and g^r to the input of the CDH problem g^a and g^b respectively, if the attacker is successful in breaking the scheme this means that it must have queried the oracle with g^{ab} somewhere in its execution. So, one of the queries consists of the answer of the CDH problem. Because otherwise, the ciphertext part c_2 is like a one-time pad due to the truly randomness assumption of random oracles. Hence, at the end of the game simulation, algorihtm B selects one of the queries randomly and returns it as the output. The probability of this output to be correct is $(1/q)\epsilon$ where q is the number of queries performed, and ϵ is the success probability of the adversary. Since the number of queries is polynomially bounded, the probability is divided into polynomial factor which is still non-negligible. Hence, the scheme is IND-CPA secure.

■

We note that in the proof of the IND-CPA RSA scheme, the success probability is preserved since we can explicitly test whether a random oracle query is the one that consists of the answer of the RSA problem, but we cannot do the same check in the proof of IND-CPA ElGamal scheme, but fortunately returning one of the queries still works since it decreases the success probability only in polynomial factor.

3.1.1.3 Existentially Unforgeable RSA Signature

In this section, we present a secure RSA-based signature scheme in the random oracle model. First, let us consider the plain RSA signature scheme:

- **Setup**: Let N be an RSA number and (e, d) is an RSA key pair.
- **Sign**(m): Given a message $m \in \mathbb{Z}_N^*$, m is signed as: $s = m^d \bmod N$.
- **Verify**(s): Given a signature (m, s), verification equation is: $m = s^e \bmod N$.

Unfortunately, this is not considered as a secure signature scheme because one can forge a message-signature pair by simply choosing a signature s randomly and computing the corresponding message m as $s^e \bmod N$.

Indeed, the most widely accepted security definition for signature schemes is as follows:

Definition 3.1.3 (Existential unforgeability:) *A signature scheme is existentially unforgeable under an adaptive chosen message attack if there exists no polynomial time algorithm that can output a valid message-signature pair given access to a signature oracle.*

So, according to this definition, the scheme above is not existentially unforgeable. However, it is possible to construct a secure signature scheme that is a modified version of the basic RSA signature scheme using a hash function as follows:

- **Setup**: Let N be an RSA number and (e, d) is an RSA key pair. Let $H : \mathbb{Z}_N^* \to \{0,1\}^\ell$ be a hash function.
- **Sign**(m): Given a message $m \in \{0,1\}^\ell$, m is signed as:

$$s = H(m)^d \bmod N.$$

- **Verify**(s): Given a signature (m, s), verification equation is

$$H(m) = s^e \bmod N.$$

The following theorem is proved in [23]

Theorem 3.1.4 *Under the RSA assumption, the modified RSA signature scheme is existentially unforgeable under a no-message attack in the random oracle model.*

Proof. The proof proceeds similar to the proof of the RSA encryption scheme. We construct an algorithm B for solving the RSA problem assuming that we have an algorithm A that can

forge a signature pair. Algorithm B is constructed as follows: Given an RSA problem instance (N, e, y), it gives A the public key (N, e). Whenever A makes random oracle queries, B responds with random values. Except that for a randomly selected query, it responds with y instead of a random value. So, when the simulation is over, and A outputs a forgery (m, s), B outputs s. Note that s is the correct answer of the RSA problem, i.e. $y = s^e \bmod N$ with a probability $(1/q)\epsilon$ where q is the number of random oracle queries and ϵ is the success probability of algorithm A. Because A must have queried m to the random oracle since otherwise $H(m)$ remains truly random and s cannot be determined thus cannot be included in a forgery. So, since a polynomially many random oracle queries are allowed, and ϵ is assumed to be non-negligible, the success probability of algorithm B is also non-negligible which contradicts the RSA assumption. So the scheme is existentially unforgeable under a no-message attack in the random oracle model. ■

We show that the same scheme is indeed existentially unforgeable under an adaptive chosen message attack in the random oracle model.

Theorem 3.1.5 *If the RSA problem is hard, then the modified RSA signature scheme above is existentially unforgeable under an adaptive chosen message attack in the random oracle model.*

Proof. The proof proceeds same as the proof of the no-message case except that the adversary must be provided with a signature oracle. This signature oracle can be simulated by using the programmability feature of the random oracle. When the adversary A requests a signature on message m, B sets $H(m)$ to be $s^e \bmod N$ for a randomly selected s and returns s to A. We note that B does not have to know d explicitly, and since it sets $H(m)$ it can respond to later random oracle queries consistently with the previous ones. Together with the previous construction, this addition is sufficient to complete the proof. ■

3.2 Game Hopping Technique

One of the most popular techniques used in security proofs is game hopping. In this method, we construct different versions of the security game played between the adversary and the challenger. Typically, the first game is the original security game usually called G_0. The idea is to start with G_0 , and slightly modify it into a number of games satisfying the following:

- Successive games are indistinguishable from the view of the adversary and this indistinguishability is shown by relating them to the usual underlying mathematically hard problems.

- Adversary gains no information in the last game, meaning that its success probability is $1/2$.

By showing these two properties, one proves that the view of the adversary in the original game and the last game are indistinguishable, therefore, the success probability in the original attack game is related to the success probability in the last game which acts like a one-time pad, thus must be negligible due to transitivity.

In order to illustrate this idea, we present two different examples which are CPA-secure in the standard model.

3.2.1 Security Analysis of ElGamal Encryption

First, we briefly recall the ElGamal encryption scheme.

- **Setup**: Let g be a generator of some prime order group $\mathbb{G}$. Let x be the private key and $h = g^x$ be the public key.

- **Encrypt**(m): Given a message $m \in \mathbb{G}$, a random $r \in \mathbb{Z}_q$ is chosen and m is encrypted as:

$$c = (g^r, h^r \cdot m)$$

- **Decrypt**(c): Given a ciphertext $c = (c_1, c_2)$,

$$m = c_2 / c_1^x.$$

Now, we briefly explain the game hopping proof of the CPA-security of the El Gamal encryption scheme in the standard model.

Theorem 3.2.1 *Under the DDH assumption, the ElGamal encryption scheme is IND-CPA secure in the standard model.*

Proof. We first consider the original CPA attack game Game 0 between an adversary A and a challenger C. Game 0 proceeds as follows:

Game 0 :

1. *C runs the setup algorithm and provides the public key to A.*
2. Find Stage: *A chooses two messages* (m_0, m_1) *of equal length and sends them to C.*
3. Challenge: *C selects a random bit b and encrypts* m_b *as* $c^* = (g^r, h^r \cdot m_b)$.
4. Guess: *A guesses* b' *for b.*

Next, with a small change, we define a new game Game 1 same as Game 0 except in the challenge ciphertext C sends $c^* = (g^r, g^z \cdot m_b)$ where z is randomly chosen from $\mathbb{Z}_q$. Now, we argue that the adversary cannot distinguish its view in games Game 0 and Game 1 depending on the DDH assumption. Because note that knowing g^r and $h = g^x$ the adversary needs to distinguish $h^r = g^{xr}$ and the random value g^z which corresponds exactly the DDH decision problem. What remains is that the success probability of the attacker in Game 1 is information theoretically $1/2$ since g^z is randomly selected from a uniform distribution over $\mathbb{G}$ which makes it like a one-time pad. This concludes the proof. ■

3.2.2 Security Analysis of Hashed ElGamal Encryption

In this section, we discuss the hashed version of the ElGamal encryption scheme which we already defined. However, this time, we prove the security of the scheme in the standard model under the DDH and entropy smoothing assumptions. First, we define entropy smoothing.

Definition 3.2.2 (Entropy smoothing:) *Let* $\mathcal{H} = \{H_k\}_{k \in K}$ *be a family of hash functions where each* $H_k : \mathbb{G} \to \{0,1\}^\ell$. $\mathcal{H}$ *is called entropy smoothing if there exists no polynomial time adversary that can effectively distinguish between the pairs* $(k, H_k(x))$ *and* (k, h)*, where* $k \in K$*,* $x \in \mathbb{G}$ *and* $h \in \{0,1\}^\ell$.

The intution behind entropy smoothness is that the range of an arbitrary hash function from the hash family is uniformly distributed. We present the semantic security of hashed ElGamal encryption scheme in the standard model using game hopping technique [37].

Theorem 3.2.3 *Under the DDH assumption and entropy smoothing property of the hash family, hashed ElGamal encryption scheme is CPA-secure in the standard model.*

Proof. Let Game 0 be the original CPA attack game.

Game 0 :

1. *C runs the setup algorithm and provides the public key to A.*

2. Find Stage: *A chooses two messages* (m_0, m_1) *of equal length and sends them to C.*

3. Challenge: *C selects a random bit b and encrypts* m_b *as* $c^* = (\ g^r\ ,\ H(h^r) \oplus m_b\ )$.

4. Guess: *A guesses* b' *for b.*

Let Game 1 be the same as Game 0 except a small change in the challenge, $c_2 = H(g^z) \oplus m_b$ instead of $H(h^r) \oplus m_b$ where z is randomly chosen from $\mathbb{Z}_q$. Note if a polynomial time adversary can distinguish its views in Game 0 and Game 1 with a non-negligible success probability, one can construct an efficient algorithm that can decide DDH problem which contradicts the hardness assumption of DDH.

Let Game 2 be the same as Game 1, except that in the challenge, $c_2 = r \oplus m_b$ instead of $H(g^z) \oplus m_b$ where r is a random element of $\{0,1\}^\ell$. Note that due to the entropy smoothing property of the hash family used in the scheme, no efficient adversary can distinguish between its views in Game 1 and Game 2.

Finally, the success probability of the adversary in Game 2 is information theoretically 1/2, i.e, it behaves like a one-time pad and this concludes the proof. ■

Constructing efficient and provably secure schemes against adaptive chosen ciphertext attacks (i.e, IND-CCA2- which is accepted as the strongest security notion in public key encryption schemes) is one of the main goals of cryptographic community. A lot of work has been done. In this context, we discuss Fujisaki and Okamoto's construction.

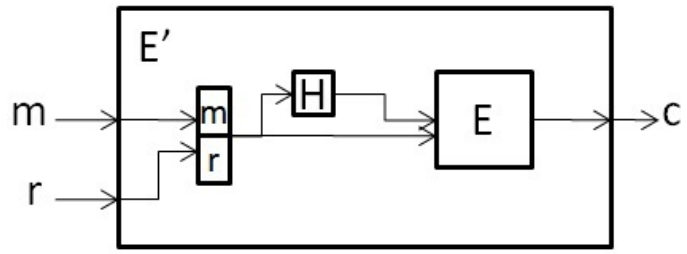

Figure 3.1: Fujisaki-Okamoto encryption operation.

3.3 A Generic Conversion from IND-CPA Security into an IND-CCA2 Security

In late 90s, Fujisaki and Okamoto [17] gave a generic construction from an IND-CPA secure one-way trapdoor function to an IND-CCA2 secure public-key encryption scheme in the random oracle model. We first describe this conversion briefly. Suppose we have an IND-CPA secure public-key encryption scheme $\Pi := (\mathcal{K}, \mathcal{E}, \mathcal{D})$ such that $\mathcal{E} : \{0,1\}^{k+k_0} \times \{0,1\}^l \rightarrow \{0,1\}^n$ and $\mathcal{D} : \{0,1\}^n \rightarrow \{0,1\}^{k+k_0}$ where k, k_0 and n denotes the bit lengths of the message, the random value, and the ciphertext of the new encryption scheme we produce. Also we assume that we have an ideal hash function $H : \{0,1\}^{k+k_0} \rightarrow \{0,1\}^l$. Using these primitives, a new encryption scheme, $\bar{\Pi} := (\bar{\mathcal{K}}, \bar{\mathcal{E}}, \bar{\mathcal{D}})$, is defined as follows:

1. $\bar{\mathcal{K}} := \mathcal{K}(1^{k+k_0})$

2. $\bar{\mathcal{E}} : \{0,1\}^k \times \{0,1\}^{k_0} \rightarrow \{0,1\}^n$ is defined as $\bar{\mathcal{E}}(m, r) = \mathcal{E}(\, m \parallel r,\ H(\, m \parallel r\,))$

3. $\bar{\mathcal{D}} : \{0,1\}^n \rightarrow \{0,1\}^k$ is defined as

$$\bar{\mathcal{D}}(c) = \begin{cases} \mathcal{D}(c)[1:k], & \text{if } c = \mathcal{E}(\,\mathcal{D}(c)\,,\ H(\,\mathcal{D}(c))) \\ \perp, & \text{otherwise.} \end{cases}$$

   where $\mathcal{D}(c)[1:k]$ denotes the first k bits of $\mathcal{D}(c)$.

Encryption and decryption operations of the construction is illustrated in Figures 3.1 and 3.2.

However, the conversion needs a re-encryption which makes it expensive in terms of computational complexity. We propose a shortcut for this construction, where we check the consistency of the ciphertext using the random value instead of requiring re-encryption [1].

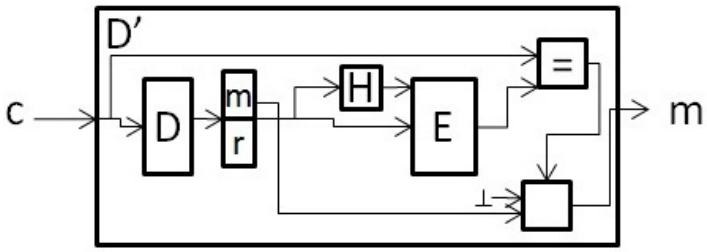

Figure 3.2: Fujisaki-Okamoto decryption operation.

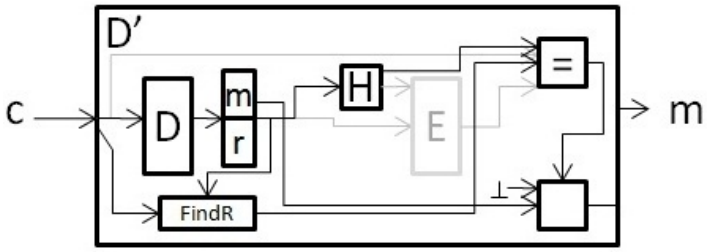

Figure 3.3: The new decryption operation.

3.3.1 Checking Consistency with r

We note that when we perform the encryption operation $c = \bar{\mathcal{E}}(m,\ r) = \mathcal{E}(m \,\|\, r,\ H(m \,\|\, r))$, the first parameter $m \,\|\, r$ and the second parameter $H(m \,\|\, r)$ act as the message and the random value of the encryption function, respectively. Therefore, in cryptosystems where we can calculate the random value from the ciphertext and the message, we can find $H(m \,\|\, r)$ from c and $m \,\|\, r$. Obviously, this requires the encryption function to be injective. Otherwise, a single ciphertext may correspond to more than one random values and it becomes theoretically impossible to find the random value used in the encryption process. Another requirement is the existence of an efficient algorithm FindR which can efficiently find the random value from the ciphertext and the plaintext. Then, we can perform the following alternative decryption instead of the original Fujisaki-Okamoto construction: Suppose that we have an algorithm FindR: $\{0,1\}^n \times \{0,1\}^{k+k_0} \to \{0,1\}^l$ which finds r from c and m where $\mathcal{E}(m,r) = c$. Upon receiving c, we first perform the decryption $\mathcal{D}(c)$ to get $m \,\|\, r$. Then we calculate FindR$(c, m \,\|\, r)$ and compare the result to the hash $H(m \,\|\, r)$. Note that this is equivalent to check whether the encryption $\mathcal{E}(m \,\|\, r, H(m \,\|\, r))$ equals c or not since $\mathcal{E}$ is injective. Thus we get rid of the re-encryption. This idea is illustrated in Figure 3.3.

Verification with r holds if and only if verification with re-encryption holds because

$$c = \mathcal{E}(\mathcal{D}(c)\ ,\ H(\ \mathcal{D}(c)))$$

if and only if FindR$(c,\ \mathcal{D}(c)) = H(\ \mathcal{D}(c))$ by definition of FindR. Here, the crucial point is the existence of the algorithm FindR.

Remark 3.3.1 *The security proof for the new construction is same as that of [17] except the definition of the knowledge extractor which is an algorithm watching the random oracle queries and the decryption oracle queries of the adversary A and extracts the knowledge of this adversary. More specifically, a* $(t, \lambda k)$*-knowledge extractor is a knowledge extractor which has a success probability greater than* $\lambda(k)$ *and runs within at most running time t, and A is* (t, q_H, q_D, ϵ) *adversary which runs in time t, makes* q_H *random oracle queries,* q_D *decryption oracle queries, and has an advantage of at least* ϵ*. In the new construction, the knowledge extractor is shown in Algorithm 2.*

Algorithm 2 Knowledge-Extractor(τ, μ, y, pk)

1: **for** q_H times **do**
2: **if** $H_i =$ FindR(c, h_i)
3: **then** $x \leftarrow h_i[1:k]$ **and break**
4: **else** $x \leftarrow \perp$
5: **return** x

We note that in the original Fujisaki-Okamoto construction, knowledge extractor was requiring a re-encryption instead of the line $H_i =$ FindR(c, h_i). This change makes no difference in terms of the security proof since we do nothing but check the same predicate, namely the consistency of the plaintext and the ciphertext. In the original construction, this is done by encrypting h_i with H_i and checking whether we end up with the same ciphertext, however in the new construction, we use the ciphertext and h_i to guess a candidate for H_i and check whether it holds. Since both the encryption and the FindR functions are available, changing this line in the knowledge extractor definition has no effect on the validity of the proof.

Our method turns out to be less generic since we can apply this method only for public key schemes where the random value can be efficiently found from the ciphertext and the plaintext. Then, we investigate suitability of this new method for several public key encryption schemes [16, 26, 29]. It turns out that this method can be used in Paillier encryption with the same

complexity as the original Fujisaki-Okamoto construction. In the other schemes we consider, our shortcut idea turned out to be inapplicable since calculation of the random value is costly or impossible.

3.3.2 Application of the New Method to Paillier Encryption

In this section, we first briefly mention about Paillier public key encryption scheme, then we discuss how our idea can be applied to the scheme. More details about the scheme can be found in [30, 31].

3.3.2.1 Paillier Encryption Scheme

Key Generation:

- $N = p \cdot q$ where p and q are large primes
- $gcd(N,\ \phi(N)) = 1$
- $|\mathbb{Z}^*_{N^2}| = \phi(N^2) = N \cdot \phi(N)$
- $\mathbb{Z}_N \times \mathbb{Z}^*_N \cong \mathbb{Z}^*_{N^2}$
- order of $(1 + N)$ in $\mathbb{Z}^*_{N^2}$ is N.

Encryption:

- Let $g \in \mathbb{Z}^*_{N^2}$ whose order is N
- To encrypt $m \in \mathbb{Z}_N$, $r \in \mathbb{Z}^*_N$ is chosen
- The challenge ciphertext is

$$c = g^m \cdot r^N \bmod N^2.$$

3.3.2.2 Application to Paillier Encryption Scheme

We find r directly from the ciphertext and the plaintext as follows:

Having c and after getting m from $c = g^m \cdot r^N \bmod N^2$, we compute

$$a = \frac{c}{g^m} = r^N \bmod N^2$$

which implies $a = r^N \bmod N$. We know that $\gcd(N, \phi(N)) = 1$ therefore by using Euclidean Algorithm we can find

$$N \cdot x + \phi(N) \cdot y = 1$$

such that $x, y \in \mathbb{Z}$. Then we get

$$a^x = r^{1-\phi(N)y} = r \pmod{N}.$$

Although it is possible to extract r from c and m, the computational performance of the construction turns out to be the same as re-encryption since it performs 2 modular exponentiations. The idea of checking consistency by using r works at least as good as checking with re-encryption. However, there is a strong intuition that there may exist variants of the existing schemes where the random element of the encryption function can be calculated from the ciphertext and the plaintext. If we apply the new construction idea to such a scheme, we end up with an IND-CCA2 secure scheme in the random oracle model more efficiently compared to the original Fujisaki-Okamoto construction.

CHAPTER 4

CONSTRUCTIONS OF IND-CCA SECURE PUBLIC KEY ENCRYPTION SCHEMES

"Opinion is the medium between knowledge and ignorance."

Plato

In this chapter, we first review some constructions of public key encryption schemes provably secure against chosen ciphertext attacks under some mathematically hard problems. We investigate these constructions since proposing a scheme with a security proof against chosen ciphertext attacks, especially adaptive one, is one of the main goals of cryptography. We mainly focus on the immunization methods proposed by Zheng-Seberry [39], especially the one with ElGamal signature adaptation. We modify this construction by adapting Schnorr signature and obtain a more efficient encryption scheme. Moreover, we also give a formal proof of IND-CCA2 security in the random oracle model.

4.1 Damgard's Scheme

Damgard [11] introduced practical approaches to constructing public key cryptosystems secure against chosen ciphertext attacks and proposed a scheme based on the Diffie Hellman / ElGamal public key cryptosystem. The security of the scheme is based on the intractability of computing discrete logarithms in finite fields but it is insecure against adaptive chosen ciphertext attacks, i.e, IND-CCA2- the strongest security notion. We briefly discuss the scheme as follows:

Let p be a n-bit prime, where n is the security parameter and g be a generator for $\mathbb{Z}_p^*$.

Suppose that Bob, B, wants to send m in secret to Alice, A, with A's public key pair (y_{A_1}, y_{A_2}) where $y_{A_1} = g_{A_1}^{x}$, $y_{A_2} = g^{x_{A_2}}$ such that (x_{A_1}, x_{A_2}) is the secret key pair of A chosen at random from $[1, p-1]$.

Encryption:

- B chooses a random $r \in [1, p-1]$.
- B creates the challenge ciphertext $c = (c_1,\ c_2,\ c_3) = (g^r,\ y_{A_1}^r,\ y_{A_2}^r \oplus m)$.

Upon receiving c, the decryption algorithm works as follows:

Decryption:

$$D(x_{A_1},\ x_{A_2},\ c_1,\ c_2,\ c_3) = \begin{cases} c_1^{x_{A_2}} \oplus c_3, & if\ c_1^{x_{A_1}} = c_2 \\ \perp, & otherwise \end{cases}$$

The scheme seems to be secure against nonadaptive chosen ciphertext attacks since, given $(g,\ y_{A_1})$, it is hard to generate $(g^r,\ y_{A_1}^r)$ without first choosing r. Hence, for the adversary it is hard to generate a valid ciphertext passing the checking step unless he already knows m. Although the simplicity of the design and security against CCA1 attackers, it is insecure against adaptive chosen ciphertext attacks which is the most severe attack type. Given $c = (c_1,\ c_2,\ c_3)$, an attacker A can choose a random message m_r, calculate $m_r \oplus c_3$ and asks the decryption algorithm with the modified ciphertext c'. The oracle answers $m' = m \oplus m_r$ and A gets the challenge ciphertext m by computing $m' \oplus m_r$. To resist this attack and to have more secure schemes, Zheng and Seberry proposed some methods.

4.2 Zheng-Seberry Encryption Schemes

Zheng and Seberry [39] proposed three immunizing methods to make public key encryption schemes secure against adaptive chosen ciphertext attacks by appending a tag which is related to the message to each ciphertext. These methods are different from each other at the point of tag generation. The first method is based on the use of one-way hash functions, the second

on the use of universal hash functions and the third on the use of digital signature schemes. In this section, we deal with only two of these three methods:

- C_{owh}: Using a one-way hash function
- C_{sig}: ElGamal digital signature adaptation

4.2.1 C_{owh} Public Key Encryption Scheme

Suppose that Bob, B, wants to send a n-bit messsage m in secret to Alice, A, with A's public key $y_A = g^{x_A}$ where x_A is the secret key of A. The encryption and the decryption procedures are as follows:

Encryption:

- r is chosen randomly from $[1, p-1]$.
- We produce ciphertext $(c_1,\ c_2)$ such that $c_1 = g^r \bmod p$ and $c_2 = G(y_A^r \bmod p) \oplus (m \parallel H(m))$ where G is a cryptographically strong pseudo-random string generator expanding a relatively short random input into an output of desired length and H is a one-way hash function which compresses arbitrarily long input strings into ℓ-bit output strings.

Decryption:

- $r' = c_1^{x_A} \bmod p$ is calculated.
- $w = c_2 \oplus G(r')$ is found.
- parse the first n bits of w as m' and the remaining as t'.
- if $H(m') = t'$ then output m', otherwise output $\perp$.

They show that C_{owh} satisfies IND-CPA security notion under the Diffie-Hellman assumption, and in order to prove security against adaptive chosen ciphertext attacks, they introduce *sole-samplability* security notion. Informally, it means that there is no other way to generate

ciphertext y than to pick a message x first and compute $y = E(x)$, i.e., there is no way to generate valid ciphertexts without knowing the underlying plaintexts. This makes the decryption oracle useless since the plaintext which is queried to the oracle is already known. Formally, they also prove that if a scheme is sole-samplable, then it is IND-CPA secure provided that IND-CCA2 secure as well [39] and they show that the scheme C_{owh} is indeed IND-CCA2 secure under the assumption of sole-samplability.

4.2.2 C_{sig} Public Key Encryption Scheme

We review the original Zheng-Seberry encryption scheme that adapts ElGamal signature. Suppose Bob, B, wants to send a n-bit messsage m in secret to Alice, A, with A's public key $y_A = g^{x_A}$ where x_A is the secret key of A. The encryption and the decryption procedures are as follows:

Encryption:

- x and k are chosen randomly from $[1, p-1]$ such that $gcd(k, p-1) = 1$.
- $r = {y_A}^{x+k} \bmod p$ and $z = G(r)$
- $c_1 = g^x \bmod p$, $c_2 = g^k \bmod p$, $c_3 = (H(m) - x \cdot r)/k \bmod p$
- $c_4 = z \oplus m$
- $C = (c_1,\ c_2,\ c_3,\ c_4)$

Decryption:

- $r' = (c_1 c_2)^{x_A} \bmod p$
- $z' = G(r'),\ \ m' = z' \oplus c_4$
- if $g^{h(m')} = c_1^{r'} \cdot c_2^{c_3} \bmod p$ then output m', otherwise $\perp$.

Zheng and Seberry were unable to prove that the scheme C_{sig} is semantically secure against chosen plaintext attacks because m appears both c_3 and c_4 hence it is not certain about the

leaked information. But they stated that if H is replaced by a random function, then the problem does not occur and the adversary has negligible probability in guessing the right b for m_b hence the scheme is IND-CPA secure.

4.3 Lim-Lee's Attack

Although C_{owh} is efficient and has a simple design, Lim and Lee [25] shows that an attacker breaks the scheme under known plaintext attacks if one wants to add authentication capability which guarantees that no third party can create a legal ciphertext between A and B. The attack is as follows:

We point out that the enciphering procedure of C_{owh} is

$$(c_1,\ c_2) = (g^r,\ G(y_A^r) \oplus (m \parallel H(m)).$$

A third party C can mount a known plaintext attack to impersonate A or B. C obtains m, then calculates $H(m)$ and by adding c_2 part of the ciphertext, gets the output of G, hence, he is able to choose m' different from m, calculates $H(m')$, with the output of G to create a valid ciphertext c'. To overcome this problem, they propose a countermeasure by using random numbers involved hash calculation which is later modified by Zheng [40]. They also present another method different from Zheng and Seberry for schemes to become secure against chosen ciphertext attacks. The proposed method is useful for an application to group oriented cryptosystems [12]. In their method, the decryption algorithm first checks whether the ciphertext is valid, then outputs the underlying plaintext, whereas in Zheng and Seberry's method, first the ciphertext is decrypted as m, and output when the checking procedure is satisfied.

4.4 Soldera's Attack

Soldera et.all [38] analysed the C_{owh} scheme and showed that it was insecure against chosen ciphertext attacks if the attacker knows the message m in the challenge ciphertext. We know that $c_2 = G(y_A^r) \oplus (m \parallel H(m)$ which depends only on m. As long as m is known, this part can be recreated as mentioned previous section. The adversary chooses m' of its own, calculates

$H(m')$ and creates $c'_2 = c2 \oplus (m' \parallel H(m') \oplus m \parallel H(m) = G(y_A^r) \oplus (m' \parallel H(m')$. This gives the adversary A to make an adaptive chosen ciphertext attack as presented in Attack 1.

Attack 1 Soldera's Attack:

1: A chooses m_0 and m_1 of equal length.

2: The challenger selects one of them randomly.

3: The challenge ciphertext is produced as $(c_1, c_2) = (g^r, G(y_A^r) \oplus m_b \parallel H(m_b))$.

4: A changes c_2 to $c_2 \oplus [m_0 \parallel H(m_0)] \oplus [m_1 \parallel H(m_1)]$.

5: If m_0 is encrypted then A has $G(y_A^r) \oplus [m_1 \parallel H(m_1)]$ and similar for m_1.

6: A has a valid ciptertext which is not equal to the challenge ciphertext.

7: A asks decryption oracle and upon receiving the plaintext, decides b.

Note that A succeeds every time. This is because the hash function, H, depends only on m. To defeat this kind of attack, not only m but also some randomness such as $r = y_A^r$ must be used in the hash function. Hence, the adversary A can no longer create the concatenation of message and hash because the attacker does not know the random value use in it. As we mention in the previous section, the idea comes from the authenticated version of Zheng-Seberry scheme.

Zheng [40] improved the tag generation methods by adding some randomness to the input of the hash function being used to get ciphertexts to accomplish the problems mentioned above. These proof techniques and modifications are given in the following sections.

4.5 Zheng's Modified Schemes

Zheng [40] improved C_{owh} encryption scheme, which is provable secure against chosen ciphertext attacks, in order to resist such attacks defined previous sections. To attain this goal, he proposed incorporating some randomness into the hash function, H utilized in the schemes. We briefly give the modified one way hash version of Zheng Seberry encryption scheme, C_{mowh}:

4.5.1 C_{mowh} PKE Scheme

Encryption:

- r is chosen randomly from $[1, p-1]$.

- $c = (c_1,\ c_2)$ such that $c_1 = g^r \bmod p$ and $c_2 = G(y_A^r) \oplus (m \parallel H(m \| y_A^r))$.

Decryption:

- $r' = c_1^{x_A} \bmod p$
- $w = c_2 \oplus G(r')$
- parse the first n bits of w as m' and and the remaining as t'.
- if $(H(m' \parallel r') = t'$ then output is m', otherwise $\perp$.

We note that the main difference is the random value y_A^r in the input of H, that is secret to the attacker which makes it hard to make the same attack as in the original version.

We also note that Baek [3] proved this scheme is secure against adaptive chosen ciphertext attacks in the ROM under the gap Diffie Hellman assumption.

Zheng also gave a solution to the authentication problem and modified C_{owh} scheme by involving the secret key x_B to the input of G and H, respectively as follows:

4.5.2 Enhanced C_{mowh} PKE Scheme with Authentication

Encryption:

- r is chosen randomly from $[1, p-1]$.
- $c = (c_1,\ c_2)$ such that $c_1 = g^r \bmod p$ and $c_2 = G(y_A^{r+x_B}) \oplus (m \parallel H(m \parallel y_A^{r+x_B}))$.

Decryption:

- $r' = (y_B \cdot c_1)^{x_A} \bmod p$
- $w = c_2 \oplus G(r')$
- parse the first n bits of w as m' and and the remaining as t'.
- if $(H(m' \parallel r') = t'$ then output is m', otherwise $\perp$.

Zheng noted that efficiency of C_{sig} can be improved by adapting Schnorr digital signature instead of ElGamal signature [16]. We first give the Schnorr signature scheme, then we modify the C_{sig} encryption scheme by adapting Schnorr signature [21].

Definition 4.5.1 (Schnorr Signature Scheme) *Let $\mathbb{G}$ be a multiplicative, prime order group in which the DLP is hard and g is a generator. Let H be a cryptographic hash function, x and $y = g^x$ are the secret and public keys, respectively.*

- *Choose a random k and set $r = g^k$.*
- *Compute $e = H(m \parallel r)$ and $s = k - xe$.*
- *(e, s) is the signature pair.*

Verification:

- *Compute $r_v = g^s y^e$ and $e_v = H(m \parallel r_v)$.*
- *Check if $e_v = e$, then the signature is verified, since*

$$r_v = g^s \cdot y^e = g^{(k-ex)} \cdot g^{ex} = g^k = r$$

and

$$e_v = H(m \parallel r_v) = H(m \parallel r) = e$$

holds.

Remark 4.5.2 *We note that under the discrete logarithm assumption, the Schnorr signature scheme [36] is existentially unforgeable under chosen message attack. The proof is similar to that of hashed RSA signature scheme. It is also efficient and generates short signatures.*

4.5.3 C_{msig} PKE Scheme with Schnorr Signature Adaptation

Let $\mathbb{G}$ be a group with prime order p in which the DLP is intractable and g be a generator. Let $y_A = g^{x_A}$ is A's public key and x_A is the private key. B wants to send a n bit message m to A. Let G and H are hash functions that are modeled as random oracles. Encryption and decryption procedure are as follows:

Encryption:

- x and k are chosen randomly from $[1, p-1]$.
- $c_1 = g^x,\ c_2 = H(m \parallel {y_A}^{x+k}),\ c_3 = k - x \cdot c_2,\ c_4 = G(y_A^{x+k}) \oplus m.$
- $c = (c_1,\ c_2,\ c_3,\ c_4)$

Decryption:

- $r' = (g^{c_3} \cdot {c_1}^{c_2+1})^{x_A}$ (which is supposed to be ${y_A}^{x+k}$)
- $m' = c_4 \oplus G(r')$
- if $(H(m' \parallel r') = c_2$ then output is m', otherwise $\perp$.

We state a variant of Diffie-Hellman problems, namely partitioned Diffie-Hellman problem and define it as follows:

Definition 4.5.3 (The Partitioned Diffie-Hellman Problem: PDH) *Let $\mathbb{G}$ be a finite, multiplicative group of order q with a generator g. Given $y_1 = g^{x_1}$, $y_2 = g^{x_2}$ and $y_3 = g^{x_3}$ for randomly chosen $(x_1,\ x_2,\ x_3)$, it is asked to compute $y = g^{x_1(x_2+x_3)}$.*

We prove that the PDH problem is equivalent to the CDH problem by showing that these problems can be reduced to each other.

- The PDH problem can be reduced to the CDH problem as follows: Given a PDH problem instance $(g^{x_1}, g^{x_2}, g^{x_3})$ and a CDH oracle, we can first multiply g^{x_2} and g^{x_3}, then give $(g^{x_1},\ g^{x_2+x_3})$ to the CDH oracle which outputs $g^{x_1(x_2+x_3)}$, exactly the result of the PDH problem we are looking for.
- CDH problem can be reduced to the PDH problem as follows: Given a CDH problem instance (g^{x_1}, g^{x_2}) and a PDH oracle, we can give (g^{x_1}, g^{x_2}, g^0) to the PDH oracle which outputs $g^{x_1(x_2+0)} = g^{x_1 x_2}$, exactly the result of the CDH problem we are looking for.

We give the definition of another variant of Diffie-Hellman problems which was introduced by Okamoto and Pointcheval in [28].

Definition 4.5.4 (The gap Diffie-Hellman Problem: gDHP) *Let $\mathbb{G}$ be a finite, multiplicative group of order q with a generator g. Given g^{x_1}, g^{x_2} and a DDH oracle, it is required to compute $g^{x_1 x_2}$.*

The Gap Diffie-Hellman Assumption The gDHP is computationally hard. Essentially, this means that CDH problem is still hard even if a DDH oracle is available. We define the success probability of the adversary by

$$\text{Succ}_{A_{GDH}} = Pr[GDH^{O_{DDH}}(g, g^{x_1}, g^{x_2}) = g^{x_1 x_2}]$$

and say that this problem is hard if $\text{Succ}_{A_{GDH}}$ is negligible.

4.5.4 The security Analysis of C_{msig}

In this section, we prove that our modified scheme C_{msig} is indistinguishable against adaptive chosen ciphertext attacks in the random oracle model. This part is our main contribution of the thesis.

We give the main theorem:

Theorem 4.5.5 *The encryption scheme C_{msig} is IND-CCA2 secure in the random oracle model if the gDHP is intractable in the underlying group.*

Proof. The proof consists of two parts, (1) proving that the scheme is IND-CPA secure, (2) proving that the scheme is plaintext aware. As we noted before, it is a well known that these two properties imply IND-CCA2 security.

First, we show that the scheme C_{msig} is semantically secure against a chosen plaintext attacker, A_{CPA}, via game hopping technique as we mention in Section 3.2.

We start with the real attack game:

***Game* G_0:** This game is actually the same as the real attack game. First, we take the security parameter and run the key generation algorithm to get public and secret keys, (g^{x_A}, x_A), respectively. The public key, g^{x_A}, is given to the attacker A_{CPA}. After, A_{CPA} chooses two messages of equal length $(m_0,\ m_1)$, we choose x^*, k^* randomly and create a challenge ciphertext

$c^* = ({c_1}^*,\ {c_2}^*,\ {c_3}^*,\ {c_4}^*)$ such that

$$c^* = (g^{x^*},\ H(m_b \parallel {y_A}^{x^*+k^*}),\ k^* - x^*{c_2}^*,\ G({y_A}^{x^*+k^*}) \oplus m_b).$$

Upon receiving c^*, A_{CPA} outputs b'. We denote S_0 the event that $b' = b$. Since this game is the same as the real attack game, we have

$$|Pr[S_0]| = 1/2 + \mathrm{Succ}_{A_{CPA}}.$$

Note that, in this security notion, there is no decryption oracle access for the adversary.

Game G_1**:**

Let G_1 be the same game as G_0 except that in the challenge ciphertext, the value ${y_A}^{x^*+k^*}$ that appears in G and H are substituted with a random value r. That is, the challenge ciphertext becomes

$$c^* = (g^{x^*},\ H(m_b \parallel r),\ k^* - x^*{c_2}^*,\ G(r) \oplus m_b)$$

We argue that the adversary A_{CPA} can distinguish its views among these two games G_0 and G_1, only when ${y_A}^{x^*+k^*}$ is queried to the oracles.

We note that since PDH problem is hard, it has a negligible probability that the critical query ${y_A}^{x^*+k^*}$ is asked by the adversary A_{CPA} to the random oracles H and G, respectively. Let ϵ_{PDH} be the advantage of A_{CPA} breaking PDH problem. Then we have

$$|Pr[S_1] - Pr[S_0]| \leq \epsilon_{PDH}.$$

Let G_2 be such a game that the challenger chooses r_1 and r_2 uniformly at random without interacting to the oracles when preparing the challenge ciphertext. Hence, the challenge ciphertext becomes $c^* = (g^{x^*},\ r_1,\ k^* - x^*{c_2}^*,\ r_2 \oplus m_b)$. The adversary A_{CPA} distinguishes which game is played between G_1 and G_2 whenever the true value is catched among all of the random oracle queries which is negligible as follows:

$$|Pr[S_2] - Pr[S_1]| \leq \frac{q_H + q_G}{2^{|\mathbb{G}|}}$$

where q_H and q_G are polynomial number of queries to the random oracles H and G, respectively.

From these equations, we conclude that the adversary A_{CPA} has negligible probability in guessing the right m_b chosen by the challenger. This shows that the scheme C_{msig} is IND-CPA secure in the random oracle model.

Plaintext awareness:

This security notion is first introduced by Bellare and Rogaway [5]. It states that it shoud be impossible to generate any valid ciphertexts without knowing the corresponding plaintexts, i.e, the adversary is aware of the decryption of the message therefore, the decryption oracle becomes useless. Plaintext awareness together with IND-CPA security implies security against chosen ciphertext attacks. In this respect, we need an algorithm K, called knowledge extractor, to perfectly simulate the decryption oracle, this means without the secret key, K is able to decrypt the ciphertexts submitted by the attacker A_{CCA} to the decryption oracle, just by watching the random oracle queries and the answers returned.

Let ℓ_G and ℓ_H be the query-answer list such that

$$\ell_G = (r_1, G_1), (r_2, G_2), ..., (r_{q_G}, G_{q_G})$$

and

$$\ell_H = (s_1, H_1), (s_2, H_2), ..., (s_{q_H}, H_{q_H})$$

respectively where q_G and q_H are polynomial number of queries of the adversary to the random oracles H and G, respectively.

Let $c^* = (c_1^*,\ c_2^*,\ c_3^*,\ c_4^*)$ be the challenge ciphertext and $y_A = g^{x_A}$ be the public key respectively. We first check whether c_2^* is included in H_i where $1 \leq i \leq q_H$. Then, parse the first n-th bit of the query s_i as m', and the rest as r' of s_i. We calculate $m' \oplus c_4^*$ and check whether it is included in G_i where $1 \leq i \leq q_G$. Then, we compare the oracle queries r_i and r', and provided that equality holds, we conclude $r_i = r' = {y_A}^{x^*+k^*}$. Then we compute g^{k^*} from $g^{{c_3}^*}({c_1}^*)^{{c_2}^*}$ and finally, with the help of DDH oracle, we check whether $(g^{x^*}, g^{x_A}, g^{k^*}, r_i)$ really satisfies PDH instance. Otherwise, ${c_3}^*$ would not be checked and this enables the adversary to make a chosen ciphertext attack. The adversary simply changes the third component of the challenge ciphertext c^* and finds b directly using the decryption oracle. We note that it is impossible for the adversary to generate a valid ciphertext without making necessary random oracle queries, since the outputs of random oracles are assumed to be truly random if not explicitly queried.

This completes the proof. ■

Remark 4.5.6 *By adapting Schnorr signature to C_{sig}, we get a more efficient scheme C_{msig}, since no inversion operation is needed and we prove the security of the scheme against chosen*

ciphertext attacks. Moreover in C_{sig}, there is no randomness for the calculation of H, hence confidentiality does not hold by utilizing only $H(m)$, i.e, there is no difference to use $H(m)$ or just m. This is because adversary knows m_0 and m_1 in the game. If we provide randomness by concatenation, the proof may hold but we are unable to get rid of the inversion operation. This is why we focus on Schnorr signature, and modification of C_{sig} by adapting it to the scheme.

CHAPTER 5

CONCLUSION

"Knowing is not enough; we must apply. Willing is not enough; we must do."

Goethe

In this thesis, we give the security definitions in terms of adversarial goals and adversarial capabilities. We present several games played between the challenger and the adversary in order to analyse the security under some mathematically hard problems.

In Chapter 3, we propose a shortcut for a generic construction from an IND-CPA secure one-way trapdoor function to an IND-CCA2 secure public key encryption given by Fujisaki-Okamoto [17]. Their conversion needs a re-encryption which makes it expensive in terms of computational complexity. In our method, we check the consistency of the ciphertext using the random value instead of requiring re-encryption. It is clear that our method is less generic than theirs, because we can apply this method only for public key encryption schemes where the random value can be efficiently found from the ciphertext and the plaintext. We investigate suitability of our method for several public key encryption schemes and show that the method can be used in Paillier encryption with the same complexity as original Fujisaki-Okamoto construction. On the other hand, in several schemes it was observed that our method is inapplicable since calculation of the random value is costly or impossible [16, 26, 29].

In Chapter 4, we mention three methods proposed by Zheng and Seberry [39] for public key encryption schemes to become secure against adaptive chosen ciphertext attacks. We focus on one of the three methods, namely C_{sig}, which is an encryption scheme with ElGamal signature adaptation. We modify this scheme by adapting Schnorr signature and this new encryption scheme C_{msig} turns out to be more efficient, since we get rid of inversion operation

which is necessary in C_{sig}. Moreover, we prove that the modified version C_{msig} is provably secure against adaptive chosen ciphertext attacks in the random oracle model under the gap Diffie Hellman assumption. To attain our goal, we first show that the scheme C_{msig} is IND-CPA secure via game hopping tecnique, then it also satisfies plaintext awareness in the ROM, finally it is a well known fact that these security notions together lead to IND-CCA2 security.

REFERENCES

[1] M. Ak, T. Hanoymak, *Eliminating Re-encryption from Fujisaki-Okamoto Construction and Its Applications*, Proceedings of Information Security and Cryptology Conference, pp.64–68, ISCTURKEY 2010, Ankara, 2010.

[2] M. Ak, T. Hanoymak, *On the Random Oracle Model and the Game Hopping Technique*, Proceedings of Information Security and Cryptology Conference, pp.273–278, ISCTURKEY 2012, Ankara, 2012.

[3] J. Baek, Y. Zheng, *Zheng and Seberry's public key encryption scheme revisited*, Int. J. Inf. Secur., 2, pp. 37-44, 2003.

[4] M. Bellare, P. Rogaway, *Random oracles are practical: A Paradigm for designing efficient protocols*. Proc. of the First ACM Conference on Computer and Communications Security, pp. 62-73, 1993.

[5] M. Bellare, P. Rogaway, *Optimal Asymmetric Encryption -How to encrypt with RSA*. Extended abstract in Advances in Cryptology - Proc., LNCS, vol. 950, EUROCRYPT'94.

[6] M.Bellare, A. Desai, D. Pointcheval, P. Rogaway, *Relations among notions of security for public-key encryption schemes*. Advances in Cryptology, CRYPTO'98.

[7] D. Boneh, R. Venkatesan, *Breaking RSA may not be equivalent to factoring*, Advances in Cryptology-Eurocrypt'98.

[8] R. Canetti, O. Goldreich, S. Halevi, *The random oracle methodology, revisited*, Proc. of the 30th ACM Symp. on Theory of Computing (STOC), pp. 209-218, 1998.

[9] R. Cramer, Victor Shoup, *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*, Proc. of the 18th Annual International Cryptology Conference on Advances in Cryptology, pp. 13-25, CRYPTO '98.

[10] R. Cramer, V. Shoup, *Universal Hash Proofs and a paradigm for adaptive chosen ciphertext secure public key encryption*, EUROCRYPT'2002.

[11] I. Damgard, *Towards Practical Public Key Systems Secure Against Chosen Ciphertext Attacks*, In Advances in Cryptology-CRYPTO'91.

[12] Y. Desmedt, *Society and group oriented cryptography: A new concept*, Advances in Cryptology-Crypto'87, LNCS vol.293, Springer-Verlag pp. 120-127, 1988.

[13] Y. Desmedt, D. Phan, *A CCA secure Hybrid Damgard's ElGamal Encryption*, Lecture Notes in Computer Science, vol. 5324, pp. 68-82, 2008.

[14] W. Diffie, M. E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, vol. IT-22, pp. 644–654, 1976.

[15] D. Dolev, C. Dwork, M. Naor, *Non-Malleable Cryptography*, STOC'91.

[16] T. Elgamal, *A public key cryptosystem and a signature scheme based on discrete logaritms*, IEEE Transactions on Information Theory, pp. 469-472, 1984.

[17] E.Fujisaki, T.Okamoto, *How to Enhance the Security of Public-Key Encryption at Minimum Cost*. PKC'99, LNCS 1560, pp. 53-68, 1999.

[18] E. Fujisaki, T. Okamoto,*Secure Integration of Asymmetric and Symmetric Encryption Schemes*, CRYPTO'99, LNCS 1666, pp. 537–554, 1999.

[19] S. Goldwasser, S. Micali, *Probabilistic encryption*, Journal of Computer and System Sciences, pp. 270–299, 1984.

[20] S. Goldwasser, S. Micali, *Probabilistic encryption and how to play mental poker keeping secret all partial information*, Proc.14-th Annual Symp. Theory and Computing, 1982.

[21] T. Hanoymak, M. Ak, A. Aydın Selçuk, *Modified Zheng-Seberry Signature Based Scheme is Provably Secure Against CCA2*, International Conference on Applied and Computational Mathematics ICACM 2012, Ankara, 2012.

[22] J. Katz, *LectureNotes*,http://www.cs.umd.edu/ jkatz/gradcrypto2/scribes.html

[23] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, 2008.

[24] N. Koblitz, A. Menezes, *Another Look at Provable Security*, J. Cryptology 20(1): pp. 3-37, 2007.

[25] C. Lim, P. Lee, *Another method for attaining security against adaptively chosen ciphertext attack* Crypto'93, LNCS(vol:3), pp. 410–434, (1993).

[26] D. Naccache, J. Stern, *A New Public Key Cryptosystem Based on Higher Residues*, In Proc. of the 5th CCCS. ACM press, 1998.

[27] M. Naor, M. Yung, *Public key cryptosystems provably secure against chosen ciphertext attacks*, Proceedings of the 22-th annual ACM Symposium of Theory and Computing, 1990.

[28] T. Okamoto, D. Pointcheval, *The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes*, Public Key Cryptography 2001, pp. 104–118, Springer LNCS, 1992.

[29] T.Okamoto, S.Uchiyama, *A New Public-Key Cryptosystem as Secure as Factoring*, pp. 308–318, EUROCRYPT'98.

[30] P. Paillier, D. Pointcheval, *Efficient Public Key Cryptosystems Provably Secure Against Active Adversaries*, Advances in Cryptology, pp. 165–179, ASIACRYPT'99.

[31] P. Paillier, *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*, Proc. of the 17th international conference on Theory and application of cryptographic techniques, pp. 223-238, EUROCRYPT'99.

[32] C. Peikert, B. Waters, *Lossy trapdoor functions and their applicaitons*, 40th ACM Symposium on Theory of Computing, STOC'08.

[33] M. Rabin, *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*, MIT Laboratory for Computer Science, January 1979.

[34] C. Rackoff, D. Simon, *Noninteractive zero-knowledge proof of knowl-edge and chosen ciphertext attack*, In Advances in Cryptology, pp. 433-444, CRYPTO'91.

[35] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21 (2), pp. 120-126, 1978.

[36] C. P. Schnorr, *Efficient identification and signatures for smart cards*, Proc. of CRYPTO '89, pp. 239-252, 1990.

[37] V. Shoup, *Sequences of games: A tool for taming complexity in security proofs*, 2006.

[38] D. Soldera, J. Seberry, J. Qu C, *The analysis of Zheng-Seberry Scheme*, LNCS, 2384, pp.159-168, 2002.

[39] Y. Zeng, J. Seberry, *Immunizing public key cryptosystems against chosen ciphertext attacks*, IEEE Journal on Selected Areas in Communications, 1992.

[40] Y. Zheng, *Improved public key cryptosystems secure against chosen ciphertext attacks*, Technical note, The centre for computer security research, 1994.

VITA

PERSONAL INFORMATION

Surname, Name: Hanoymak, Turgut

Date and Place of Birth: 1980 - Aydın

Marital Status: Single

email: turguthanoymak@gmail.com

ACADEMIC DEGREES

Ph.D. after B.S. Degree	METU, Department of Cryptography	2012
	Graduate School of Applied Mathematics	
	Middle East Technical University-Ankara	
	Supervisor: Prof. Dr. Ersan Akyıldız	
	Co-supervisor: Assist. Prof. Dr. Ali Aydın Selçuk	
	On Provable Security of Some Public Key Encryption Schemes	
B.S.	Ankara University, Department of Mathematics	2002
High School	Kuşadası Kaya Aldoğan High School	1998

WORK EXPERIENCE

2002 - 2012	METU, Institute of Applied Mathematics	Research Assistant

PUBLICATIONS

- with M. Ak, Eliminating Re-encryption from Fujisaki-Okamoto Construction and Its Applications., Proceedings of Information Security and Cryptology Conference, (ISC-TURKEY 2010), Ankara, 2010 pp. 64-68.
- with M. Ak, On the Random Oracle Model and the Game Hopping Technique, Proceedings of Information Security and Cryptology Conference, (ISCTURKEY 2012), Ankara, 2012, pp.273-278.
- with M. Ak and A. Aydın Selçuk, Modified Zheng-Seberry Signature Based Scheme is Provably Secure Against CCA2., International Conference on Applied and Computational Mathematics (ICACM 2012), Ankara