Comparison Based Semantic Security is Probabilistic Polynomial Time Equivalent to Indistinguishability

Ali Bagherzandi[1,2], Javad Mohajeri[2], and Mahmoud Salmasizadeh[2]
(Corresponding author: Ali Bagherzandi)

Computer Engineering Department, Sharif University of Technology[1]
P. O. Box 11155-8639 Azadi Avenue 14588 Tehran, Iran (Email: bagherzandi@ce.sharif.edu)
Electronic Research Center, Sharif University of Technology[2]

(Received Dec. 31, 2005; revised and accepted Jan. 27, 2006)

Abstract

In this paper we try to unify the frameworks of definitions of semantic security, indistinguishability and non-malleability by defining semantic security in comparison based framework. This facilitates the study of relations among these goals against different attack models and makes the proof of the equivalence of semantic security and indistinguishability easier and more understandable. Besides, our proof of the equivalence of semantic security and indistinguishability does not need any intermediate goals such as non devidability to change the definition framework.

Keywords: Comparison based definition, indistinguishability, non-malleability, semantic security, simulator based definition

1 Introduction

The security of public key cryptosystems can be evaluated as achieving certain cryptographic goals such as semantic security, indistinguishability, non-malleability, plaintext awareness and non-devidability. In this paper we focus on semantic security and indistinguishability which has been defined in [5] for the first time. The latter is also known as polynomial security or Goldwasser-Micali security.

Roughly speaking, indistinguishability formalizes an adversary's inability to distinguish between two plaintexts given the encryption of one of them. It is rather an artificial goal but suggests an applicable method for evaluating security in provable security context. On the other hand, an encryption scheme is said to be semantically secure if no polynomially bounded adversary can be found to extract any partial information about the plaintext of a given ciphertext. Thus semantic security is a direct intuition of privacy and comparing whit Shannon's perfect security [7] it can be considered as the computational version of perfect security. Unlike indistinguishability, semantic security does not suggest any method for security evaluation.

The term "information" in the definition of semantic security can be modelled by functions from message space to $\sum^*$ in which $\sum$ is the alphabet of computation model. Proving that no such function exists for a cryptosystem implicitly proves the indistinguishability goal for that cryptosystem. Such a close relationship between indistinguishability and semantic security was firstly demonstrated in [5] as their equivalence. In the original definition of semantic security in [5] there is no restriction on the computability of the functions modelling information about plaintext. But as it has bean said in [6] what good would it do any adversary to "guess" a function if he can not even verify that his guess is correct. In later formulations of semantic security the functions modelling "information" restricted to be polynomially verifiable [8].

Another important turning point was introduced in [1]. Bellare et al. suggested that cryptographic goals to be studied in connection with attack models and not in isolation. Using this method, relations among indistinguishability and semantic security is discussed in [1] against chosen plaintext attack, non-adaptive chosen ciphertext attack and adaptive chosen ciphertext attack.

Semantic security can be formalized under two different frameworks namely simulator based and comparison based [9]. The simulator based definitions requests that for any adversary given a ciphertext there exists a poly-time algorithm called a simulator which succeeds in the attack (i.e. extracting non negligible information) without the ciphertext essentially as well as the adversary. The comparison based definition requests that any adversary in possession of the ciphertext obtains no advantage over one which performs only random guess. Since random guess can be regarded as a special case of simulation the comparison based notion may seem stronger than the

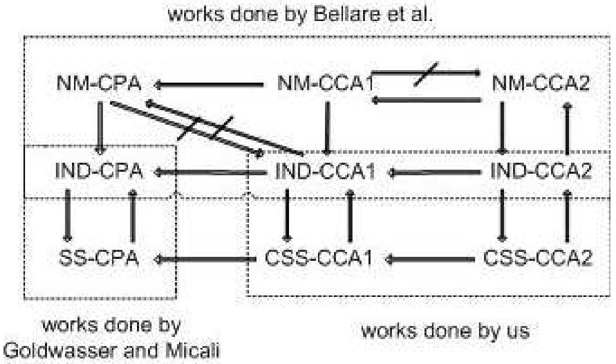


Figure 1: Relations among security notions

simulator-based one. On the other hand in the simulator based definition there is no restriction on the computability of partial information which an adversary wishes to extract while in the comparison based the partial information has to be efficiently generated and evaluated by a poly-time algorithm. This may show that the former is stronger than the latter.

In [1] non-malleability is defined in comparison based framework while in previous definitions [3, 4] it has bean defined using a simulator. Besides in [1] it has been shown that these two definitions are equivalent. Semantic security as defined in [8] is a simulator based one. Using this definition results in some contradictions as mentioned above and makes proving the equivalence between semantic security and indistinguishability difficult. Besides, the proof of the equivalence between semantic security and indistinguishability in this framework requires some other artificial security goals such as non-devidability to be defined in order to unify the definition frameworks.

In this paper using the idea in [1], we define semantic security in comparison based framework and study the relations between semantic security and indistinguishability against chosen plaintext attack (*cpa*), non-adaptive chosen ciphertext attack (*cca*1) and adaptive chosen ciphertext attack (*cca*2). Finally we suggest a simple and more understandable proof of equivalence of semantic security and indistinguishability.

Figure (1) shows the summary of works done in this category.

In Figure 1 the arrows indicate implication and the hatched arrows indicate the non implications. Thus the existence of a path from a pair of goal - attack $G_1 - A_1$ to $G_2 - A_2$ shows that if the goal G_1 in a cryptosystem is achieved in the sense of attack A_1 then goal G_2 is also achieved against attack A_2. For example if a cryptosystem is proved to be non-malleable against adaptive chosen ciphertext attack then it is semantically secure against chosen plaintext attack.

In Section 2 we introduce some preliminary definitions. Then in Section 3 we introduce our definition of comparison based semantic security as well as a slightly modified definition of indistinguishability based on comparison and then in Section 4 we study our proof of equivalence of semantic security and indistinguishability in the new framework.

2 Preliminary Definitions

Definition 1. Polynomially Verifiable Function. *The function $f : M \to \sum^*$ is said to be polynomially verifiable if there exists a probabilistic poly-time algorithm such that:*

$$\forall x \in M : A(x, f(x)) = 1 \text{ and } y \neq f(x) \Rightarrow A(x, y) = 0$$

In this definition M is the message space and $\sum^*$ is the whole information about plaintext.

Definition 2. Negligible Function. *The function $\epsilon : N \to R$ is negligible if*

1) $\forall n \in N : \epsilon(n) \geq 0$

2) $\forall c \geq 0 \exists k_c \ni \forall k \geq k_c \epsilon(k) < k^{-c}$

Definition 3. Public Key Encryption Scheme. *A public key encryption scheme $\Pi = (K, E, D)$ is a triple of algorithms such that:*

1) The key generation algorithm K is a probabilistic poly-time algorithm that takes a security parameter $k \in N$ as the input and outputs a pair (pk, sk) of matching public and secret keys,

2) The encryption algorithm E is a probabilistic poly-time algorithm that takes a public key pk and a message $x \in \{0,1\}^*$ as the input and outputs a ciphertext y,

3) The decryption algorithm D is a deterministic poly-time algorithm that takes a secret key sk and a ciphertext y as the input and outputs either a message $x \in \{0,1\}^*$ or a special symbol $\perp$, if no legal decryption can be found for y.

Definition 4. Adversary Model. *An adversary is modelled as a pair of probabilistic poly-time algorithms $A = (A_1, A_2)$.The exact purpose of each algorithm depends on the particular adversarial goal, but in general, in the first stage i.e. using A_1, the adversary given the public key seeks and outputs some test instance and in second stage the adversary is issued a challenge ciphertext y generated as a probabilistic function of the test instance in a manner depending on the goal. In addition, A_1 can output some state information that will be passed to A_2. The adversary $A = (A_1, A_2)$ is said to be successful if it passes the challenge.*

In chosen plaintext attack (*CPA*) the adversary can encrypt any arbitrary plaintext. In non-adaptive chosen ciphertext attack (*CCA1*) we give A_1 (the public key) and access to a decryption oracle but we do not allow A_2 access to a decryption oracle. Thus the decryption oracle can be used to generate test instance but is taken away before the challenge appears. In adaptive chosen ciphertext attack (*CCA2*) we continue to give A_1 the public key and the access to decryption oracle but we also give A_2 the access to the same decryption oracle, with the only restriction that the challenge ciphertext cannot be queried.

3 Definitional Contributions

3.1 Indistinguishability

Let $\Pi = (K, E, D)$ be a public key encryption scheme and $A = (A_1, A_2)$ be a polynomially bounded adversary. For $atk \in \{cpa, cca1, cca2\}$ and $k \in N$ and $b \in \{0, 1\}$, we define $Exp^{ind-atk-b}_{\Pi,A}(k)$ as below:

```
$Exp^{ind-atk-b}_{\Pi,A}(k)$
    $(pk, sk) \leftarrow K(k); (x_0, x_1, s) \leftarrow A_1^{0_1(.)}(pk);$
    $y \leftarrow E_{pk}(x_b); d \leftarrow A_2^{0_2(.)}(x_0, x_1, s, y);$
$return\ d.$
```

In which for any $x, x' \in M$ we have $|x| = |x'|$; and the adversary A has the oracle access to a decryption oracle as below:

if $atk = cpa$ *then* $O_1(.) = \epsilon$ *and* $O_2(.) = \epsilon$,
if $atk = cca1$ *then* $O_1(.) = D_{sk}(.)$ *and* $O_2(.) = \epsilon$,
if $atk = cca2$ *then* $O_1(.) = D_{sk}(.)$ *and* $O_2(.) = D_sk(.)$.

However in the case of $atk = cca2$, A_2 is not allowed to request the decryption of the challenged ciphertext y.

The advantage of the adversary which is a criterion of its correct guess is defined as the difference between the probability of outputting a correct I and the probability of outputting a wrong I.

In a formal setting the advantage of the adversary is defined to be

$$\begin{aligned} Adv^{ind-atk}_{\Pi,A}(k) &= Pr[Exp^{ind-atk-l}_{\Pi,A}(k) = 1] \\ &\quad -Pr[Exp^{ind-atk-0}_{\Pi,A}(k) = 1]. \end{aligned}$$

The public key encryption scheme $\Pi = (K, E, D)$ is said to be secure in the sense of IND_ATK if $\forall A$ $Adv^{ind-atk}_{PE,A}(k)$ is negligible.

3.2 Simulator Based Semantic Security

Let $A = (A_1, A_2)$ be an adversary attacking the public key encryption scheme $\Pi = (K, E, D)$. For $atk \in \{cpa, cca1, cca2\}$ and $k \in N$, $Exp^{sss-atk-1}_{\Pi,A}(k)$ and $Exp^{sss-atk-0}_{\Pi,A}(k)$ is defined to be,

```
$Exp^{sss-atk-1}_{\Pi,A}(k)$
    $(pk, sk) \leftarrow K(k); (M, s) \leftarrow A_1^{O_1(.)}(pk); x \leftarrow M;$
    $y \leftarrow E_{pk}(x); (v, f) \leftarrow A_2^{O_2(.)}(M, s, y)$
    $if\ v = f(x)\ then\ d \leftarrow 1$
    $else\ d \leftarrow 0;$
$return\ d.$
```

```
$Exp^{sss-atk-0}_{\Pi,A'}(k)$
    $(pk, sk) \leftarrow K(k); (M, s) \leftarrow A'_1(pk);$
    $x \leftarrow M; (v, f) \leftarrow A'_2(M, s)$
    $if\ v = f(x)\ then\ d \leftarrow 1$
    $else\ d \leftarrow 1$
$return\ d.$
```

In which for any $x, x' \in M$ we have $|x| = |x'|$; and the adversary A has the oracle access to a decryption oracle as below:

if $atk = cpa$ *then* $O_1(.) = \epsilon$ *and* $O_2(.) = \epsilon$
if $atk = cca1$ *then* $O_1(.) = D_{sk}(.)$ *and* $O_2(.) = \epsilon$
if $atk = cca2$ *then* $O_1(.) = D_{sk}(.)$ *and* $O_2(.) = Dsk(.)$.

However in the case of $atk = cca2$, A_2 is not allowed to request the decryption of the challenged ciphertext y.

The advantage of the adversary, $Adv^{sss-atk}_{\Pi,A,A'}(k)$, is defined to be

$$\begin{aligned} &Adv^{sss-atk}_{\Pi,A,A'}(k) \\ &= Pr[Exp^{sss-atk-1}_{\Pi,A}(k) = 1] - Pr[Exp^{sss-atk-0}_{\Pi,A'}(k) = 1]. \end{aligned}$$

The public key encryption scheme $\Pi = (K, E, D)$ is said to be secure in the sense of SSS_ATK if

$$\forall A \exists A' : Adv^{sss-atk}_{\Pi,A,A'}(k)\ is\ negligible.$$

3.3 Comparison Based Semantic Security

Let $A = (A_1, A_2)$ be an adversary attacking the public key encryption scheme $\Pi = (K, E, D)$. The adversary in the first phase of attack i.e. using algorithm A_1 takes as the input the public key pk and outputs the pair (M, s) in which the first component is a message space samplable in poly-time and the second component is any information that should be delivered from A_1 to A_2. Then a random message $x \in M$ is selected and encrypted by E_{pk} to produces the challenge ciphertext y. In the second phase of attack, the algorithm A_2 takes as the input the massage space, the state information and the challenge ciphertext i.e. (M, s, y) and outputs the pair (v, f). A random $x \in M$ is also selected by the algorithm *sample* using the information delivered to A_2.

The algorithm *sample* is said to be successful if the random that it selects satisfies the equation $v = f(x)$.

If the difference of the success of the adversary and the algorithm *sample* as a function of k, the security parameter, is a negligible function, then $\Pi = (K, E, D)$ is said to be secure in the sense of CSS_ATK.

In formal setting let $\Pi = (K, E, D)$ be a public key encryption scheme and $A = (A_1, A_2)$ be a polynomially bounded adversary. For $atk \in \{cpa, cca1, cca2\}$ and $b \in \{0, 1\}$ and $k \in N$ we define the experiment

$Exp^{css-atk-b}_{\Pi,A,Sample}(k)$ as below.

```
$Exp^{css-atk-b}_{\Pi,A,Sample}(k)$
    $(pk, sk) \leftarrow K(k); (M, s) \leftarrow A_1^{O_1(.)}(pk);$
    $x_1 \leftarrow M; y \leftarrow E_{pk}(x_1);$
    $x_0 \leftarrow Sample(M, s); (vf) \leftarrow A_2^{O_2(.)}(M, s, y);$
    $if\ v = f(x_b)\ then\ d \leftarrow 1;$
    $else\ d \leftarrow 0;$
$return\ d.$
```

In which for any $x, x' \in M$ we have $|x| = |x'|$; and the adversary A has the oracle access to a decryption oracle as below:

if $atk = cpa$ *then* $O_1(.) = \epsilon$ *and* $O_2(.) = \epsilon$
if $atk = cca1$ *then* $O_1 = D_{sk}(.)$ *and* $O_2 = \epsilon$
if $atk = cca2$ *then* $O_1(.) = D_{sk}(.)$ *and* $O_2(.) = D_{sk}(.)$.

However in the case of $atk = cca2$, A_2 is not allowed to request the decryption of the challenged ciphertext y.

The advantage of the adversary, $Adv^{css-atk}_{\Pi,A,A'}(k)$, is defined to be

$$\begin{aligned} Adv^{css-atk}_{\Pi,A,Sample}(k) &= Pr[Exp^{css-atk-1}_{\Pi,A,Sample}(k) = 1] \\ &\quad -Pr[Exp^{css-atk-0}_{\Pi,A,Sample}(k) = 1]. \end{aligned}$$

The public key encryption scheme $\Pi = (K, E, D)$ is secure in the sense of CSS_ATK if

$$\forall A \exists S : Adv^{css-atk}_{\Pi,A,Sample}(k)\ is\ negligible.$$

We can also define the two experiments above in the following experiment.

4 Relating IND and CSS

In this section we present two theorems to discuss the relation between comparison based semantic security and indistinguishability against CPA, $CCA1$ and $CCA2$. Theorem 1 studies the horizontal arrows in lower part of Figure 1 and Theorem 2 studies the vertical ones. Theorem 2 provides a direct reduction between CSS_ATK and IND_ATK, $ATK \in \{CPA, CCA1, CCA2\}$ and vice versa. Similar works has been done in [8] and [9] but the former studies the equivalence between indistinguishability and *simulator* based semantic security and it uses some artificial intermediate goals namely non-devidability to unify underlying frameworks and in the latter the direct reduction is presented between indistinguishability and two special cases of comparison based semantic security.

Theorem 1. *The public key encryption scheme* $\Pi = (K, E, D)$ *is secure in the sense of* $GOAL - CCA1$ *if it is secure in the sense of* $GOAL - CCA2$*; and it is secure in the sense of* $GOAL - CPA$ *if it is secure in the sense of* $GOAL - CCA1$ *for any* $GOAL \in \{IND, CCS\}$.

Proof. The proof is straight forward. However it is discussed here for completeness and to reveal the effectiveness of the adversary formalization introduced in previous section. Let $Res^O_{A,ATK}$ denotes the response of oracle O for the request from the adversary A under the attack mode $ATK \in \{CPA, CCA1, CCA2\}$. Obviously, we have:

$$\begin{aligned} Res^{O_1(.)}_{A_1,CPA} &\subset Res^{O_1(.)}_{A_1,CCA1} \subset Res^{O_1(.)}_{A_1,CCA2} \\ Res^{O_2(.)}_{A_2,CPA} &\subset Res^{O_2(.)}_{A_2,CCA1} \subset Res^{O_2(.)}_{A_2,CCA2}. \end{aligned}$$

So, the knowledge of adversary in $CCA2$ mode is more than its knowledge in $CCA1$mode. On the other hand the behavior of the adversary attacking a certain goal under different attack types is the same (The difference is modelled by the different responses of decryption oracle). So what an adversary can perform under $CCA2$ mode it can perform under $CCA1$ mode. Therefore, if an adversary can attack some $GOAL \in \{IND, CSS\}$ of a public key encryption scheme under $CCA1$ mode it can attack the same goal under $CCA2$. Thus if an encryption scheme is secure in the sense of $GOAL - CCA2$ then it is secure in the sense of $GOAL - CCA1$.

Similar argument can be set forth to prove if an encryption scheme is secure in the sense of $GOAL - CCA1$ then it is secure in the sense of $GOAL - CPA$. □

Theorem 2. *The public key encryption scheme* $\Pi = (K, E, D)$ *is secure in the sense of* CSS_ATK *if and only if it is secure in the sense of* IND_ATK*, for any attack* $ATK \in \{CPA, CCA1, CCA2\}$.

Proof. First we prove the "if" part of the theorem, namely $CSS\_ATK \Rightarrow IND\_ATK$: Suppose $\Pi = (K, E, D)$ is a public key encryption scheme that is secure in the sense of CSS_ATK but it is not secure in the sense of IND_ATK. For such an encryption scheme, there exists a poly-time adversary $A = (A_1, A_2)$ being able to distinguish between two plaintexts given their ciphertexts. Using $A = (A_1, A_2)$ as a subroutine, we construct the poly-time adversary $B = (B_1, B_2)$ that can extract some non-negligible information about some plaintext, given its ciphertext. Constructing B is straight forward; every poly-time algorithm that can distinguish between $x_0, x_1 \in M$, given their ciphertexts, will predict the value of the following function:

$$f : \{x_0, x_1\} \rightarrow \{0, 1\}$$
$$f(x) = \begin{cases} 0\ if\ x = x_0 \\ 1\ if\ x = x_1. \end{cases}$$

Thus the adversary $B = (B_1, B_)$ can be formalized as bellow:

```
$B_1^{O_1(\cdot)}(pk)$
    $(x_0, x_1, s) \leftarrow A_1^{O_1(\cdot)}(pk); M \leftarrow \{x_0, x_1\};$
$return\ (M, s).$
```

```
$B_2^{O_2(\cdot)}(M, s, y)$
    $d \leftarrow A_2^{O_2(\cdot)}(x_0, x_1, s, y); v \leftarrow d$
    $f : \{x_0, x_1\} \rightarrow \{0, 1\}$
    $f(x) = \begin{cases} 0\ if\ x = x_0 \\ 1\ if\ x = x_1 \end{cases}$
$return\ (v, f).$
```

Since A_1 and A_2 are poly-time algorithms, so are B_1 and B_2.

To prove that $B = (B_1, B_2)$ can attack the CSS goal of the encryption scheme we show $Adv_{\Pi,A}^{css-atk}(k)$ is non-negligible.

According to the definition of comparison based semantic security,

$$\begin{aligned} &Pr[Exp_{\Pi,A,Sample}^{css-atk-1}(k) = 1] \\ &\quad = Pr[(pk, sk)\overset{R}{\leftarrow}K(k); (M, s) \leftarrow B_1^{O_1(\cdot)}(pk); \\ &\qquad x_1 \leftarrow M; y \leftarrow E_{pk}(x_1); \\ &\qquad (v, f) \leftarrow B_2^{O_2(\cdot)}(M, s, y) : v = f(x_1)]. \end{aligned}$$

and

$$\begin{aligned} &Pr[Exp_{\Pi,A,Sample}^{css-atk-0}(k) = 1] \\ &\quad = Pr[(pk, sk)\underset{\leftarrow}{R}K(k); (M, s) \leftarrow B_1^{O_1(\cdot)}(pk); \\ &\qquad x_0 \leftarrow sample(M, s); \\ &\qquad (v, f) \leftarrow B_2^{O_2}(M, s) : v = f(x_0)]. \end{aligned}$$

But since the function f is deterministic,

$$\begin{aligned} &Pr[Exp_{\Pi,A,Sample}^{css-atk-1}(k) = 1] \\ &= Pr[A_2^{O_2(\cdot)}(x_0, x_1, s, y)\ outputs\ 1] \\ &= Pr[Exp_{\Pi,A}^{ind-atk-1}(k) = 1]. \end{aligned}$$

Similarly,

$$Pr[Exp_{\Pi,A,Sample}^{css-atk-0}(k) = 1] = Pr[Exp_{\Pi,A}^{ind-atk-0}(k) = 1].$$

Thus,

$$\begin{aligned} Adv_{\Pi,A}^{css-atk}(k) = &Pr[Exp_{\Pi,A,Sample}^{css-atk-1}(k) = 1] \\ &-Pr[Exp_{\Pi,A,Sample}^{css-atk-0}(k) = 1] \qquad (1) \\ Pr[Exp_{\Pi,A}^{IND-atk-1}&(k) = 1] - Pr[Exp_{\Pi,A}^{IND-atk-0}(k) = 1] \\ = Adv_{\Pi,A}^{ind-atk}&(k). \end{aligned}$$

So, whenever $Adv_{\Pi,A}^{ind-atk}(k)$ is non-negligible, neither is $Adv_{\Pi,A}^{css-atk}(k)$.

Note that Equation (1) holds whenever $Adv_{\Pi,A}^{ind-atk}(k)$ is not a negligible function (i.e IND_ATK can be performed against the encryption scheme). Therefore still we need to prove the "only if" part of the theorem; namely, $IND\_ATK \Rightarrow CSS\_ATK$:Again the proof is by contradiction.

Suppose $B = (B_1, B_2)$ is an adversary attacking semantic goal of the cryptosystem, i.e. can extract some non-negligible information about some plaintext given its corresponding ciphertext. The Adversary $A = (A_1, A_2)$ is constructed attacking the indistinguishability goal of the cryptosystem by using $B = (B_1, B_2)$ as a subroutine. The adversary $A = (A_1, A_2)$ is defined as bellow:

```
$A_1^{O_1(\cdot)}(pk)$
    $(M, s) \leftarrow B_1^{O_1(\cdot)}(pk); x_0, x_1 \leftarrow M;$
$return(x_0, x_1, s).$
```

```
$A_2^{O_2(\cdot)}(x_0, x_1, s, y)$
    $(v, f) \leftarrow B_2^{O_2(\cdot)}(M, s, y);$
    $if\ v = f(x_0)\ andv \neq f(x_1)\ then\ d \leftarrow 0;$
    $if\ v = f(x_1)\ andv \neq f(x_0)\ then\ d \leftarrow 1;$
    $else\ d\underset{\leftarrow}{R}\{0, 1\}$
$return\ d.$
```

Note that in order to distinguish between x_0 and x_1, one should make sure that the function f has different values over x_0 and x_1.

Since f is polynomially verifiable, we have: $B = (B_1, B_2)$ *runs in polynomial* $\Rightarrow A = (A_1, A_2)$ *runs in polynomial.*

To prove that $A = (A_1, A_2)$ can attack the IND goal of the encryption scheme we show $Adv_{\Pi,A}^{ind-atk}(k)$ is non-negligible.

The algorithm A_2 outputs the value 1 when:

1) $v = f(x_1)$ and $v \neq f(x_0)$ in which the output will deterministically be 1.

2) $v \neq f(x_1)$ and $v \neq f(x_0)$ in which the output will be 1 by the probability $\frac{1}{2}$.

Thus,

$$\begin{aligned} &Pr[Exp_{\Pi,A}^{IND-ATK-1}(k) = 1] \\ &\quad = Pr[A_2\ outputs\ 1 | y \leftarrow E_{pk}(x_1)] \\ &\quad = Pr[v = f(x_1)\ and\ v \neq f(x_0)] \qquad (2) \\ &\qquad + \frac{1}{2}(Pr[v \neq f(x_1)\ and\ v \neq f(x_0)] \\ &\qquad + Pr[v = f(x_1) and\ v = f(x_0)]). \end{aligned}$$

According to the definition of comparison-based semantic security, Equation 2 reduces to

$$\begin{aligned} &Pr[Exp_{\Pi,A}^{IND-ATK-1}(k) = 1] \\ &\quad = \frac{1}{2} + \frac{1}{2}(Pr[Exp_{\Pi,A}^{CSS-ATK-1}(k) = 1] \quad (3) \\ &\qquad -Pr[Exp_{\Pi,A}^{CSS-ATK-0}(k) = 1]). \end{aligned}$$

So, if a $CSS - ATK$ is applicable to a public key encryption scheme, the difference of probabilities above namely $pr[Exp_{\Pi,A}^{CSS-ATK-1}(k) = 1] - pr[Exp_{\Pi,A}^{CSS-ATK-0}(k) = 1]$ is non-negligible. Therefore, the probability $pr[Exp_{\Pi,A}^{IND-ATK-1}(k) = 1]$ is non-negligibly greater than $\frac{1}{2}$. And the adversary $A =$

(A_1, A_2) will be able to distinguish between x_0 and x_1 with a probability greater than $\frac{1}{2}$ by a non-negligible factor.

More formally one can evaluate $pr[Exp_{\Pi,A}^{IND-ATK-0}(k) = 1]$ in the same way and yield

$$\begin{aligned} pr[Exp_{\Pi,A}^{IND-ATK-0}(k) = 1] \\ = \frac{1}{2} + \frac{1}{2}(pr[Exp_{\Pi,A}^{CSS-ATK-0}(k) = 1] \quad (4) \\ -pr[Exp_{\Pi,A}^{CSS-ATK-1}(k) = 1]). \end{aligned}$$

Subtracting Equation (4) from Equation (3) yields:

$$\begin{aligned} & Adv_{\Pi,A}^{ind-atk}(k) \\ & = pr[Exp_{\Pi,A}^{IND-ATK-1}(k) = 1] \\ & \quad -pr[Exp_{\Pi,A}^{IND-ATK-0}(k) = 1] \\ & = pr[Exp_{\Pi,A}^{CSS-ATK-1}(k) = 1] \\ & \quad -pr[Exp_{\Pi,A}^{CSS-ATK-0}(k) = 1] \\ & = Adv_{\Pi,A}^{css-atk}(k). \end{aligned}$$

Thus, whenever $Adv_{\Pi,A}^{css-atk}(k)$ is non-negligible, so is $Adv_{\Pi,A}^{ind-atk}(k)$. □

5 Conclusion

In this paper, we formalized semantic security in comparison based framework. This unifies the definition frameworks of semantic security and indistinguishability and facilitates the study of relation between indistinguishability and semantic security against chosen plaintext attack, non-adaptive chosen ciphertext attack and adaptive chosen ciphertext attack removing the contradictions that was mentioned in the introduction. Then we provided two theorems to study the relations between security notions. We suggested a simple proof for the equivalence of semantic security and indistinguishability in the new setting. Our proof is more understandable than previous ones and does not need any intermediate goals such as non-devidability to be defined to change definition framework.

References

[1] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public key encryption schemes," in *Proceedings of Advances in Cryptology - Crypto'98*, LNCS 1462, pp. 26-45, Springer-Verlag, 1998.

[2] M. Bellare and A. Sahai, "Non-malleable encryption: Equivalence between two Notions, and an indistinguishability-based characterization," in *Proceedings of Advances in Cryptology - Crypto'98*, LNCS 1666, pp. 519-536, Springer-Verlag, 1998.

[3] D. Delov. C. Dework, and M. Naor, *Non-Malleable Cryptography*, Technical Report CS95-27, Weismann Institute of Science, 1995.

[4] D. Delov, C. Dework, and M. Naor, *Non-Malleable Cryptograph*, Manuscript, 1998.

[5] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, pp. 270-299, 1984

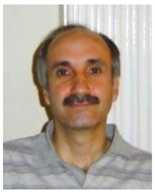
[6] S. Micali, C. Racko, B. Sloan, "The notion of security for probabilistic cryptosystems," *SIAM Journal of Computing*, vol. 17, no. 2, pp. 412-426, 1988.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.

[8] Y. Watanabe, J. Shikata, and H. Imai, "Equivalence between semantic security and indistinguishability against chosen ciphertext attacks," in *Proceedings of International Workshop on Practice and Theory in Public Key Cryptosystems - PKC 2003*, LNCS 2567, pp. 71-84, Springer-Verlag, 2003.

[9] Y. Watanabe and J. Shikata, *Relation among Simulator-Based and Comparison-Based Definitions of Semantic Security*, Cryptology ePrint Archive: Report 2003/078.

Ali Bagherzandi was born in 1983 in Urmia, Iran. He is a senior B.Sc. student in Computer Engineering department of Sharif University of Technology, Tehran, Iran, studying a dual degree program of computer science and hardware engineering. He has joined electronic research center of Sharif University of Technology as a research assistant in Jan 2005. He is the principal author of 5 refereed papers. His main research interests include theory of computation, foundations of cryptography and data and network security.



Javad Mohajeri received his B.Sc. in Mathematics from Isfahan University, Isfahan, Iran in 1986 and his M.S. in Mathematics from Sharif University of Technology, Tehran, Iran in 1990. He is a lecturer in the electronic research center of Sharif University of Technology. Javad Mohajeri has published 31 papers in refereed journals and conferences. He is a member of founding committee of Iranian Society of Cryptology. He was the chairman of the technical program committee of the 2nd Iranian society of cryptology conference on cryptology communications and computer security. His research interests include design and analysis of cryptographic algorithms, data security, secret sharing schemes and PKI.

Mahmoud Salmasizadeh received the B. S. and M. S. degrees in Electrical Engineering from Sharif University of Technology in Iran, in 1972 and 1989, respectively. He also received the Ph.D. degree in Information Technology from Queensland University of Technology in Australia, in 1997. Currently he is an assistant professor in Electronic Research Center and adjunct assistant professor in Electrical Engineering Department at Sharif University of Technology, Tehran, Iran. His research interests include cryptology and network security. He is the founding member and the head of scientific committee of Iranian Society of Cryptology.