On Provable Security of Cryptographic Schemes

Turgut Hanoymak

Institute of Applied Mathematics, Middle East Technical University, 06531, Ankara, Turkey
Department of Mathematics, Yüzüncü Yıl University, 65080, Van, Turkey
e-mail: hturgut@yyu.edu.tr

Abstract—Provable security is an important issue in modern cryptography because it satisfies the security of the encryption schemes in a theoretical way via a reduction method. To prove the security of a cryptographic scheme, it is necessarry to define the goals and the capabilities of the adversary. In this paper, we explain 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. We review the definition of provable 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 investigate the security of some public key encryption schemes such as RSA, Rabin, Goldwasser-Micali, ElGamal, Cramer-Shoup and discuss under which circumstances they satisfy which security notions.

Keywords—provable security, security notions, public key encryption, standard model, random oracle model.

1. Introduction

Throughout the last century, especially with the beginning of public key cryptography due to Diffie-Hellman [7], 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, 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 [11] and the notion of semantic security which is also called polynomial indistinguishability was defined. 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 [14]. 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 [16] 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 be 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 [8] 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 [10] 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 [5] 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 [18] 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. 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.

In provable 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 [4] 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 [1]. 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. [3] 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.

In this paper, 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 public key encryption schemes and show that under which assumptions they satisfy which security notions in the standard model.

2. Security Notions and Public Key Encryption Schemes

In this section, 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 [4] 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: 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.

2.2. 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 2.2: 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

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

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.

2.3. 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.

2.4. Adversarial Goals

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.

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 2.3: 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 2.4: 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 [11].

Definition 2.5: 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

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

Malleability

The notion of malleability is introduced by Naor et al. [8]. 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.

2.5. Adversarial Capabilities and IND-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 2.6: 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: $PubK^{ind-cca1}_{A,\Pi}$

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: $PubK^{ind-cca2}_{A,\Pi}$

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.

2.6. 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 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

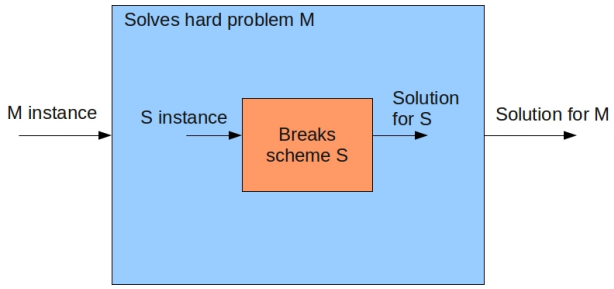

Fig. 1. The reduction idea to prove security of public key schemes

is assumed to be impossible. This is explained in Figure 1.

3. Security Analysis of Some Public Key Encryption Schemes

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

Definition 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 3.2: The multiplicative group of $\mathbb{Z}_N$ is

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

3.1. The RSA Encryption Scheme

Rivest, Shamir, Adleman proposed this scheme due to the trapdoor one way permutation property of the RSA function [17]. 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 $m = c^d \bmod N$.

We state **the RSA problem** as follows:

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.

The 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 3.3: Bellare and Rogaway [2] 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.

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 factorization 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 [15] 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.

3.3. Goldwasser-Micali Encryption Scheme

Goldwasser and Micali [11] 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:

Given $N = p \cdot q$ where p, q are primes and $a \in \mathbb{Z}_N^*$ with

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

decide whether a is quadratic residue mod N.

We note that $a \in \mathbb{Z}_N^*$ 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 $a \bmod N$. We recall that if $a \in \mathbb{Z}_N^*$ is quadratic residue, then the Jacobi symbol denoted as $\left(\frac{a}{N}\right)$ is 1, otherwise -1.

Remark 3.4: The Jacobi symbol is an extension of the Legendre symbol for a prime $N = p$.

Remark 3.5: Given a and N (with unknown factorization), it is possible to compute the Jacobi symbol of a in polynomial time.

The Quadratic Residuosity Assumption:

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

Remark 3.6: 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.

Goldwasser-Micali 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 3.7: Although, Goldwasser-Micali encryption scheme is the first probabilistic encryption scheme satisfiying semantic security, efficiency does not hold because of ciphertext expansion.

3.4. ElGamal Encryption Scheme

Before we give the description of the scheme, we recall some mathematically hardness assumptions and relations between them.
We state **the discrete logarithm problem** as follows:
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.
Recall that **the computational Diffie-Hellman problem** is defined as follows:
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 $\mathbb{G}$.

We state **the decisional Diffie-Hellman problem** as the following:
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 3.8: 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 [9] 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 [13].

Theorem 3.9: 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

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

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 3.10: 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 3.11: Damgard proposed [5] 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 [6] 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.

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 [4], [12].

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 3.12: 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 3.13: 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 3.14: 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 $\alpha,\ \beta,\ r$ 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. □

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 3.15: 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 3.16: 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 3.17: 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 [4], [12] 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

$$log_{g_1} w = a \cdot log_{g_1} g_3 + b \cdot log_{g_1} g_4 \qquad (1)$$

and from the public key c, A learns that

$$log_{g_1} c = a + b \cdot log_{g_1} g_2. \quad (2)$$

From (1) and (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;

$$log_{g_1} \frac{e}{m} = x \cdot r + y \cdot r' \cdot log_{g_1} g_2 \quad (3)$$

from the public key h, A learns that

$$log_{g_1} h = x + y \cdot log_{g_1} g_2. \quad (4)$$

Since (3) and (4) are linearly independent, A can compute the values of (x, y) and finally decrypt the challenge ciphertext. □

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 3.18: 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.

□

4. Conclusion

In this paper, we summarize the basic concepts about provable security of public key encryption schemes giving security models in terms of adversarial goals and adversarial capabilities. In this respect, we briefly explain several games between the challenger and the adversary to prove the security of a cryptographic scheme. Finally we give some public key encryption schemes to demonstrate the ideas. We hope that the ideas presented here provide the readers a better understanding about the security proofs in modern cryptography.

Acknowledgment

We would like to express our sincere gratitude to the anonymous referees for their valuable comments, to Ersan Akyıldız for his diligent guidance and to Ali Aydın Selçuk for useful discussions.

References

[1] 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.

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

[3] 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.

[4] 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.

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

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

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

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

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

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

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

[12] J. Katz, *LectureNotes*,http://www.cs.umd.edu/ jkatz

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

[14] 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.

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

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

[17] 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.

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