

## Lecture 8

Lecturer: Victor Shoup

Scribe: Prashant Puniya

## Overview

In this lecture, we will introduce the notion of *Public-Key Encryption*. We will define the basic notion of security for this primitive, i.e. *Semantic Security*. We will discuss an alternative formulation of the semantic security definition that is sometimes more intuitive to work with. Finally, we will give two examples of semantically-secure public-key encryption schemes, namely the *El-Gamal Encryption* and the *Paillier Encryption* schemes.

Throughout the sequel, we denote the security parameter by  $\lambda$ .

## Public-Key Encryption

A public-key encryption (PKE) scheme  $\mathcal{E} = (G, E, D)$  consists of three algorithms.

- The *key generation algorithm*  $G$  takes as input the security parameter  $\lambda$  in unary form and outputs a pair  $(PK, SK)$ , the public key and secret key for  $\mathcal{E}$ . That is  $(PK, SK) \leftarrow G(1^\lambda)$ .
- The *encryption algorithm*  $E$  takes as input a public key  $PK$  and a message  $m$  and outputs a ciphertext  $c$ . That is,  $c \leftarrow E(PK, m)$ .
- The *decryption algorithm*  $D$  takes as input a secret key  $SK$  and a ciphertext  $c$  and outputs a message  $m$ . That is  $m \leftarrow D(SK, c)$ .

Usually, the key generation and encryption algorithms are probabilistic while the decryption algorithm is deterministic<sup>1</sup>. The *correctness* property of the PKE scheme  $\mathcal{E}$  is defined as:

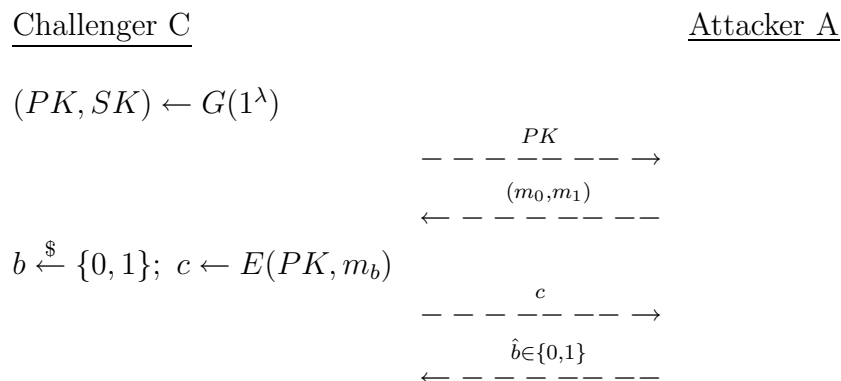
$$\forall (PK, SK) \leftarrow G(1^\lambda) \forall m : D(SK, E(PK, m)) = m$$

The most basic notion of security for a PKE encryption scheme  $\mathcal{E}$  is *Semantic Security* or *Indistinguishability*. As usual, we define this notion in terms of a game between a challenger

---

<sup>1</sup>The encryption algorithm must be probabilistic, even to satisfy the most basic notion of security for PKE schemes. The decryption algorithm may be probabilistic, but for most PKE schemes it is possible to derandomize the

$C$  and an attacker  $A$  which proceeds as follows:



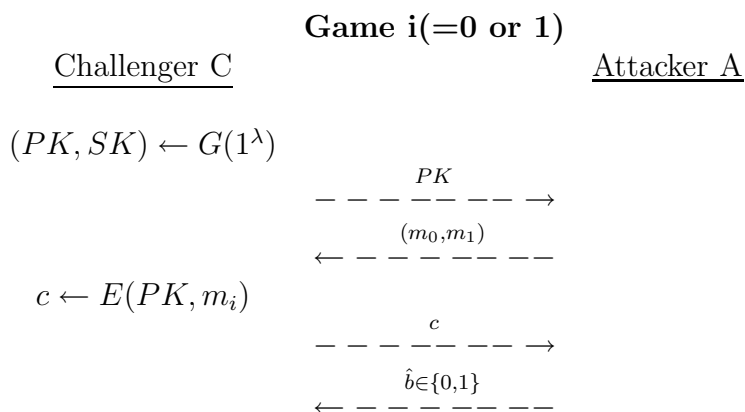
The advantage of the adversary  $A$  against an encryption scheme  $\mathcal{E}$  in the above game is defined as follows:

$$AdvDist_A[\mathcal{E}] \stackrel{def}{=} \left| \Pr[\hat{b} = b] - \frac{1}{2} \right|$$

The encryption scheme  $\mathcal{E}$  is said to be *semantically secure* if for all probabilistic polynomial time adversaries  $A$ , the advantage  $AdvDist_A[\mathcal{E}]$  is negligible.

## Alternative Definition

We will now give an alternative way to define the security of a public-key encryption scheme that will be more useful when analyzing the encryption scheme as a part of a large cryptosystem. In this alternative definition, we define two games between the challenger and the adversary as follows:



The task of the adversary  $A$  in this definition is to distinguish between these two games and its advantage against the encryption scheme  $\mathcal{E}$  is defined as:

$$AdvDist'_A[\mathcal{E}] \stackrel{def}{=} \left| \Pr[\hat{b} = 1 \mid \text{game 0}] - \Pr[\hat{b} = 1 \mid \text{game 1}] \right|$$

A public-key encryption scheme  $\mathcal{E}$  is said to be secure under this definition if the advantage  $AdvDist'_A$  is negligible for any probabilistic polynomial-time adversary  $A$ . We will now show

that this alternative definition is essentially the same as the *semantic security* definition given above.

**Claim 1.** For any public-key encryption scheme  $\mathcal{E} = (G, E, D)$  and any adversary  $A$ ,

$$AdvDist'_A[\mathcal{E}] = 2 \cdot AdvDist_A[\mathcal{E}]$$

*Proof.*

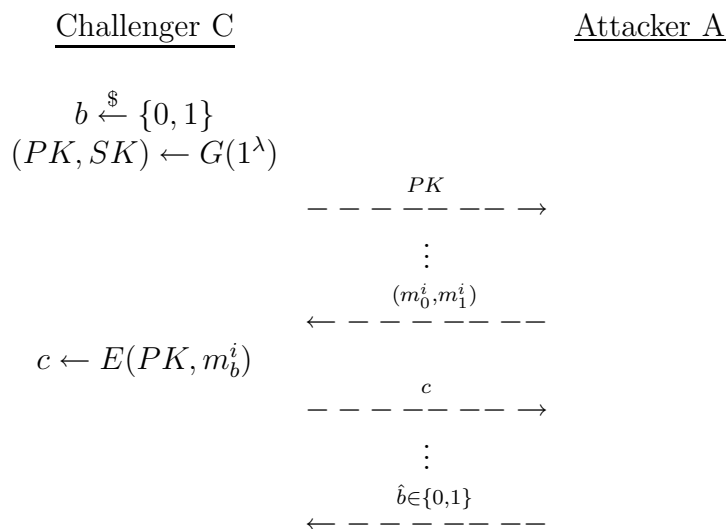
$$\begin{aligned} \frac{1}{2} AdvDist'_A[\mathcal{E}] &= \frac{1}{2} \left| Pr[\hat{b} = 1 | b = 0 \text{ in } 1^{st} \text{ definition}] - Pr[\hat{b} = 1 | b = 1 \text{ in } 1^{st} \text{ definition}] \right| \\ &= \frac{1}{2} \left| (1 - Pr[\hat{b} = b | b = 0 \text{ in } 1^{st} \text{ defn.}]) - Pr[\hat{b} = b | b = 1 \text{ in } 1^{st} \text{ defn.}] \right| \\ &= \left| \frac{1}{2} - \left( Pr[\hat{b} = b \wedge (b = 0 \text{ in } 1^{st} \text{ defn.})] + Pr[\hat{b} = b \wedge (b = 1 \text{ in } 1^{st} \text{ defn.})] \right) \right| \\ &= \left| \frac{1}{2} - Pr[\hat{b} = b \text{ in } 1^{st} \text{ definition}] \right| \\ \Rightarrow AdvDist'_A[\mathcal{E}] &= 2 \cdot AdvDist_A[\mathcal{E}] \end{aligned}$$

□

When analyzing the security of a larger system which makes use of the encryption scheme, this alternative definition turns out to be more natural to use than the *semantic security* definition.

## Multi-message security

We can modify the definition of semantic security to define the notion of *multi-message security* for public-key encryption schemes. This definition is again given as a game between the challenger  $C$  and the adversary  $A$ .



As before, the task of the adversary is to predict the value of  $b$  used by the challenger.

$$\text{AdvDistM}_A[\mathcal{E}] = \left| 1/2 - \Pr[b = \hat{b}] \right|$$

It seems as though the adversary should have a better chance of guessing the challenger's bit  $b$ , since it gets to send more than one challenge message pairs. However, it can be shown that the a semantically-secure public-key encryption scheme is also multi-message semantically secure.

**Claim 2.** *If an encryption scheme  $\mathcal{E}$  is semantically-secure then it is also multi-message semantically-secure.*

*Proof.* Let us assume that the multi-message adversary  $A$  sends  $q$  challenge message pairs,  $(m_0^j, m_1^j)_{j=1\dots q}$ . Then we construct  $(q + 1)$  hybrid games between the challenger and the adversary, game 0 to game  $q$ . In game  $i$ , the challenger encrypts the message  $m_0^j$  for  $j \leq i$ , and  $m_1^j$  for  $j > i$ . Thus in game 0 the challenger encrypts the message  $m_0^j$  for all  $j$  and in game  $q$  it encrypts the message  $m_1^j$  for all  $j$ . If the multi-message adversary  $A$  has non-negligible advantage, then the probability that it outputs 1 in game 0 and in game  $q$  differs by a non-negligible amount. Thus, we can deduce that there is an  $i \in \{0 \dots (q - 1)\}$  such that the probability that the adversary  $A$  outputs 1 in game  $i$  and in game  $(i + 1)$  differs by a non-negligible amount.

We construct the semantic-security adversary  $A'$  using the multi-message adversary  $A$  as a subroutine. The adversary  $A'$  chooses a random  $i \in \{0 \dots (q - 1)\}$  and encrypts the message  $m_0^j$  for  $j \leq i$  for the first  $i$  message pairs given by  $A$ . It sends the  $(i + 1)^{\text{th}}$  message pair sent by  $A$  to the semantic security challenger  $C'$  and sends the response of  $C'$  to the multi-message adversary  $A$ . For the remaining  $(q - i - 1)$  message pairs sent by  $A$ , the adversary  $A'$  always encrypts the message  $m_1^j$ . Finally it outputs the bit  $\hat{b}$  output by  $A$ .  $\square$

We can extend the above claim and define the notion of *multi-key multi-message semantic-security* for public-key encryption schemes. However, a hybrid argument, slightly more involved than the one above, can be used to show that any semantically-secure encryption scheme satisfies this notion as well.

## Examples of Semantically-secure Encryption Schemes

We will discuss two examples of semantically secure encryption schemes, the *El-Gamal Encryption scheme* and the *Paillier Encryption scheme*.

### El-Gamal Encryption

The El-Gamal encryption scheme is defined over a group  $G$  of order  $q$ . The encryption scheme  $\mathcal{E}_{\text{El-Gamal}} = (\text{KeyGen}, E, D)$  consists of the following three algorithms.

$KeyGen(sysParams, 1^k)$ :  
 $g \xleftarrow{\$} \mathbf{G} \setminus \{1_{\mathbf{G}}\}$ ;  
 $x \xleftarrow{\$} \mathbb{Z}_q$ ;  $h \leftarrow g^x$ ;  
 $PK \leftarrow (g, h)$ ;  $SK \leftarrow x$ ;  
 output  $(PK, SK)$

$E(PK, m)$ ,  $m \in \mathbf{G}$ :  
 $r \xleftarrow{\$} \mathbb{Z}_q$ ;  
 $u \leftarrow g^r$ ;  $v \leftarrow h^r$ ;  
 $w \leftarrow v \cdot m$ ;  
 output  $c \leftarrow (u, w)$ ;

$D(SK, (u, w))$ :  
 output  $m \leftarrow w/u^x$ ;

We shall prove the semantic security of this scheme based on the *Diffie-Hellman assumption*. We define two variations of the Diffie-Hellman assumption next.

**Assumption 3 (Computational Diffie-Hellman (CDH) assumption).** For a generator  $g$  of the group  $\mathbf{G}$  of order  $q$ , and for  $x, r \xleftarrow{\$} \mathbb{Z}_q$ , it is hard to compute  $g^{xr}$  given  $(g, g^x, g^r)$ .

**Assumption 4 (Decisional Diffie-Hellman (DDH) assumption).** For a generator  $g$  of the group  $\mathbf{G}$  of order  $q$ , and for  $x, r, y \xleftarrow{\$} \mathbb{Z}_q$ ,

$$(g, g^x, g^r, g^{xr}) \stackrel{comp}{\approx} (g, g^x, g^r, g^y)$$

Here  $\stackrel{comp}{\approx}$  denotes computational indistinguishability.

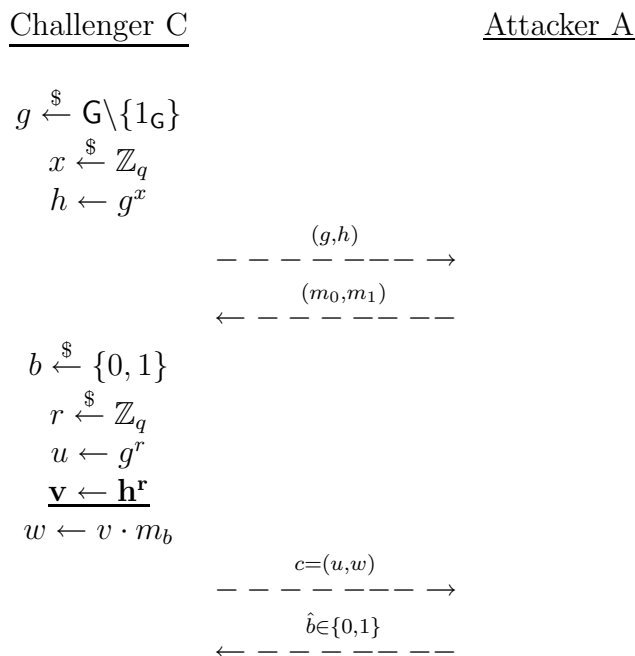
It is easy to see that the CDH assumption is a weaker assumption than the DDH assumption. We will base the security of the El-Gamal encryption scheme on the DDH assumption for the underlying group  $\mathbf{G}$ .

**Theorem 5.** *The El-Gamal encryption scheme is semantically-secure, provided the DDH assumption holds for the underlying group  $\mathbf{G}$ .*

*Proof.* We will prove this theorem via a hybrid argument. Let us describe the sequence of hybrid games.

**GAME 0.** This is the semantic security game between the challenger  $C$  and the adversary

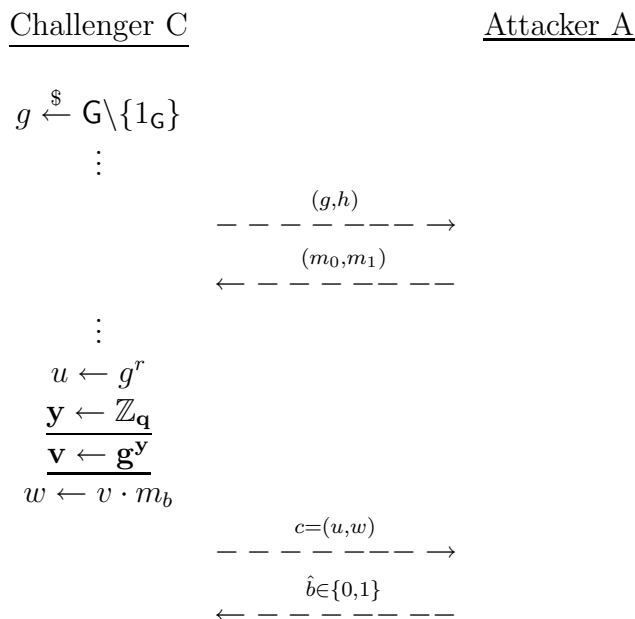
A defined for the El-Gamal encryption scheme.



In the next game, we will modify the underlined text in the description of the challenger. We will define an event associated with this game:

$$W_0 \stackrel{def}{=} \{(b = \hat{b}) \text{ in game } 0\}$$

GAME 1. Now we will modify game 0 so that the ciphertext  $c$  sent by the challenger looks like a random group element to the adversary.



Let us define a similar event associated with the adversary in this game.

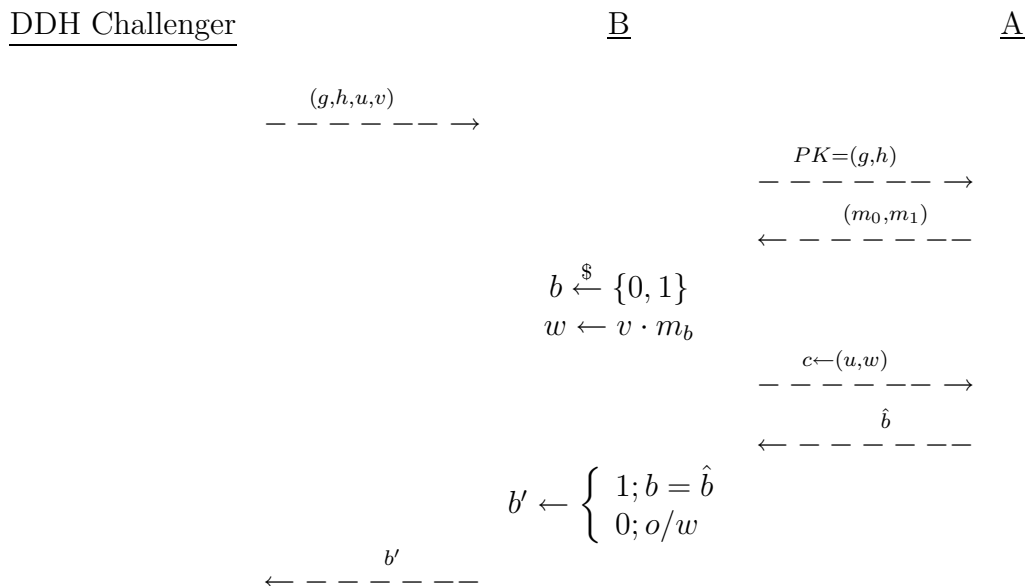
$$W_1 \stackrel{def}{=} \{(b = \hat{b}) \text{ in game 1}\}$$

We will first show that if the DDH assumption holds for the underlying group  $G$ , then games 0 and 1 look similar to the adversary  $A$ . Let us start by defining what we mean by the advantage of a DDH adversary  $B$ , i.e.  $AdvDDH'_B$ . The DDH attacker  $B$  gets a tuple  $(g, h, u, v)$  from the DDH challenger, and outputs either 1 or 0. The advantage  $AdvDDH'_B$  is defined as the difference in the probability that  $B$  outputs 1 when it gets a valid DDH tuple and when  $v$  is a random group element.

**Claim 6.** *There is a DDH adversary  $B$  for the group  $G$  that has advantage*

$$AdvDDH'_B = |\Pr[W_0] - \Pr[W_1]|$$

*Proof.* The DDH adversary  $B$  uses the El-Gamal adversary  $A$  as follows:



If  $(g, h, u, v)$  is a DDH tuple, then the attacker  $B$  acts as the challenger of game 0, otherwise it acts as the challenger in game 1.  $\square$

Next we show that from the attacker  $A$  cannot do better than guess the bit  $b$  at random in game 1.

**Claim 7.**  $\Pr[W_1] = 1/2$

*Proof.* This is clearly true since  $w$  sent by the challenger is simply a random group element and in particular, it is independent of the choice of bit  $b$ .  $\square$

Finally we can combine the above claims to deduce that

$$|\Pr[W_0] - 1/2| = AdvDDH'_B$$

$\square$

## Paillier Encryption Scheme

Let us start by describing the mathematical set-up for the *Paillier encryption scheme*. Let  $N = PQ$  be a product of two large prime numbers  $P$  and  $Q$ , so that  $\phi(N) = (P-1)(Q-1)$ . We additionally assume that  $\gcd(\phi(N), N) = 1$ . The Paillier encryption scheme works over the multiplicative subgroup  $\mathbb{Z}_{N^2}^*$ . Using *Chinese remainder theorem*, we can show that  $\mathbb{Z}_{N^2}^*$  is isomorphic to  $\mathbb{Z}_N \times \mathbb{Z}_N^*$  as follows:

$$\begin{aligned} \mathbb{Z}_{N^2} &\cong \mathbb{Z}_{P^2} \times \mathbb{Z}_{Q^2} \\ \Rightarrow \mathbb{Z}_{N^2}^* &\cong \mathbb{Z}_{P^2}^* \times \mathbb{Z}_{Q^2}^* \\ &\cong \mathbb{Z}_{P(P-1)} \times \mathbb{Z}_{Q(Q-1)} \\ &\cong \mathbb{Z}_P \times \mathbb{Z}_Q \times \mathbb{Z}_{(P-1)} \times \mathbb{Z}_{(Q-1)} \\ &\cong \mathbb{Z}_{PQ} \times \mathbb{Z}_{(P-1)} \times \mathbb{Z}_{(Q-1)} \\ &\cong \mathbb{Z}_N \times \mathbb{Z}_N^* \end{aligned}$$

In fact, we can make this isomorphism explicit by providing a representation of any element of  $\mathbb{Z}_{N^2}$  in terms of an element each from  $\mathbb{Z}_N$  and  $\mathbb{Z}_N^*$ . We denote by  $[k]_{N^2}$ , the residue class corresponding to  $k$  in the ring  $\mathbb{Z}_{N^2}$ . Now let  $\alpha \stackrel{\text{def}}{=} [1 + N]_{N^2}$ . Then we can deduce that,

$$\alpha^k = [(1 + N)^k]_{N^2} = [1 + Nk]_{N^2}$$

Also, we can represent any element  $\beta \in \mathbb{Z}_{N^2}$  as  $[b + Nc]_{N^2}$ , for  $0 \leq b, c < N$ . Moreover, elements  $\beta \in \mathbb{Z}_{N^2}^*$  are of the form  $[b + Nc]_{N^2}$ , where  $0 \leq b, c < N$  and  $\gcd(b, N) = 1$ . From these observations, we can deduce that  $\alpha$  is an element of  $\mathbb{Z}_{N^2}^*$  of order  $N$ . Additionally, it is easy to compute  $k$  given  $\alpha^k$ . We can set up a homomorphism from  $\mathbb{Z}_N$  to  $\mathbb{Z}_{N^2}^*$  using  $\alpha$  as follows:

$$\begin{aligned} \rho_1 : \mathbb{Z}_N &\rightarrow \mathbb{Z}_{N^2}^* \\ [k]_N &\mapsto \alpha^k = [1 + Nk]_{N^2} \end{aligned}$$

We can also set up a homomorphism from  $\mathbb{Z}_N^*$  to  $\mathbb{Z}_{N^2}^*$  as follows:

$$\begin{aligned} \rho_2 : \mathbb{Z}_N^* &\rightarrow \mathbb{Z}_{N^2}^* \\ [b]_N &\mapsto [b^N]_{N^2} \end{aligned}$$

In order to see that this map is well defined, consider  $b_1 \equiv b_2 \pmod{N}$ . Then we can deduce that

$$\begin{aligned} b_1 &= b_2 + Nc \\ \Rightarrow b_1^N &= b_2^N + \binom{N}{1} b_2^{N-1} Nc + \text{terms with } N^2 \\ \Rightarrow b_1^N &\equiv b_2^N \pmod{N^2} \end{aligned}$$

Moreover, this homomorphism is also one-to-one which can be seen by computing the kernel of  $\rho_2$ .

$$\begin{aligned} b^N &\equiv 1 \pmod{N^2} \\ \Rightarrow b^N &\equiv 1 \pmod{N} \\ \Rightarrow b &\equiv 1 \pmod{N} \quad \{\text{because } \gcd(N, \phi(N)) = 1\} \end{aligned}$$

Hence we can deduce that  $Im(\rho_1)$  is a subgroup of  $\mathbb{Z}_{N^2}$  of order  $N$ . On the other hand  $Im(\rho_2)$  has an exponent dividing  $\phi_N$ . Since we know that  $\gcd(N, \phi(N)) = 1$ , we can deduce that

$$Im(\rho_1) \cap Im(\rho_2) = \{[1]_{N^2}\}$$

Thus, we can combine the above homomorphisms to get an isomorphism between  $\mathbb{Z}_N \times \mathbb{Z}_N^*$  and  $\mathbb{Z}_{N^2}^*$  as follows:

$$\begin{aligned} \rho : \mathbb{Z}_N \times \mathbb{Z}_N^* &\rightarrow \mathbb{Z}_{N^2}^* \\ ([k]_N, [b]_N) &\mapsto \alpha^k \cdot [b^N]_{N^2} \end{aligned}$$

This map  $\rho$  is one-to-one because  $kernel(\rho) = \{[1]_{N^2}\}$ . This is because no element in  $Im(\rho_1)$  has a multiplicative inverse in  $Im(\rho_2)$  except  $[1]_{N^2}$ . And since the cardinalities of the sets  $\mathbb{Z}_N \times \mathbb{Z}_N^*$  and  $\mathbb{Z}_{N^2}^*$  are the same, we can also deduce that  $\rho$  is onto. Hence  $\rho$  defines an explicit isomorphism between  $\mathbb{Z}_N \times \mathbb{Z}_N^*$  and  $\mathbb{Z}_{N^2}^*$ .

Now we are ready to describe the *Paillier encryption scheme*. The encryption scheme is  $\mathcal{E}_{Paillier} = (KeyGen, E, D)$ , with the following algorithms:

*KeyGen*(*sysParams*,  $1^k$ ):  
generate  $N = PQ$  with  $\gcd(N, \phi(N)) = 1$   
 $PK \leftarrow N$ ;  $SK \leftarrow (P, Q)$   
output  $(PK, SK)$

*E*( $PK, k$ ),  $k \in \mathbb{Z}_N$ :  
 $b \xleftarrow{\$} \mathbb{Z}_N^*$   
 $c \leftarrow \rho(k, b) (= \alpha^k \cdot [b^N]_{N^2})$   
output  $c$ ;

*D*( $SK, c$ ):  
compute  $c^{\phi(N)} = \alpha^{k\phi(N)}$   
compute  $(\alpha^{k\phi(N)})^{\phi(N)^{-1} \pmod{N}} = \alpha^k$   
output  $k$  from  $\alpha^k$

The semantic security of Paillier encryption scheme is based on a slightly non-standard assumption.

**Assumption 8 (Decisional Composite Residuosity (DCR) assumption).** For  $N$  chosen as described above, it is the case that

$$\mathbb{Z}_{N^2}^* \stackrel{comp}{\approx} (\mathbb{Z}_{N^2}^*)^N$$

The DCR assumption essentially says that a random element of the group  $\mathbb{Z}_{N^2}^*$  is computationally indistinguishable from a random element of  $\mathbb{Z}_{N^2}^*$  of order  $\phi(N)$ . Given this assumption, it is easy to see that the adversary gets essentially no information regarding the message from the ciphertext  $c$ .

$$\begin{aligned} c &= \alpha^k \cdot [b^N]_{N^2} \quad \text{for random } b \in \mathbb{Z}_N^* \\ &\stackrel{comp}{\approx} \alpha^k \cdot \alpha^r \cdot [b_1^N]_{N^2} \quad \text{for random } r \in \mathbb{Z}_N \text{ and } b \in \mathbb{Z}_N^* \\ &= \alpha^{k+r} \cdot [b_1^N]_{N^2} \end{aligned}$$

The Paillier encryption scheme is especially interesting because it is a *Homomorphic PKE scheme*. That is, given a ciphertext for two messages  $k_1$  and  $k_2$ , one can compute the ciphertext for  $k_1 + k_2$  without knowing the secret key.

$$\begin{aligned} c_1 &= \alpha^{k_1} \cdot [b_1]_{N^2} \quad \text{and} \quad c_2 = \alpha^{k_2} \cdot [b_2]_{N^2} \\ \Rightarrow c_1 \cdot c_2 &= \alpha^{k_1+k_2} \cdot [b_1 \cdot b_2]_{N^2} \\ \Rightarrow D(SK, c_1 \cdot c_2) &= k_1 + k_2 \end{aligned}$$