NAIST-IS-DT0061012

Doctor's Thesis

Theoretical Classifications of Security Notions on Public-key Cryptosystems

Ako Suzuki

February 7, 2003

Department of Information Processing
Graduate School of Information Science
Nara Institute of Science and Technology

Doctor's Thesis
submitted to Graduate School of Information Science,
Nara Institute of Science and Technology
in partial fulfillment of the requirements for the degree of
DOCTOR of ENGINEERING

Ako Suzuki

Thesis committee:	Hiroyuki Seki, Professor
	Minoru Ito, Professor
	Kenichi Matsumoto, Professor
	Yuichi Kaji, Associate Professor

Theoretical Classifications of Security Notions on Public-key Cryptosystems[*]

Ako Suzuki

Abstract

The security of public-key cryptosystems is usually evaluated according to adversary's computational complexity necessary to achieve his/her malicious goal. Bellare et al. presented formal definitions of important properties, *non-malleability* and *indistinguishability*, of public-key cryptosystems under three different types of adversaries, and clarified the relationship among the properties. On the other hand, Goldreich proposed a formal definition of *one-wayness*, which is another important property of cryptosystems. The works by Bellare et al. and Goldreich were given independently, and relations between their results have not yet been clarified. Furthermore, other properties of public-key cryptosystems, not covered by their works, have not been discussed.

This thesis is to unify and extend the results by Bellare et al. and Goldreich. In the first part of the thesis, formal definitions of *equivalence undecidability* and *non-verifiability* are presented, and both of them are shown to be equivalent to indistinguishability. Both of them are important properties of public-key cryptosystems, but their formal definitions have not yet been considered. The second part of the thesis is devoted to presenting more detailed formalizations of non-malleability and one-wayness, and to clarifying relations among the original and our formalizations. In the proposed formalizations, an adversary is allowed to specify a message space from which a plaintext underlying the challenge ciphertext is chosen. Difference in the size of the message space essentially affects on the advantage of adversaries. In this thesis, three different levels are considered based on the size of the message space, and detailed formalizations are induced for each level. It is shown

[*] Doctor's Thesis, Department of Information Processing, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-DT0061012, February 7, 2003.

that some of our formalizations coincide with Bellare et al.'s and Goldreich's formalizations, thus the result can be regarded as a natural extension of the original results.

Keywords:

public-key cryptosystems, probabilistic algorithm, non-malleability, indistinguishability, one-wayness

Acknowledgements

By looking back this journey of research, there are many people have been involved in many ways. I would like to express my gratitude to all individuals who supported and collaborated with me to complete this thesis. I would like to thank my supervisor, Professor Hiroyuki Seki. He has been advising me to be a researcher from the first step and continuously supporting me throughout the research. Without his broad-mind and knowledge, I would never have kept working in the same track and have come to this far.

I am privileged to have Professor Hiroyuki Seki, Professor Minoru Ito, Kenichi Matsumoto and Associate Professor Yuichi Kaji as my thesis committee. I thank Professor Ito for advising from my master thesis. His lecture on computational theory helped understanding the basic theory of my research, and it has being my great asset. I thank Professor Matsumoto for valuable comments and critiques from a different point of view which enlighten me to reconsider the subject. I especially thank my advisor and collaborator, Associate Professor Yuichi Kaji. His spirit and stance toward the research encouraged me, and his keen insights and proper advice derived many breakthroughs with simple and clever way. I am proud of being a student of a wise and open-minded pioneer.

I would like to thank Professor Tadao Kasami at Hiroshima University, Professor Koji Torii, a president of Nara Institute of Science and Technology, and Professor Shinji Kimura at Waseda University, NAIST at the time, for giving me an opportunity to study at NAIST.

I thank Professor Toru Fujiwara at Osaka University for advising as a committee member of my master thesis and for giving me an opportunity to discuss with a study group.

I am grateful to Doctor Hajime Watanabe at Electrotechnical Laboratory for early discussion and advice, and for being a coauthor of my first paper, and I also thank to Mr. Takashi Kitagawa at Electrotechnical Laboratory for early discussion and for studying together.

I thank Professor Toyoo Takata at Iwate Prefectural University. His interesting lecture on Cryptography underlies my basic knowledge in the field.

I thank Associate Professor Yasunori Ishihara and Research Assistant Maki Yoshida at Osaka University for comments and discussion, and also letting me in the collaborative study group.

I thank Research Assistant Naoya Nitta for exchanging valuable information from the other research field of view and having discussion, and specially thank for being a colleague

and a good friend with your wonderful family.

Throughout my research years, I have benefited from many teachers, friends and fellows. I thank to all of them.

In addition to my research, my study abroad to the United States for undergraduate education became precious experiment along with my graduate years. I thank my all excellent teachers at Red Rocks Community College and University of Colorado at Boulder, and my all friends in the United States. I thank Mrs. Yuri Chandonnet and Mr. Naruo Sgawara for their support since then. Forever and ever my favorite English teacher is Professor Dee Worman who was an English teacher at NAIST. I would like to thank for correcting my papers and being my personal adviser and friend. I also thank Sadahiko Yamazaki, a president of Japan Microsystems Incorporation, for his support. My most thanks go to my all family members and relatives for supporting my student life. Specially, I would like to thank my parents who gave me these opportunities to have the best education as possible. And I would like to thank Doctor Fumio Suzuki for supporting and encouraging me as my best teacher and as a president of Abel Systems Incorporation. I could never have come this point without him, and I am proud of having him as my father. I dedicate this thesis to him.

List of Publications

Journal Papers

- Ako Suzuki, Yuichi Kaji and Hajime Watanabe, *Relations among Security Goals of Probabilistic Public-Key Cryptosystems*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Institute of Electronics, Information and Communication Engineers E84-A(1), pp. 172–178, Jan. 2001.

International Conferences

- Ako Suzuki, Yuichi Kaji and Hajime Watanabe, *Relations among Security Goals of Probabilistic Public-Key Cryptosystems*, Proceedings of the 2000 International Symposium on Information Theory and Its Applications (ISITA'00), pp. 657–660, Hawaii, U.S.A., Nov. 2000.

- Ako Suzuki and Yuichi Kaji, *Detailed Classification of Public-key Cryptosystems*, Proceedings of the 2002 International Symposium on Information Theory and Its Applications (ISITA'02), pp. 747–750, Xi'an, China, Oct. 2002.

Workshops

- Ako Suzuki, Yuichi Kaji and Hajime Watanabe, *Relations among Security Goals of Probabilistic Public-Key Cryptosystems*, Proceedings of the 2000 Symposium on Cryptography and Information Security (SCIS'00), A26, pp. 1–8, Jan. 2000.

- Shinichrou Kondoh, Ako Suzuki and Yuichi Kaji, *On the Formalizations of the Non-malleability and the One-wayness of Public Key Cryptosystems*, Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS'01), pp. 435–440, Jan. 2001.

- Ako Suzuki and Yuichi Kaji, *Does Non-malleability Really Imply Indistinguishability?*, Technical Report of IEICE, Institute of Electronics, Information and Communication Engineers, ISEC2001-15, May 2001.

- Koji Komori, Ako Suzuki and Yuichi Kaji, *On the Formalization of Non-malleability in Public-key Cryptosystems*, Proceedings of the 2002 Symposium on Cryptography and Information Security (SCIS'02), pp. 137–142, Jan. 2002 (in Japanese).

Master's Thesis

- Ako Suzuki, *Relations among Security Goals of Probabilistic Public-Key Cryptosystems*, Master's Thesis, NAIST-IS-MT9851052, Nara Institute of Science and Technology, 2000.

Contents

List of Figures

Chapter 1

Introduction

1.1. The Security of Public-key Cryptosystems

A public-key cryptosystem plays essential roles in modern computer networks. The primal property required for public-key cryptosystems is that nobody can decrypt ciphertexts without a proper decryption key. This property, however, is not sufficient to realize secure systems. The study of Bleichenbacher [10], briefly reviewed below, gives us a good example to illustrate the motivation behind our study.

PKCS #1 (Public-Key Cryptography Standards) [30] is the RSA encryption standard used in SSL (Secure Sockets Layer) [32] and other popular security mechanisms to provide confidentiality for exchanging symmetric encryption keys (digital envelopes), and for constructing digital signatures. PKCS family of standards for public-key cryptosystems consist of a number of components such as #1, #3, #5, #6, #7, #8, #9 and #10. These standards cover RSA encryption, Diffie-Hellman key agreement, password-based encryption, extended-certificate syntax, cryptographic message syntax, private-key information syntax and certification request syntax.

Currently, according to [10], PKCS #1 asserts plaintexts to be encrypted to satisfy a block format of k-byte length of the form

$$EB = 00\ 02||PS||00||D$$

where D is the information to be transmitted, 00 and 02 are hexadecimal representations of two bytes, PS is a padding string to make the block k-byte length, and $||$ denotes the concatenation of strings. The padding string PS is generated randomly but should not contain 00 inside. The byte 00 between PS and D is to separate PS and D. The sender converts the string EB to an integer m with the most significant byte first, encrypts m with the RSA scheme by the usual exponentiation, $c = m^e \bmod n$, and sends the ciphertext c to the recipient. The recipient decrypts the ciphertext c by computing $m = c^d \bmod n$, converts the integer m to a string EB, and checks that EB has the expected form. If EB has the valid form, then the recipient recovers the data value D; otherwise, an error message is returned to the sender.

Consider an implementation of the recipient of PKCS #1 which returns an error message if the string EB obtained by decrypting the ciphertext does not satisfy the expected form. In this case, an adversary can send a ciphertext y of his/her choice to the recipient, and observe the behavior of the recipient. If the recipient returns an error message after the adversary sent a ciphertext y, the adversary can find that the first two bytes of the plaintext of y is not 00 02. If the recipient does not return any error message, then the adversary can tell that the first two bytes of the plaintext of y is 00 02. Therefore, the adversary will be able to get partial information on the ciphertext of his/her choice using the recipient as if it were a decryption oracle which returns some information (in this case, the first two bytes) about the decryption result.

In the case of the RSA scheme employed in PKCS #1, there is a systematic way for the adversary to choose the ciphertexts to be tested by the decryption oracle so that he/she finally breaks a given ciphertext. For example, let $c = m^e \bmod n$ be the challenge ciphertext and the adversary does not know m. For any choice of an integer constant b, the adversary can obtain the ciphertext of bm, without knowing m, by computing $b^e c \bmod n$. By giving $b^e c \bmod n$ to the decryption oracle, he/she knows partial information on bm. Since b is chosen by the adversary, he/she can cancel the effect of b from the partial information, and obtain the partial information on m. By repeating such attacks using a different constant b, the adversary finally reveals the secret message m.

This example suggests us two important facts. First, decryption oracles are not merely theoretical facilities, but they do exist on the real-world network. Second, even if one cannot decrypt a ciphertext, he/she may reveal the secret message by making use of other defects of cryptosystems. In the case of RSA, the defect is that one can transform a ciphertext to another ciphertext so that their plaintexts are "meaningfully related." Therefore, it is important to discuss if a cryptosystem involves this kind of defects or not.

1.2. Related Works

With the recent development of computer and network technology, a public-key cryptosystem has become an important research subject, and many public-key cryptosystems have been proposed. For the long time, the security of public-key cryptosystems were discussed individually. Recently, some researchers try to establish a systematic and formal method to evaluate the security of cryptosystems. One important approach among such studies is to present formal conditions (requirements) for a cryptosystem to be secure. The condition can be regarded as a definition of security since a cryptosystem is secure if and only if it satisfies the condition.

When we discuss security of cryptosystems, we need to pay attention to two aspects; what the goals of adversaries are, and what the abilities of adversaries are. The goals of adversaries are, for example, to decrypt a given ciphertext without a key, to rewrite a plaintext underlying the given ciphertext, and so on. This idea was originally introduced by Naor [4]. Concerning such goals, cryptosystems are expected to satisfy some properties. Some of the important properties which are required to cryptosystems are *non-malleability*, *indistinguishability* and *one-wayness*. The non-malleability is first introduced by Dolev, Dwork and Naor [15, 16, 17] and its current revision [18], and the indistinguishability is introduced by Goldwasser and Micali [23]. Intuitively, the non-malleability is that an adversary cannot modify a ciphertext to another meaningfully related ciphertext without decryption; the indistinguishability is that an adversary cannot tell which one of the given two plaintexts is the decryption of a given ciphertext (either one is a decryption of the given ciphertext); the one-wayness is that an adversary cannot decrypt a ciphertext and obtain a plaintext. Three types of adversaries' abilities are: *chosen-plaintext attack* (CPA), *non-adaptive chosen ciphertext attack* (CCA1), and *adaptive chosen ciphertext attack* (CCA2). Under CPA, an adversary can obtain the ciphertext from a plaintext of his/her choice. Under CCA1, formalized by Naor and Yung [26], in addition to the CPA case, an adversary can also have access to a decryption oracle before obtaining a challenge ciphertext y. Under CCA2, formalized by Rackoff and Simon [29], an adversary can have access to a decryption oracle any time even after he/she obtained the challenge ciphertext y. The only restriction is that the adversary cannot ask the oracle to decrypt y itself.

The adaptive chosen ciphertext attack has been considered to be an unrealistic attack model; however, Bleichenbacher showed that it is realistic in some situations as we saw in

Section 1.1. Thus the realization of public-key encryption schemes which are robust against the adaptive chosen ciphertext attack is an important subject, not only in a theoretical sense but in a practical sense.

To provide secure encryption scheme, an enhancement scheme of existing cryptosystems, known as OAEP (Optimal Asymmetric Encryption Padding) [7], is proposed and employed by RSA Laboratories. OAEP is said to be secure against chosen ciphertext attack, if the underlying cryptosystem has certain robustness. Besides OAEP, there are other conversion schemes which also make use of with hash functions, [21, 22]. A conversion of weak public-key and weak symmetric-key encryption schemes into a strong public-key encryption scheme against CCA2 is presented in [20]. These techniques are based on the random oracle model [6] in which we assume that there are random hash functions. It is considered that a random hash function is easier to construct than one-way functions or pseudo-random functions which output ideal random strings. For a practical example, one can construct a random hash function by using DES (Data Encryption Standard) [19], which converts a simple input to a complex output.

Different from the approach to enhance existing cryptosystems, there is an approach to develop a cryptosystem which is robust against chosen ciphertext attacks by nature. Such cryptosystems are called probabilistic public-key encryption schemes. In probabilistic public-key encryption schemes, there are exponentially many ciphertexts for a single plaintext, and an encryption algorithm probabilistically chooses one of them as an encryption of the plaintext. It has been proved that appropriately designed probabilistic public-key encryption schemes are robust against chosen ciphertext attacks. Such schemes include CS (Cramer and Shoup) [14] and EPOC (Efficient Probabilistic Public-Key Encryption) [27, 28] encryption schemes. Only these two schemes and OAEP are proven to be secure against chosen ciphertext attack.

Bellare et al. considered two security properties, non-malleability and indistinguishability against CPA, CCA1 and CCA2. They proposed six security notions NM-CPA, NM-CCA1, NM-CCA2, IND-CPA, IND-CCA1 and IND-CCA2 as formal definitions of non-malleability and indistinguishability against the above three adversary models. The remarkable point of Bellare et al.'s work is that the formalizations are given in terms of the theory of computational complexity. In the theory of computational complexity, it is possible to reduce a problem A to another problem B, which means that solving A is not more difficult than solving B. By considering similar reductions between security notions, we can discuss the relationship among security notions. Actually, Bellare et al. completely clarified the relations among the six notions which they proposed. On the other hand, as for one-wayness of cryptosystems, the study of Goldreich is remarkable. Goldreich presented a formal definition of one-way functions, which can be straightforwardly converted to a Bellare-style definition of one-wayness (OW-ATK) for cryptosystems. However, the relations among OW-ATK, NM-ATK and IND-ATK are not known.

There are many related work around this topic. For example, [11, 31] discuss the relation between the indistinguishability and the semantic security. The security notions on symmetric-key cryptosystems against CPA is presented in [3], and against CCA is in [13]. Security notions required in multicast [2], blind signatures [1], key exchange [12], etc. are also discussed.

1.3. Contents of the Thesis

This study is to fill the uncovered topics on security notions of public-key cryptosystems by providing new formalizations, showing relations, and unifying and generalizing the formalizations of Bellare et al. and Goldreich. In Chapter 2, we review some previous works by Bellare et al. and Goldreich. In Chapter 3, we discuss properties of cryptosystems which were not considered by Bellare et al. and Goldreich. The properties we consider are *equivalence undecidability* and *non-verifiability*. Equivalence undecidability (EU) is the property such that an adversary cannot make a decision whether decryptions of two given ciphertexts y and y' are the same or not. Non-verifiability (NV) is the property such that an adversary cannot verify whether a challenge ciphertext y is an encryption of a given plaintext x or not. By combining these goals with the three attack models, we can consider six more notions of security. Formalizations of these new notions are presented, and the relation among these new notions and those of Bellare et al. is discussed. The result is that equivalence undecidability, non-verifiability and indistinguishability are all equivalent in the sense of security. In Chapter 4, we consider formalizations of non-malleability and one-wayness which are different from those of Bellare et al. and Goldreich. When we consider these properties in a formal way, an adversary is represented as a pair of polynomial-time algorithms (A_1, A_2), where A_1 performs a kind of "precomputaion" and A_2 attacks the challenge ciphertext. In the formalization of NM-ATK by Bellare, A_1 outputs a set of plaintexts (message space). An encryption oracle chooses a message in the specified message space, and constructs a challenge by encrypting the chosen message. We need to remark that the size of the message space affects essentially the advantage of adversaries. Choosing a small message space makes A_2 more advantageous, while choosing a message space larger makes it more difficult to attack. In the case of NM-ATK, there is no lower-bound limit on the size of the message space and an adversary can choose a very small message space. This models a very powerful adversary, and it makes NM-ATK very strong security notion. Surely such a powerful adversary model is interesting from the theoretical viewpoint, but it might be too much as a model of practical adversaries. In this thesis, we consider three different formalizations of non-malleability and one-wayness according to the lower-bound limit on the size of the message space. We clarify the relation among the original and our formalizations, showing that NM-ATK and OW-ATK (formalization of one-wayness by Goldreich) coincide with some of our formalizations. Hence the results by Bellare and Goldreich are unified and subsumed in our results. In Chapter 5, we conclude the thesis by summarizing results and discuss some future works.

Chapter 2

Preliminary

2.1. Notations

We use the standard notations and conventions for writing probabilistic algorithms and experiments. If A is a probabilistic algorithm, then $A(x_1, x_2, ..., x_n; r)$ is the result of running A on inputs $x_1, x_2, ..., x_n$ using a random sequence r. We write $y \leftarrow A(x_1, x_2, ..., x_n)$ to denote the experiment of picking r at random and letting y be the output of $A(x_1, x_2, ..., x_n; r)$. For a finite set S, let $x \leftarrow S$ be the operation of picking an element uniformly from S. If α is neither an algorithm nor a set then $x \leftarrow \alpha$ is a simple assignment statement. We say that y can be an output of $A(x_1, x_2, ..., x_n)$ if there exists r such that $A(x_1, x_2, ..., x_n; r) = y$.

A public-key encryption scheme is given by a triple of algorithms, $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, where

- $\mathcal{K}$, the *key generation algorithm*, is a probabilistic algorithm that takes a unary security parameter $k \in \mathbf{N}$ (key length for example) and returns a pair (pk, sk) of matching public and secret keys.

- $\mathcal{E}$, the *encryption algorithm*, is a probabilistic algorithm that takes a public key pk and a message $x \in \{0,1\}^*$ and produces a ciphertext y. It is emphasized that the encryption is a probabilistic operation. Even if the same pair of pk and x are given to the algorithm, the ciphertext y is not always the same.

- $\mathcal{D}$, the *decryption algorithm*, is a deterministic algorithm which takes a secret key sk and a ciphertext y and produces a message $x \in \{0,1\}^*$, or a special symbol $\perp$ to indicate that the ciphertext was invalid.

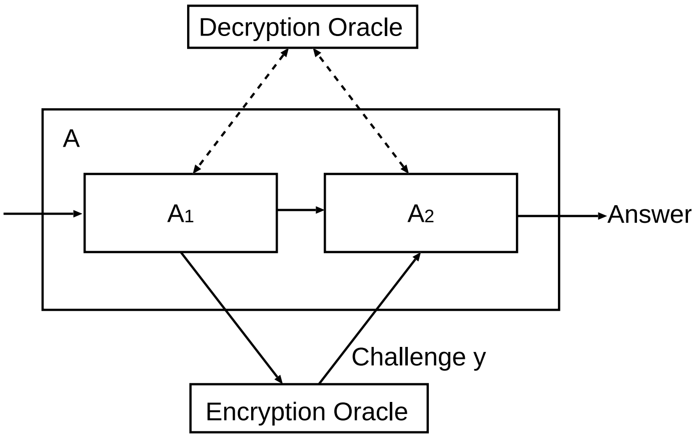

Figure 2.1. The adversary model

For each (pk, sk) which is the output of $\mathcal{K}(1^k)$, for each $x \in \{0,1\}^*$, and for each y which is the output of $\mathcal{E}_{pk}(x)$, we require that $\mathcal{D}_{sk}(y) = x$. The keys for the encryption and decryption are indicated as subscripts to the algorithms.

We say that $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is probabilistic if a plaintext is encrypted to a ciphertext in exponentially many different ways. That is, $\{y : y \leftarrow \mathcal{E}_{pk}(x)\}$ contains exponential number of ciphertexts to the security parameter (such as the length of keys). Thus a polynomial-time adversary cannot enumerate all ciphertexts of given x and pk.

As in Figure 2.1, an adversary is modeled by a pair of probabilistic polynomial-time algorithms $A = (A_1, A_2)$, where A_1 performs computation before a *challenge* is given, and A_2 performs computation after the challenge is given. A *challenge* is a ciphertext for which an adversary tries to attack, and chosen by an *encryption oracle* which is an entity different from the adversary. An algorithm is superscripted by an oracle. For example, $A_i^{\mathcal{O}_i}$ denotes an algorithm A_i which can use an algorithm $\mathcal{O}_i$ as an oracle. A function ϵ: $\mathbf{N} \to \mathbf{R}$ is *negligible* if, for any constant $c \geq 0$, there exists an integer k_c such that $\epsilon(k) \leq k^{-c}$ for all $k \geq k_c$.

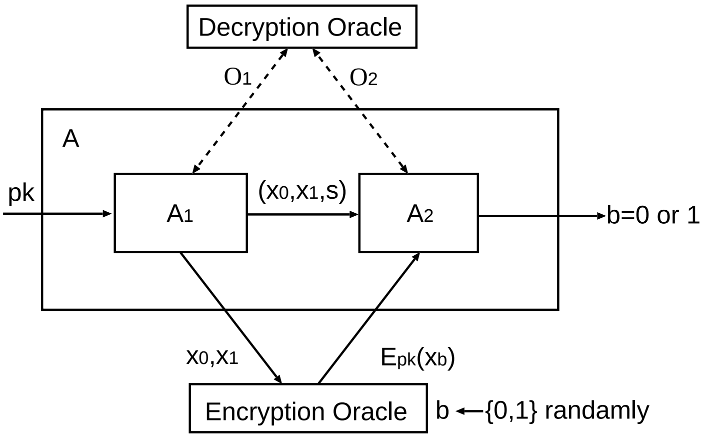

Figure 2.2. The IND adversary model

2.2. Previous Works

Prior to our research, Bellare et al. presented a formal definition of non-malleability and indistinguishability with three attack models [4]. In the following sections, we briefly review their formalizations.

2.2.1 Indistinguishability (IND)

The indistinguishability is one notion of the security of probabilistic public-key encryption scheme. Intuitively, a scheme is indistinguishable if any adversary cannot learn any information about the plaintext of the challenge ciphertext. Formally, an adversary for the indistinguishability is a pair of probabilistic algorithms (A_1, A_2) (Figure 2.2). The algorithm A_1 takes the public key pk as an input, and outputs a triple (x_0, x_1, s), the first two components being messages (of the same length), and the last component being the state information (possibly including pk) which are useful for A_2. The encryption oracle receives the output (x_0, x_1, s) of A_1, and generates $b \in \{0, 1\}$ randomly. Then, the challenge ciphertext is determined so that $y = \mathcal{E}_{pk}(x_i)$ and is sent to A_2. The algorithm A_2 receives the challenge ciphertext y from the encryption oracle, and (x_0, x_1, s) from A_1. Then A_2 determines whether $y = \mathcal{E}_{pk}(x_0)$ or $y = \mathcal{E}_{pk}(x_1)$. Bellare et al. considered the indistinguishability for the CPA, CCA1 and CCA2 attacks.

Definition 1: [4] Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa, cca1, cca2} and $k \in \mathbf{N}$, define

$$\begin{aligned}\mathrm{Adv}^{\text{ind-atk}}_{A,\Pi}(k) = 2 \cdot \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &b \leftarrow \{0,1\}; y \leftarrow \mathcal{E}_{pk}(x_b) : A_2^{\mathcal{O}_2}(x_0, x_1, s, y) = b] - 1.\end{aligned}$$

The oracle is defined as follows where $\mathcal{O}_i(\cdot) = \varepsilon$ means that no oracle is available;

if atk=cpa then $\mathcal{O}_1(\cdot) = \varepsilon$ and $\mathcal{O}_2(\cdot) = \varepsilon$,
if atk=cca1 then $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ and $\mathcal{O}_2(\cdot) = \varepsilon$, and
if atk=cca2 then $\mathcal{O}_1(\cdot) = \mathcal{D}_{sk}(\cdot)$ and $\mathcal{O}_2(\cdot) = \mathcal{D}_{sk}(\cdot)$.

We also assume that A_1 outputs distinct plaintexts x_0 and x_1 with $|x_0| = |x_1|$. In the case of CCA2, A_2 is not allowed to ask its oracle to decrypt y. The encryption scheme Π is said to be secure in the sense of IND-CPA, IND-CCA1 and IND-CCA2 if $\mathrm{Adv}^{\text{ind-cpa}}_{A,\Pi}(k)$, $\mathrm{Adv}^{\text{ind-cca1}}_{A,\Pi}(k)$ and $\mathrm{Adv}^{\text{ind-cca2}}_{A,\Pi}(k)$ are negligible for any adversary A, respectively. □

2.2.2 Non-Malleability (NM)

The non-malleability is a notion of security of public-key encryption scheme concerning the forgeability of ciphertexts. In some public-key encryption scheme, we can convert a ciphertext y to another ciphertext y', without decrypting y, so that the plaintexts of y and y' are meaningfully related. For example, consider RSA and let y be a ciphertext of RSA. For any positive integer c, we can obtain a ciphertext of a message $c \cdot \mathcal{D}_{sk}(y)$ by computing $c^e \cdot y \bmod n$ where e and n are public encryption keys. Such property helps adversary attacking the encryption scheme [10]. A scheme is non-malleable if the scheme does not have such a property.

To discuss the non-malleability in a more formal way, some notations to deal with vectors of plaintexts or ciphertexts are introduced. A vector is denoted in boldface, as in $\mathbf{x}$. The number of components in $\mathbf{x}$ is denoted $|\mathbf{x}|$, and $\mathbf{x}[i]$ denotes the i-th component, therefore, $\mathbf{x} = (\mathbf{x}[1], ..., \mathbf{x}[|\mathbf{x}|])$. The set membership notation is extended to vectors so that $x \in \mathbf{x}$ if and only if $x \in \{\mathbf{x}[i] : 1 \leq i \leq |\mathbf{x}|\}$. It will be convenient to extend the decryption notation so that operations are performed componentwise. Thus $\mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y})$ is the shorthand for the following:

$$\textbf{for } 1 \leq i \leq |\mathbf{y}| \textbf{ do } \mathbf{x}[i] \leftarrow \mathcal{D}_{sk}(\mathbf{y}[i]).$$

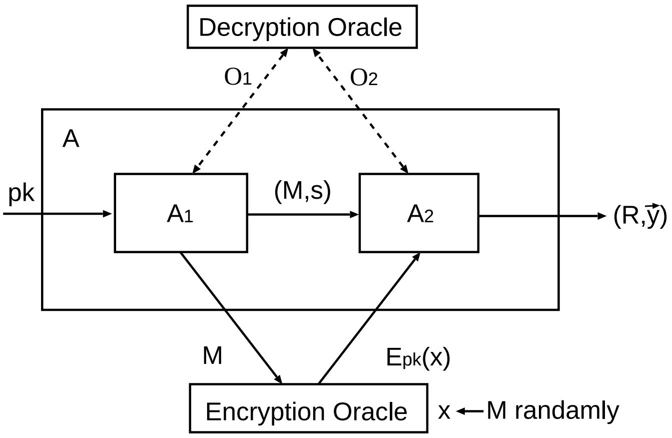

Figure 2.3. The NM adversary model

A *relation* is a boolean predicate on plaintexts or ciphertexts. Usually, a relation R with t parameters is written as $R(x_1, ..., x_t)$. We also use the notation $R(x, \mathbf{x})$ with $\mathbf{x} = (x_1, ..., x_{t-1})$ to represent $R(x, x_1, ..., x_{t-1})$. A simple example of relations is a "complement" relation $R(x_0, x_1)$ which is true if and only if x_0 and x_1 have the same length, and x_0 is the bitwise complement of x_1. Another example is an "identity" relation $R(x_0, x_1)$ which is true if and only if $x_0 = x_1$. The identity relation can be extended to a relation with t parameters so that $R(x_1, ..., x_t)$ is true if and only if there is $i \in \{2, ..., t\}$ such that $x_1 = x_i$.

Given a challenge ciphertext y, the goal of the adversary is not to learn something about its plaintext x, but to output a vector $\mathbf{y}$ of ciphertexts whose decryption $\mathbf{x}$ is "meaningfully related" to x, meaning that there is a relation R (which is not the identity relation) and the probability that $R(x, \mathbf{x})$ is true for the vector $\mathbf{x}$ is non-negligibly larger (or smaller) than the probability that $R(\tilde{x}, \mathbf{x})$ is true for a randomly chosen $\tilde{x}$.

Let $A = (A_1, A_2)$ be an adversary (Figure 2.3). In the first stage of the adversary's attack, A_1 is given the public key *pk*, and outputs a subset M of the message space of the encryption scheme. The encryption oracle randomly chooses a message $x \in M$, encrypts x, and sends $\mathcal{E}_{pk}(x)$ to the adversary. In the second stage of the adversary's attack, A_2 receives an encryption y of a random message $x \in M$. The adversary then outputs a description of a relation R and a vector $\mathbf{y}$ which should not contain y itself as a component, hoping that

$R(x, \mathbf{x})$ holds where $\mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y})$. An adversary is *successful* if the probability that $R(x, \mathbf{x})$ is true is significantly more than the probability that $R(\tilde{x}, \mathbf{x})$ is true for some random $\tilde{x} \leftarrow M$.

Definition 2: [4] Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and let $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa,cca1,cca2} and $k \in \mathbf{N}$, define

$$\mathrm{Adv}^{\text{nm-atk}}_{A,\Pi}(k) = |\mathrm{Succ}^{\text{nm-atk}}_{A,\Pi}(k) - \mathrm{Succ}^{\text{nm-atk}}_{A,\Pi,\$}(k)|$$

where

$$\begin{aligned}\mathrm{Succ}^{\text{nm-atk}}_{A,\Pi}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (M, s) \leftarrow A_1^{\mathcal{O}_1}(pk); x \leftarrow M; y \leftarrow \mathcal{E}_{pk}(x);\\ &(R, \mathbf{y}) \leftarrow A_2^{\mathcal{O}_2}(M, s, y); \mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y}) : y \notin \mathbf{y} \wedge \perp \notin \mathbf{x} \wedge R(x, \mathbf{x})],\end{aligned}$$

and

$$\begin{aligned}\mathrm{Succ}^{\text{nm-atk}}_{A,\Pi,\$}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (M, s) \leftarrow A_1^{\mathcal{O}_1}(pk); x, \tilde{x} \leftarrow M; y \leftarrow \mathcal{E}_{pk}(x);\\ &(R, \mathbf{y}) \leftarrow A_2^{\mathcal{O}_2}(M, s, y); \mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y}) : y \notin \mathbf{y} \wedge \perp \notin \mathbf{x} \wedge R(\tilde{x}, \mathbf{x})].\end{aligned}$$

The oracle to be used is the same as IND-ATK. We say that Π is secure in the sense of NM-CPA, NM-CCA1 and NM-CCA2 if $\mathrm{Adv}^{\text{nm-cpa}}_{A,\Pi}$, $\mathrm{Adv}^{\text{nm-cca1}}_{A,\Pi}$ and $\mathrm{Adv}^{\text{nm-cca2}}_{A,\Pi}$ are negligible for any adversary A, respectively. □

The condition $y \notin \mathbf{y}$ is to exclude identity relations. Without this condition the adversary can output the identity relation R and $\mathbf{y} = (y)$, and be successful with probability one. The adversary is unsuccessful when some ciphertext $\mathbf{y}[i]$ does not have a valid decryption, $\perp \in \mathbf{x}$, because in this case, the receiver is simply going to reject the adversary's message.

2.2.3 Relations between IND and NM

Bellare et al. showed implication and separation results among six definitions presented in Definitions 1 and 2. Fig.2.4 summarizes their result[1].

For security notions α and β, we write

[1] The figure is drawn in a different manner from [4] for simplicity, but it represents the same relations among the presented notions.

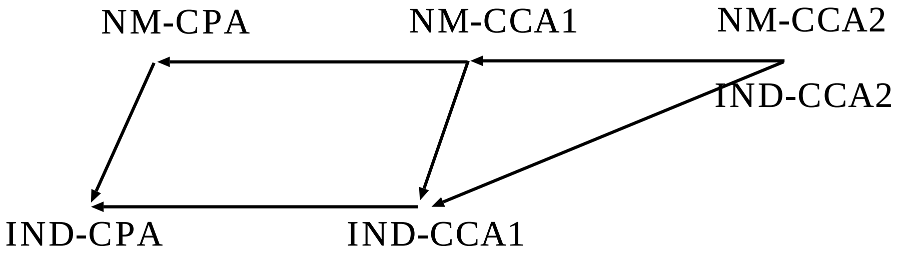

Figure 2.4. IND-ATK and NM-ATK

- $\alpha \Rightarrow \beta$ to mean that if Π is an encryption scheme which meets the security notion α, then Π also meets the security notion β.
- $\alpha \not\Rightarrow \beta$ to mean that even if Π meets the security notion α, Π does not always meet the security notion β.

Theorem 1: NM-ATK ⇒ IND-ATK
If encryption scheme Π *is secure in the sense of* NM-ATK, *then* Π *is secure in the sense of* IND-ATK *for any attack* ATK $\in$ {CPA, CCA1, CCA2}. □

Theorem 2: IND-CCA2 ⇒ NM-CCA2 □

Theorem 3: IND-CCA1 $\not\Rightarrow$ NM-CPA
Even if an encryption scheme Π *is secure in the sense of* IND-CCA1, Π *is not always secure in the sense of* NM-CPA. □

Theorem 4: NM-CPA $\not\Rightarrow$ IND-CCA1 □

Theorem 5: NM-CCA1 $\not\Rightarrow$ NM-CCA2 □

In the figure, if there is a directed path from α to β, then it means that a cryptosystem which is secure in the sense of α is always secure in the sense of β. If there is no directed path from α to β, then the security in the sense of α does not always implay the security in the sense of β.

2.2.4 One-wayness (OW)

To the authors' knowledge, one-wayness of public-key cryptosystems is not discussed explicitly in the context of the formal definitions for security notions. Even so Goldreich has presented a formal definition for a function to be one-way[24].

Definition 3: [24] A one-way function f is a polynomial-time computable function such that for every probabilistic polynomial-time algorithm A, for every positive polynomial $p(\cdot)$, and for all sufficiently large k's, we define

$$\sum_{x\in\{0,1\}^k} 2^{-k}\cdot \Pr[A(f(x)) \in f^{-1}(f(x))] < \frac{1}{p(k)}.$$

□

The definition is for a general function rather than encryption functions. Also, we remark that the sum is over all binary strings of length k. If we translate the above definition to Bellare-style formalization, then we have a following formal definition of one-wayness.

Definition 4: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa, cca1, cca2} and $k \in \mathbf{N}$, define

$$\begin{aligned}\mathrm{Adv}^{\text{ow-atk}}_{A,\Pi}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); s \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x \leftarrow \{0,1\}^k; y \leftarrow \mathcal{E}_{pk}(x); z \leftarrow A_2^{\mathcal{O}_2}(s, y) : x = z].\end{aligned}$$

The oracle to be used is the same as IND-ATK. The encryption scheme Π is said to be secure in the sense of OW-CPA, OW-CCA1 and OW-CCA2 if $\mathrm{Adv}^{\text{ow-cpa}}_{A,\Pi}(k)$, $\mathrm{Adv}^{\text{ow-cca1}}_{A,\Pi}(k)$ and $\mathrm{Adv}^{\text{ow-cca2}}_{A,\Pi}(k)$ are negligible for any adversary A, respectively. □

Chapter 3

New Security Notions for Public-Key Cryptosystems

3.1. Equivalence Undecidability (EU)

A new notion of security of cryptographic schemes, named equivalence undecidability, is proposed in this section. This notion is related to a goal of an adversary who tries to intrude an electric voting system, for example. Consider a simple system such that the voting is made by encrypting "yes" or "no" and sending the ciphertext to the server of the system (See, Fig. 3.1).

The primal requirement to the voting system is that an adversary cannot know from the ciphertext y_i which of yes or no the voter i made. In addition to the primal requirement, it is often required that the adversary cannot know whether two voting ciphertexts y_i and y_j are encryptions of an identical plaintext or not ("yes" or "no"). The equivalence undecidability is to deal with the latter requirement. An adversary is given two ciphertexts, and decides whether the two ciphertexts are encryptions of an identical plaintext or not.

Formally, an adversary $A = (A_1, A_2)$ behaves as follows. Algorithm A_1 takes a public key pk as an input, and outputs a pair (M, s) where the first component is a subset of messages, and the second component is the state information which will be passed to A_2. An encryption oracle randomly chooses two messages $x_0, x_1 \in M$, and computes two ciphertexts $y = \mathcal{E}_{pk}(x_0)$ and $y' = \mathcal{E}_{pk}(x_b)$ where $b \in \{0, 1\}$ is randomly chosen. The algorithm A_2 determines if decryptions of y and y' are the same or not. Figure 3.2 sketches

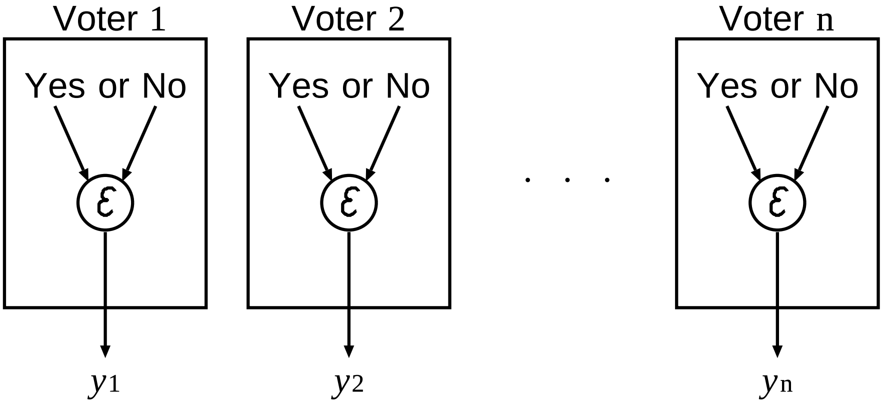

Figure 3.1. An example of EU in the electronic election

the above adversary.

Definition 5: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and let $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa, cca1, cca2} and $k \in \mathbf{N}$, let

$$\begin{aligned}\mathrm{Adv}^{\mathrm{eu-atk}}_{A,\Pi}(k) = 2 \cdot \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s) \leftarrow A_1^{\mathcal{O}_1}(pk); x_0, x_1 \leftarrow M;\\ &b \leftarrow \{0,1\}; y \leftarrow \mathcal{E}_{pk}(x_0); y' \leftarrow \mathcal{E}_{pk}(x_b) : A_2^{\mathcal{O}_2}(s, y, y') = b] - 1.\end{aligned}$$

The oracle to be used is the same as IND-ATK. We say that Π is secure in the sense of EU-CPA, EU-CCA1 and EU-CCA2 if $\mathrm{Adv}^{\text{eu-cpa}}_{A,\Pi}$, $\mathrm{Adv}^{\text{eu-cca1}}_{A,\Pi}$ and $\mathrm{Adv}^{\text{eu-cca2}}_{A,\Pi}$ are negligible for any adversary A, respectively. □

3.2. Non-Verifiability (NV)

The next notion we consider is the non-verifiability. The notion has relationship to a goal of an adversary who tries to intrude, for example, an anonymous electronic bids system. Consider the following simple example. For a certain item, users of the system make price, and send the encryption of the price to the server of the system. A user who makes the largest price is the winner. The server opens the largest price, but the name of the winner is kept anonymous. (See Figure 3.3.)

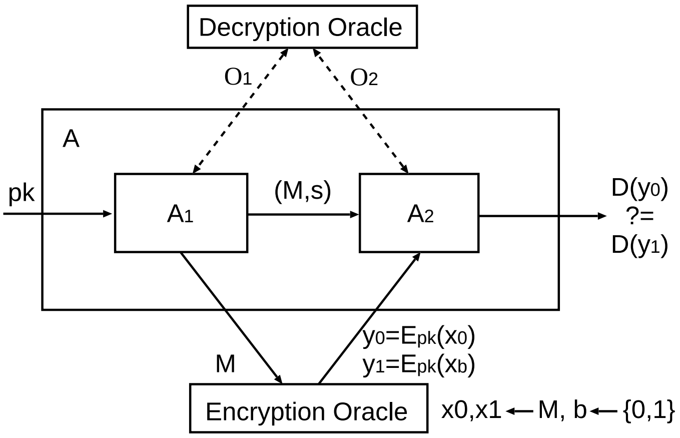

Figure 3.2. The EU adversary model

An intruder who knows the largest price tries to find who the winner is, by examining the ciphertexts sent from users. Thus, an adversary is given a plaintext x and a ciphertext y, and decides if y is an encryption of x.

Formally, an adversary $A = (A_1, A_2)$ behaves as follows. In the first stage of the adversary's attack, A_1 takes a public key pk, and outputs a subset M of the message space. An encryption oracle randomly chooses two messages $x_0, x_1 \in M$, and also chooses $b \in \{0,1\}$ randomly. Then the plaintext x_0 and the ciphertext $y = \mathcal{E}_{pk}(x_b)$ is sent to the adversary. The algorithm A_2 verifies if y is an encryption of x_0 or not. Figure 3.4 shows a adversaries' model of NV.

Definition 6: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and let $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa,cca1,cca2} and $k \in \mathbf{N}$, let

$$\mathrm{Adv}^{\mathrm{nv-atk}}_{A,\Pi}(k) = |\mathrm{Succ}^{\mathrm{nv-atk}}_{A,\Pi}(k) - \mathrm{Succ}^{\mathrm{nv-atk}}_{A,\Pi,\$}(k)|$$

where

$$\mathrm{Succ}^{\mathrm{nv-atk}}_{A,\Pi}(k) = \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s) \leftarrow A_1^{\mathcal{O}_1}(pk); x_0 \leftarrow M;$$

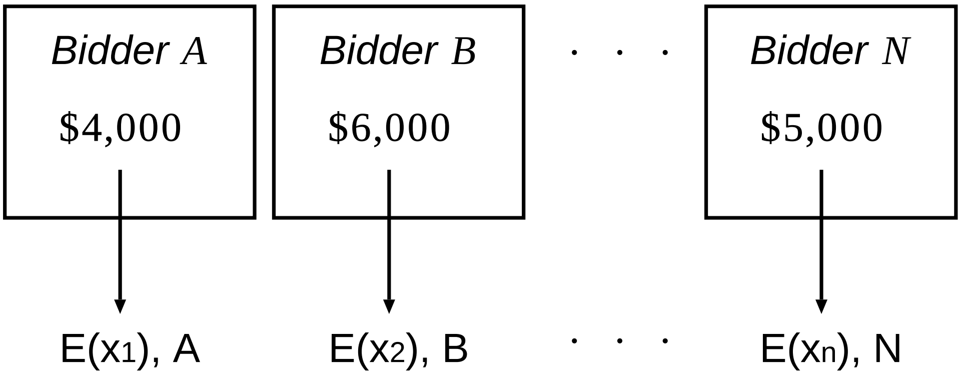

Figure 3.3. An example of NV in the electronic bit

$$y \leftarrow \mathcal{E}_{pk}(x_0) : A_2^{\mathcal{O}_2}(x_0, s, y) = 1]$$

and

$$\begin{aligned}\mathrm{Succ}_{A,\Pi,\$}^{\mathrm{nv-atk}}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s) \leftarrow A_1^{\mathcal{O}_1}(pk); x_0, x_1 \leftarrow M;\\ &y \leftarrow \mathcal{E}_{pk}(x_1) : A_2^{\mathcal{O}_2}(x_0, s, y) = 1].\end{aligned}$$

The oracle to be used is the same as IND-ATK. We say that Π is secure in the sense of NV-CPA, NV-CCA1 and NV-CCA2 if $\mathrm{Adv}_{A,\Pi}^{\text{nv-cpa}}$, $\mathrm{Adv}_{A,\Pi}^{\text{nv-cca1}}$ and $\mathrm{Adv}_{A,\Pi}^{\text{nv-cca2}}$ are negligible for any adversary A, respectively. □

3.3. Relation among NM, IND, EU and NV

The relation among the proposed notions and these of [1] is discussed in this section.

Theorem 6: IND-ATK ⇒ EU-ATK

Proof: We show that $\mathrm{Adv}_{B,\Pi}^{\mathrm{eu-atk}}(\cdot)$ is negligible for any adversary B if Π is secure in the IND-ATK sense. Let $B = (B_1, B_2)$ be an EU-ATK adversary attacking Π. To prove the theorem, we construct an IND-ATK adversary $A = (A_1, A_2)$ attacking Π by using $B = (B_1, B_2)$ so that A succeeds the attack if B does, that is, $\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(\cdot)$ is not negligible if $\mathrm{Adv}_{B,\Pi}^{\mathrm{eu-atk}}(\cdot)$ is not negligible, implying that $\mathrm{Adv}_{B,\Pi}^{\mathrm{eu-atk}}(\cdot)$ is negligible if $\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(\cdot)$ is

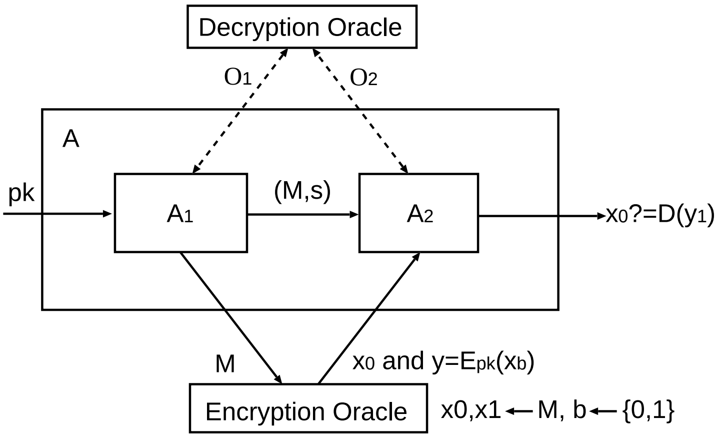

Figure 3.4. The NV adversary model

negligible. Adversaries A and B have access to an oracle $\mathcal{O}_1$ in their first stage and an oracle $\mathcal{O}_2$ in the second stage.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
  $(M, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
  $x_0, x_1 \leftarrow M$
  $y_0 \leftarrow \mathcal{E}_{pk}(x_0)$
  $s' \leftarrow (s, y_0)$
  return $(x_0, x_1, s')$

**Algorithm** of $A_2^{\mathcal{O}_2}(x_0, x_1, s', y)$ where $s' = (s, y_0)$
  $d \leftarrow B_2^{\mathcal{O}_2}(s, y_0, y)$
  return $d$
```

$A_1^{\mathcal{O}_1}$ outputs plaintexts x_0 and x_1, and a modified state information s', including a ciphertext y_0. $A_2^{\mathcal{O}_2}$ outputs $d \in \{0, 1\}$ so that $d = 0$ when the decryptions of y and y_0 are the same and $d = 1$ when the decryptions of y and y_0 are different. Notice that A is a polynomial time algorithm if the running time of B is bounded by a fixed polynomial in k.

We consider the advantage of A, given by

$$\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k) = 2 \cdot \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1}(pk); b \leftarrow \{0, 1\};$$

$$y \leftarrow \mathcal{E}_{pk}(x_b) \colon\ A_2^{\mathcal{O}_2}(x_0, x_1, s, y) = b] - 1.$$

Since $b \in \{0,1\}$ is chosen uniformly, we have

$$\begin{aligned}\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k) &= 2 \cdot (\tfrac{1}{2}p_k(0) + \tfrac{1}{2}p_k(1)) - 1\\ &= p_k(0) + p_k(1) - 1\end{aligned}$$

where

$$\begin{aligned}p_k(i) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s') \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &y \leftarrow \mathcal{E}_{pk}(x_i)\colon\ A_2^{\mathcal{O}_2}(x_0, x_1, s', y) = i]\end{aligned}$$

for $i \in \{0,1\}$.

On the other hand, $\mathrm{Adv}_{B,\Pi}^{\mathrm{eu-atk}}(k)$ is written as

$$\begin{aligned}\mathrm{Adv}_{B,\Pi}^{\mathrm{eu-atk}}(k) &= 2 \cdot (\tfrac{1}{2}p'_k(0) + \tfrac{1}{2}p'_k(1)) - 1\\ &= p'_k(0) + p'_k(1) - 1\end{aligned}$$

where

$$\begin{aligned}p'_k(i) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s) \leftarrow B_1^{\mathcal{O}_1}(pk); x_0, x_1 \leftarrow M;\\ &y_0 \leftarrow \mathcal{E}_{pk}(x_0);\ y \leftarrow \mathcal{E}_{pk}(x_i) :\ B_2^{\mathcal{O}_2}(s, y_0, y) = i]\end{aligned}$$

for $i \in \{0,1\}$. Remark that $(x_0, x_1, s') \leftarrow A_1^{\mathcal{O}_1}(pk)$ if and only if $(M, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$ and $x_0, x_1 \leftarrow M$, and that $A_2^{\mathcal{O}_2}(x_0, x_1, s', y) = i$ if and only if $B_2^{\mathcal{O}_2}(s, y_0, y) = i$. Hence, $p_k(i) = p'_k(i)$ for $i \in \{0,1\}$, and therefore, $\mathrm{Adv}_{B,\Pi}^{\mathrm{eu-atk}}(k) = \mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k)$. If Π is secure in the sense of IND-ATK, then $\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k)$ is negligible, and consequently, $\mathrm{Adv}_{B,\Pi}^{\mathrm{eu-atk}}(k)$ is also negligible and Π is secure in the sense of EU-ATK. □

Theorem 7: EU-ATK ⇒ IND-ATK

Proof: We show that $\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(\cdot)$ is negligible for any adversary B if Π is secure in the EU-ATK sense. Let $B = (B_1, B_2)$ be an IND-ATK adversary attacking Π. We construct an EU-ATK adversary $A = (A_1, A_2)$ attacking Π by using $B = (B_1, B_2)$ so that A succeeds the attack if B does.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
  $(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
```

```
    $M := \{x_0, x_1\}$
    $s' \leftarrow (x_0, x_1, s)$
    return $(M, s')$

**Algorithm** of $A_2^{\mathcal{O}_2}(s', y, y')$ where $s' = (x_0, x_1, s)$
    $d \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, y)$
    return $d$
```

$A_1^{\mathcal{O}_1}$ outputs a subset M of messages and a modified state information s'. The output of $A_2^{\mathcal{O}_2}$ is $d \in \{0,1\}$ where $d = 0$ for $\mathcal{D}_{sk}(y) = x_0$ and $d = 1$ for $\mathcal{D}_{sk}(y) = x_1$. Notice that A is a polynomial time algorithm if the running time of B is bounded by a fixed polynomial in k.

Similar to the proof of Theorem 6, $\mathrm{Adv}_{A,\Pi}^{\mathrm{eu-atk}}(k)$ is written as

$$\begin{aligned}\mathrm{Adv}_{A,\Pi}^{\mathrm{eu-atk}}(k) &= 2 \cdot (\tfrac{1}{2}p_k(0) + \tfrac{1}{2}p_k(1)) - 1 \\ &= p_k(0) + p_k(1) - 1\end{aligned}$$

where

$$\begin{aligned}p_k(i) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s') \leftarrow A_1^{\mathcal{O}_1}(pk); x_0, x_1 \leftarrow M; \\ &y \leftarrow \mathcal{E}_{pk}(x_0);\ y' \leftarrow \mathcal{E}_{pk}(x_i) : A_2^{\mathcal{O}_2}(s', y, y') = i]\end{aligned}$$

for $i \in \{0,1\}$.

On the other hand, $\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(k)$ is written as

$$\begin{aligned}\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(k) &= 2 \cdot (\tfrac{1}{2}p'_k(0) + \tfrac{1}{2}p'_k(1)) - 1 \\ &= p'_k(0) + p'_k(1) - 1\end{aligned}$$

where

$$\begin{aligned}p'_k(i) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk); \\ &y \leftarrow \mathcal{E}_{pk}(x_i) : B_2^{\mathcal{O}_2}(x_0, x_1, s, y) = i]\end{aligned}$$

for $i \in \{0,1\}$. Remark that $(M, s') \leftarrow A_1^{\mathcal{O}_1}(pk)$ and $(x_0, x_1) \leftarrow M$ if and only if $(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$, and that $A_2^{\mathcal{O}_2}(s', y, y') = i$ if and only if $B_2^{\mathcal{O}_2}(x_0, x_1, s, y) = i$. Hence, $p_k(i) = p'_k(i)$ for $i \in \{0,1\}$, and therefore, $\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(k) = \mathrm{Adv}_{A,\Pi}^{\mathrm{eu-atk}}(k)$. If Π is secure in the sense of

EU-ATK, then $\mathrm{Adv}_{A,\Pi}^{\mathrm{eu-atk}}(k)$ is negligible, and consequently, $\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(k)$ is also negligible and Π is secure in the sense of IND-ATK. □

Theorem 8: IND-ATK ⇒ NV-ATK

Proof: We will show that $\mathrm{Adv}_{B,\Pi}^{\mathrm{nv-atk}}(\cdot)$ is negligible for any adversary B if Π is secure in the IND-ATK sense. Let $B = (B_1, B_2)$ be a NV-ATK adversary attacking Π. We construct an IND-ATK adversary $A = (A_1, A_2)$ attacking Π by using $B = (B_1, B_2)$ so that A succeeds the attack if B does.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
  $(M, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
  $(x_0, x_1) \leftarrow M$
  $s' \leftarrow (M, s)$
  return $(x_0, x_1, s')$
```

```
**Algorithm** of $A_2^{\mathcal{O}_2}(x_0, x_1, s', y)$ where $s' = (M, s)$
  $d \leftarrow B_2^{\mathcal{O}_2}(x_0, s, y)$
  if $d = 1$ then $c \leftarrow 0$        ($d = 1$ means that $B_2^{\mathcal{O}_2}$ believes $\mathcal{D}_{sk}(y) = x_0$)
    else $c \leftarrow \{0,1\}$          (coin flip)
  return $c$
```

$A_1^{\mathcal{O}_1}$ outputs plaintexts x_0 and x_1, and a modified state information s'. $A_2^{\mathcal{O}_2}$ outputs $c \in \{0,1\}$ such that $y = \mathcal{E}(x_c)$. Notice that A is a polynomial time algorithm if the running time of B, and the time to sample messages from M are both bounded by a fixed polynomial in k.

According to the definition of the indistinguishability, the advantage of A is

$$\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k) = 2 \cdot \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1}(pk);$$
$$b \leftarrow \{0,1\};\ y \leftarrow \mathcal{E}_{pk}(x_b) \colon A_2^{\mathcal{O}_2}(x_0, x_1, s, y) = b] - 1.$$

Let the probability $p_k(b)$ for $b \in \{0,1\}$ as

$$p_k(b) = \Pr[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s') \leftarrow A_1^{\mathcal{O}_1}(pk);$$
$$y \leftarrow \mathcal{E}_{pk}(x_b) :\ A_2^{\mathcal{O}_2}(x_0, x_1, s', y) = 0].$$

$p_k(0)$ is the probability that A_2 outputs the correct answer 0 under the condition that b

is chosen to be 0 by the encryption oracle, and $p_k(1)$ is the probability that A_2 outputs the incorrect answer under the condition that b is chosen to be 1 by the encryption oracle. Remark that

$$\begin{aligned}&\Pr[(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s') \leftarrow A_1^{\mathcal{O}_1}(pk); b \leftarrow \{0,1\};\\ &\qquad y \leftarrow \mathcal{E}_{pk}(x_b) :\ A_2^{\mathcal{O}_2}(x_0, x_1, s', y) = b]\\ &\quad = \tfrac{1}{2}p_k(0) + \tfrac{1}{2}(1 - p_k(1))\\ &\quad = \tfrac{1}{2}p_k(0) - \tfrac{1}{2}p_k(1) + \tfrac{1}{2},\end{aligned}$$

and hence,

$$\begin{aligned}\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k) &= 2(\tfrac{1}{2}p_k(0) - \tfrac{1}{2}p_k(1) + \tfrac{1}{2}) - 1\\ &= p_k(0) - p_k(1).\end{aligned}$$

Next, we consider the advantage of B, given by

$$\mathrm{Adv}_{B,\Pi}^{\mathrm{nv-atk}}(k) = |\mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k) - \mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k)|$$

where

$$\begin{aligned}\mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s) \leftarrow B_1^{\mathcal{O}_1}(pk);\ x_0 \leftarrow M;\\ &y \leftarrow \mathcal{E}_{pk}(x_0) :\ B_2^{\mathcal{O}_2}(x_0, s, y) = 1]\end{aligned}$$

and

$$\begin{aligned}\mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s) \leftarrow B_1^{\mathcal{O}_1}(pk);\\ &x_0, x_1 \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x_1) :\ B_2^{\mathcal{O}_2}(x_0, s, y) = 1].\end{aligned}$$

Consider the case that $y = \mathcal{E}_{pk}(x_0)$ is given to $A_2^{\mathcal{O}_2}$. In this case the probability $p_k(0)$ that $A_2^{\mathcal{O}_2}$ outputs the correct answer is

$$\begin{aligned}p_k(0) &= \mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k) + (1 - \mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k)) \cdot \tfrac{1}{2}\\ &= \tfrac{1}{2}\mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k) + \tfrac{1}{2}.\end{aligned}$$

Note that $A_2^{\mathcal{O}_2}$ outputs the correct answer 0 if $B_2^{\mathcal{O}_2}$ outputs 1, or if $B_2^{\mathcal{O}_2}$ outputs 0 and c is chosen to be 0. The probability of the former case is $\mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k)$, and the probability of the latter case is $(1 - \mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k)) \cdot \frac{1}{2}$, and hence, $p_k(0)$ is the summation of the above two probabilities. Similarly, consider the case that $y = \mathcal{E}(x_1)$ is given to $A_2^{\mathcal{O}_2}$. In this case, we have

$$\begin{aligned} p_k(1) &= \mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k) + (1 - \mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k)) \cdot \tfrac{1}{2} \\ &= \tfrac{1}{2}\mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k) + \tfrac{1}{2}. \end{aligned}$$

Note that $A_2^{\mathcal{O}_2}$ outputs the incorrect answer 0 if $B_2^{\mathcal{O}_2}$ outputs 1, or if $B_2^{\mathcal{O}_2}$ outputs 0 and c is chosen to be 0. The probability of the former case is $\mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k)$, and the probability of the latter case is $(1 - \mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k)) \cdot \frac{1}{2}$, and hence $p_k(1)$ is the summation of the above two probabilities.

We rewrite the advantage of IND-ATK as

$$\begin{aligned} &\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k) \\ &\quad = p_k(0) - p_k(1) \\ &\quad = (\tfrac{1}{2} + \tfrac{1}{2}\mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k)) \\ &\quad\quad - (\tfrac{1}{2} + \tfrac{1}{2}\mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k)) \\ &\quad = \tfrac{1}{2}(\mathrm{Succ}_{B,\Pi}^{\mathrm{nv-atk}}(k) - \mathrm{Succ}_{B,\Pi,\$}^{\mathrm{nv-atk}}(k)) \\ &\quad = \tfrac{1}{2}\mathrm{Adv}_{B,\Pi}^{\mathrm{nv-atk}}(k). \end{aligned}$$

Therefore, $\mathrm{Adv}_{A,\Pi}^{\mathrm{ind-atk}}(k)$ is negligible if and only if $\mathrm{Adv}_{B,\Pi}^{\mathrm{nv-atk}}(k)$ is negligible. If the scheme Π is secure in the IND-ATK sense, then Π is secure in the NV-ATK sense. □

Theorem 9: NV-ATK ⇒ IND-ATK

Proof: We show that $\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(\cdot)$ is negligible for any adversary B if Π is secure in the NV-ATK sense. Let $B = (B_1, B_2)$ be an IND-ATK adversary attacking Π. We will construct NV-ATK adversary $A = (A_1, A_2)$ attacking Π by using $B = (B_1, B_2)$.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
  $(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
  $M := \{x_0, x_1\}$
  $s' \leftarrow (x_0, x_1, s)$
  return $(M, s')$

**Algorithm** of $A_2^{\mathcal{O}_2}(x_0, s', y)$ where $s' = (x_0, x_1, s)$
  $b \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, y)$
```

```
if $b = 0$ then $d \leftarrow 1$
   else $d \leftarrow 0$
return $d$
```

$A_1^{\mathcal{O}_1}$ outputs a message space M, and a modified state information s', including plaintexts x_0 and x_1. $A_2^{\mathcal{O}_2}$ outputs $d \in \{0,1\}$ so that $d = 1$ if the adversary believes $y = \mathcal{E}(x_0)$ and $d = 0$ otherwise. Notice that A is a polynomial time algorithm if the running time of B is bounded by a fixed polynomial in k.

By the definition of NV, the advantage of A is

$$\mathrm{Adv}_{A,\Pi}^{\mathrm{nv-atk}}(k) = |\mathrm{Succ}_{A,\Pi}^{\mathrm{nv-atk}}(k) - \mathrm{Succ}_{A,\Pi,\$}^{\mathrm{nv-atk}}(k)|$$

where

$$\begin{aligned}\mathrm{Succ}_{A,\Pi}^{\mathrm{nv-atk}}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s') \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x_0 \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x_0) :\ A_2^{\mathcal{O}_2}(x_0, s', y) = 1]\end{aligned}$$

and

$$\begin{aligned}\mathrm{Succ}_{A,\Pi,\$}^{\mathrm{nv-atk}}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (M, s') \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x_0, x_1 \leftarrow M;\ y \leftarrow \mathcal{E}_{pk}(x_1) :\ A_2^{\mathcal{O}_2}(x_0, s', y) = 1].\end{aligned}$$

Now we consider the advantage of B. Define

$$\begin{aligned}p_k(b) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k);\ (x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk);\\ &y \leftarrow \mathcal{E}_{pk}(x_b) :\ B_2^{\mathcal{O}_2}(x_0, x_1, s, y) = 0]\end{aligned}$$

for $b \in \{0,1\}$. Then, similarly to the proof of Theorem 8, we have

$$\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(k) = p_k(0) - p_k(1).$$

On the other hand, $\mathrm{Succ}_{A,\Pi}^{\mathrm{nv-atk}}(k) = p_k(0)$ since $A_2^{\mathcal{O}_2}$ outputs 1 if and only if $B_2^{\mathcal{O}_2}$ outputs 0, and $\mathrm{Succ}_{A,\Pi,\$}^{\mathrm{nv-atk}}(k) = p_k(1)$ similarly. Hence,

$$\mathrm{Adv}_{A,\Pi}^{\mathrm{nv-atk}}(k) = |p_k(0) - p_k(1)|$$

which is negligible if and only if $\mathrm{Adv}_{B,\Pi}^{\mathrm{ind-atk}}(k)$ is. This implies that if the scheme Π is secure in the NV-ATK sense, then it is secure in the IND-ATK sense. □

The four theorems imply that IND, EU and NV are equivalent for any attack of CPA, CCA1 and CCA2. The results together with those of [4] are illustrated in Figure 3.5.

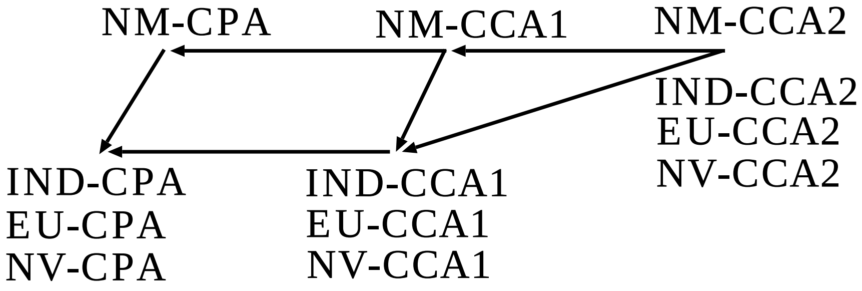

Figure 3.5. The relation among EU, NV, IND and NM

3.4. Discussion

New notions of the security of probabilistic public-key encryption schemes have been proposed. The notions are derived by new goals, equivalence undecidability and non-verifiability. As an extension of the result by Bellare et al., this paper considered the relation among the new notions and those of Bellare et al. The conclusion is that equivalence undecidability, non-verifiability and indistinguishability are all equivalent in the sense of security.

Chapter 4

Detailed Formalizations of Non-Malleability and One-Wayness

4.1. Motivation

Besides the goal of adversaries, there is an essential difference between NM-ATK and OW-ATK. In the case of NM-ATK, an adversary specifies a set M of messages from which an encryption oracle chooses x and constructs the challenge y. Hereafter, the set M is called a *message space* for simplicity. In the case of OW-ATK, on the other hand, the message space is fixed to the set of all messages of length k, and the adversary knows nothing about x except the message length k. Obviously, adversaries in NM-ATK are more advantageous than adversaries in OW-ATK. Actually, a NM-ATK adversary is allowed to choose a very small set M, and perform certain kinds of exhaustive attacks for each message in M. Remark that such exhaustive attacks are not possible for OW-ATK adversaries since the number of messages in the message space is beyond the polynomial-bound of the adversary in OW-ATK framework.

The purpose of this chapter is to discuss non-malleability of cryptosystems against adversaries who are not as powerful as those in NM-ATK setting. For example, consider a situation such that an adversary obtains a ciphertext y by wiretapping. He wants to forge another message y' so that the plaintexts of y and y' are meaningfully related, but he knows nothing about the plaintext underlying y except that the plaintext is just k bits. We would like to present a formal definition of non-malleability of cryptosystems under such a situation. Since we consider less powered adversaries than those in NM-ATK (with respect to the message space), the cryptosystem does not have to be as robust as NM-ATK, that is, the security notion which we should consider in this case is weaker than NM-ATK. However, since the above described situation is very common in the real world, the induced security notion will be practical and significant in an engineering sense.

4.2. Generalized Non-malleability (NMi)

We will devise new formalizations of non-malleability by imposing a lower-bound limit on the message space which is specified by the adversary A_1. First, we need to modify the polynomial-time algorithm A_1 so that it is able to handle message spaces with the exponential number of messages. This is possible by introducing *predicates* on messages. Let $\mathcal{M}$ be the set of all messages available in the public-key cryptosystem. A *predicate* on $\mathcal{M}$ is a boolean function which maps each message in $\mathcal{M}$ to a boolean value, true or false. For a set $\mathcal{M}$ of messages and a predicate p on $\mathcal{M}$, let $\mathcal{M}_p$ be the subset of $\mathcal{M}$ such that messages in $\mathcal{M}_p$ make the predicate p true. Thus $\mathcal{M}_p = \{m : m \in \mathcal{M}, p(m) = \text{true}\}$. A predicate p is a *level-1* predicate if $|\mathcal{M}_p|/|\mathcal{M}|$ is not negligible. We say that p is *level-2* if $|\mathcal{M}_p|$ is not bounded by any polynomial, and *level-3* if there is no restriction on $|\mathcal{M}_p|$. We assume that predicates are represented by a certain well-defined scheme such as logic circuits or expressions. A predicate p is *polynomial-time describable* if the representation of p is in polynomial-order.

Definition 7: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa, cca1, cca2} and $k \in \mathbf{N}$, define

$$\mathrm{Adv}_{A,\Pi}^{\mathrm{nm}i\text{-atk}}(k) = |\mathrm{Succ}_{A,\Pi}^{\mathrm{nm}i\text{-atk}}(k) - \mathrm{Succ}_{A,\Pi,\$}^{\mathrm{nm}i\text{-atk}}(k)|$$

where

$$\begin{aligned}\mathrm{Succ}_{A,\Pi}^{\mathrm{nm}i\text{-atk}}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (p, s) \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x \leftarrow \mathcal{M}_p; y \leftarrow \mathcal{E}_{pk}(x); (R, \mathbf{y}) \leftarrow A_2^{\mathcal{O}_2}(p, s, y);\end{aligned}$$

$$\mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y}) : y \notin \mathbf{y} \wedge \bot \notin \mathbf{x} \wedge R(x, \mathbf{x})],$$

and

$$\begin{aligned}\mathrm{Succ}^{\mathrm{nm}i\text{-atk}}_{A,\Pi,\$}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (p, s) \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x, x' \leftarrow \mathcal{M}_p; y \leftarrow \mathcal{E}_{pk}(x); (R, \mathbf{y}) \leftarrow A_2^{\mathcal{O}_2}(p, s, y);\\ &\mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y}) : y \notin \mathbf{y} \wedge \bot \notin \mathbf{x} \wedge R(x', \mathbf{x})].\end{aligned}$$

The oracle to be used is the same as IND-ATK. It is assumed that the predicate p is polynomial-time describable. For i with $i \in \{1, 2, 3\}$, the encryption scheme Π is said to be secure in the sense of NMi-CPA, NMi-CCA1 and NMi-CCA2 if p is level-i, and if $\mathrm{Adv}^{\mathrm{nm}i\text{-cpa}}_{A,\Pi}(k)$, $\mathrm{Adv}^{\mathrm{nm}i\text{-cca1}}_{A,\Pi}(k)$ and $\mathrm{Adv}^{\mathrm{nm}i\text{-cca2}}_{A,\Pi}(k)$ are negligible for any adversary A, respectively. □

The difference between the above definition and NM-ATK is that the adversary in NM-ATK outputs a message space M directly, while the adversary in the above definition outputs a predicate p.

4.3. Relation among NMi, NM and IND

We consider relations among IND-ATK, NM-ATK and NMi-ATK with $i = \{1, 2, 3\}$. For security notions α and β, we write

- $\alpha \Rightarrow \beta$ to mean that if Π is an encryption scheme which is secure in the sense of α, then Π is also secure in the sense of β.
- $\alpha \not\Rightarrow \beta$ to mean that even if Π is secure in the sense of α, Π is not always secure in the sense of β.

We first show that NM3-ATK is equivalent to NM-ATK.

Lemma 1: NM3-ATK $\Rightarrow$ NM-ATK

Proof: Let Π be a cryptosystem which is secure in the sense of NM3-ATK, and consider a NM-ATK adversary $B = (B_1, B_2)$. We construct a NM3-ATK adversary $A = (A_1, A_2)$ attacking Π using $B = (B_1, B_2)$ so that A succeeds the attack if B does; that is, $\mathrm{Adv}^{\mathrm{nm3\text{-}atk}}_{A,\Pi}(\cdot)$

is not negligible if $\mathrm{Adv}^{\text{nm-atk}}_{B,\Pi}(\cdot)$ is not negligible. Adversaries A and B have access to an oracle $\mathcal{O}_1$ in their first stage and an oracle $\mathcal{O}_2$ in the second stage. The construction of A_1 and A_2 is as follows.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
  $(M, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
  $s' \leftarrow (M, s)$
  $p := (p(x) = \text{true if and only if } x \in M)$
  return $(p, s')$

**Algorithm** of $A_2^{\mathcal{O}_2}(p, s', y)$ where $s' = (M, s)$
  $(R, \mathbf{y}) \leftarrow B_2^{\mathcal{O}_2}(M, s, y)$
  return $(R, \mathbf{y})$
```

Since M contains polynomial-number of messages, the predicate p defined by $A_1^{\mathcal{O}_1}(pk)$ is level-3. We need to show that if $\mathrm{Adv}^{\text{nm-atk}}_{B,\Pi}(k)$ is not negligible, then $\mathrm{Adv}^{\text{nm3-atk}}_{A,\Pi}(k)$ is not negligible also.

Consider the advantage of A, given by

$$\mathrm{Adv}^{\text{nm3-atk}}_{A,\Pi}(k) = |\mathrm{Succ}^{\text{nm3-atk}}_{A,\Pi}(k) - \mathrm{Succ}^{\text{nm3-atk}}_{A,\Pi,\$}(k)|$$

where

$$\begin{aligned}\mathrm{Succ}^{\text{nm3-atk}}_{A,\Pi}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (p, s') \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x \leftarrow \mathcal{M}_p; y \leftarrow \mathcal{E}_{pk}(x); (R, \mathbf{y}) \leftarrow A_2^{\mathcal{O}_2}(p, s', y);\\ &\mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y}) : y \notin \mathbf{y} \wedge \bot \notin \mathbf{x} \wedge R(x, \mathbf{x})],\end{aligned}$$

and

$$\begin{aligned}\mathrm{Succ}^{\text{nm3-atk}}_{A,\Pi,\$}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (p, s') \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x, x' \leftarrow \mathcal{M}_p; y \leftarrow \mathcal{E}_{pk}(x); (R, \mathbf{y}) \leftarrow A_2^{\mathcal{O}_2}(p, s', y);\\ &\mathbf{x} \leftarrow \mathcal{D}_{sk}(\mathbf{y}) : y \notin \mathbf{y} \wedge \bot \notin \mathbf{x} \wedge R(x', \mathbf{x})].\end{aligned}$$

Now, we consider the advantage of B. The advantage of B is identical to the advantage of A except the message space M; however, the message space of A is equivalent to the message space of B, $\mathcal{M}_p = M$. Thus the chosen plaintext of x_0 and x_1 should be in M.

Therefore, $\mathrm{Succ}_{B,\Pi}^{\text{nm-atk}}(k) = \mathrm{Succ}_{A,\Pi}^{\text{nm3-atk}}(k)$, and $\mathrm{Succ}_{B,\Pi,\$}^{\text{nm-atk}}(k) = \mathrm{Succ}_{A,\Pi,\$}^{\text{nm3-atk}}(k)$. Then,

$$\begin{aligned}
\mathrm{Adv}_{B,\Pi}^{\text{nm-atk}}(k) &= |\mathrm{Succ}_{B,\Pi}^{\text{nm-atk}}(k) - \mathrm{Succ}_{B,\Pi,\$}^{\text{nm-atk}}(k)| \\
&= |\mathrm{Succ}_{A,\Pi}^{\text{nm3-atk}}(k) - \mathrm{Succ}_{A,\Pi,\$}^{\text{nm3-atk}}(k)| \\
&= \mathrm{Adv}_{A,\Pi}^{\text{nm-atk}}(k)
\end{aligned}$$

However, since Π is NM3-ATK secure, $\mathrm{Adv}_{A,\Pi}^{\text{nm3-atk}}(k)$ is negligible, and hence $\mathrm{Adv}_{B,\Pi}^{\text{nm-atk}}(k)$ is also negligible. □

Lemma 2: NM-ATK ⇒ NM3-ATK

Proof: Similar to the previous lemma, we construct a NM-ATK adversary $A = (A_1, A_2)$ attacking Π using a NM3-ATK adversary $B = (B_1, B_2)$ so that A succeeds the attack if B does.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
    $(p, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
    $M := \mathcal{M}_p$
    $s' \leftarrow (p, s)$
    return $(M, s')$

**Algorithm** of $A_2^{\mathcal{O}_2}(M, s', y)$ where $s' = (p, s)$
    $(R, \mathbf{y}) \leftarrow B_2^{\mathcal{O}_2}(p, s, y)$
    return $(R, \mathbf{y})$
```

Since the predicate p defined by $B_1^{\mathcal{O}_1}(pk)$ is level-3, $\mathcal{M}_p$ contains polynomial number of messages, and we can assign M of $A_1^{\mathcal{O}_1}(pk)$ as $\mathcal{M}_p$. Therefore, M is identical to $\mathcal{M}_p$. The following discussion on the advantages (probabilities) only needs an opposit argument of Lemma 1. We assumed that if $\mathrm{Adv}_{B,\Pi}^{\text{nm3-atk}}(\cdot)$ is not negligible, then $\mathrm{Adv}_{A,\Pi}^{\text{nm-atk}}(\cdot)$ is not negligible also. But since Π is NM-ATK secure, $\mathrm{Adv}_{A,\Pi}^{\text{nm-atk}}(\cdot)$ is negligible, and hence $\mathrm{Adv}_{B,\Pi}^{\text{nm3-atk}}(\cdot)$ is also negligible. □

The following relation holds obviously from the definition.

Lemma 3: NM3-ATK ⇒ NM2-ATK ⇒ NM1-ATK □

Next we consider the following useful lemma.

Lemma 4: NM2-CCA2 $\not\Rightarrow$ NM3-CPA

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of NM2-CCA2. We will construct another cryptosystem $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ artificially so that Π' is NM2-CCA2 but not NM3-CPA. The construction is as follows.

```
Algorithm of $\mathcal{K}'(1^k)$
    return $(\mathcal{K}(1^k))$

Algorithm of $\mathcal{E}'_{pk}(x)$
    if $x = 0$ or $x = 1$ then return $(0||x)$
      else return $(1||\mathcal{E}_{pk}(x))$

Algorithm of $\mathcal{D}'_{sk}(c||y)$
    if $c = 0$ and $y = 0$ or 1 then return $y$
      else if $c = 0$ and $y \neq 0$ or 1 then return $\perp$
        else return $(\mathcal{D}_{sk}(y))$
```

A ciphertext in the new scheme is $c||y$. A bit c works as a flag, 0 to indicate special plaintext $x = 0$ or 1, and 1 for otherwise. In the case of $c = 0$, the last part of the ciphertext is the plaintext itself. If it is not the case, the last part of the ciphertext is the encryption of the plaintext with the original encryption algorithm $\mathcal{E}_{pk}$. The behavior of Π' is almost equivalent to Π except for two plaintexts 0 and 1. Therefore, if Π is NM2-CCA2 secure then Π' is also NM2-CCA2 secure. Formally, this is proved by showing the following.

To show that Π' is not NM3-CPA, consider an adversary which selects a predicate p so that $p(x)$ =true if and only if x is either 0 or 1. We can do this by the definition of level-3 predicate which is to say the same for NM-CPA. Since the encryption oracle needs to pick a plaintext from $\mathcal{M}_p = \{0, 1\}$, the challenge ciphertext for the adversary is either $\mathcal{E}'_{pk}(0)$ or $\mathcal{E}'_{pk}(1)$. The both ciphertexts are easily breakable by only looking at the last part of the ciphertexts, the plaintext itself, and this can be done with probability one in obviously polynomial-time.

To prove Π' is secure in the NM2-CCA2 sense, we construct a NM2-CCA2 adversary $A = (A_1, A_2)$ attacking Π, using a NM2-CCA2 adversary $B = (B_1, B_2)$ attacking Π'.

```
**Algorithm** of $A_1^{\mathcal{D}_{sk}}(pk)$
    $(p, s) \leftarrow B_1^{\mathcal{D}_{sk}}(pk)$
    return $(p, s)$

**Algorithm** of $A_2^{\mathcal{D}_{sk}}$
    $(R, \mathbf{y}) \leftarrow B_2^{\mathcal{D}_{sk}}(p, s, 1||y)$
    return $(R, \mathbf{y})$
```

$\mathrm{Adv}_{A,\Pi}^{\text{nm2-cca2}}(k)$ is evaluated in terms of $\mathrm{Adv}_{B,\Pi'}^{\text{nm2-cca2}}(k)$ is that

$$\mathrm{Adv}_{A,\Pi}^{\text{nm2-cca2}}(k) = \mathrm{Adv}_{B,\Pi'}^{\text{nm2-cca2}}(k) + \frac{2}{|\mathcal{M}_p|}.$$

Since the predicate is level-2, $\mathcal{M}_p$ is an exponential number of messages by definition. So the second term of $2/|\mathcal{M}_p|$ is negligible. Thus $\mathrm{Adv}_{A,\Pi}^{\text{nm2-cca2}}(k)$ is equivalent to $\mathrm{Adv}_{B,\Pi'}^{\text{nm2-cca2}}(k)$. But since Π is NM2-CCA2 secure, $\mathrm{Adv}_{A,\Pi}^{\text{nm2-cca2}}(\cdot)$ is negligible, and hence $\mathrm{Adv}_{B,\Pi'}^{\text{nm2-cca2}}(\cdot)$ is also negligible. □

As corollaries of Lemma 4, we can show that NM2-ATK $\not\Rightarrow$ NM3-ATK' for any combinations of ATK, ATK' $\in$ {CPA,CCA1,CCA2}. For example, we have NM2-CCA2 $\not\Rightarrow$ NM3-CCA2; otherwise, if NM2-CCA2 $\Rightarrow$ NM3-CCA2 then NM2-CCA2 $\Rightarrow$ NM3-CCA2 $\Rightarrow$ NM3-CPA, and it contradicts to Lemma 4. The following lemma can be shown similarly to Lemma 4.

Lemma 5: NM1-CCA2 $\not\Rightarrow$ NM2-CPA

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of NM1-CCA2. We will construct another cryptosystem $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ artificially so that Π' is NM1-CCA2 but not NM2-CPA. The construction is as follows.

```
Algorithm of $\mathcal{K}'(1^k)$
    return $(\mathcal{K}(1^k))$

Algorithm of $\mathcal{E}'_{pk}(x)$
    if $x \in \mathcal{M}_p$ then return $(0||x)$
        else return $(1||\mathcal{E}_{pk}(x))$

Algorithm of $\mathcal{D}'_{sk}(c||y)$
    if $c = 0$ and $y \in \mathcal{M}_p$ then return $y$
        else if $c = 0$ and $y \notin \mathcal{M}_p$ then return $\perp$
            else return $(\mathcal{D}_{sk}(y))$
```

The behavior of Π' is almost equivalent to Π except for some plaintexts in $\mathcal{M}_p$ (level-2). Therefore, if Π is NM1-CCA2 secure then Π' is also NM1-CCA2 secure and NM3-CCA2 secure. (Formally, this is proved by showing that any NM1-CCA2 adversary for Π' works as a NM1-CCA2 adversary for Π as similarly in the proof of Lemmas 1 and 2.) To show that Π' is not NM1-CPA, consider an adversary which selects a predicate p so that $p(x)$ =true if and only if x is either 0 or 1. Since the encryption oracle needs to pick a plaintext from $\mathcal{M}_p = \{0, 1\}$, the challenge ciphertext for the adversary is either $\mathcal{E}'_{pk}(0)$ or $\mathcal{E}'_{pk}(1)$, either of which is easily breakable. □

We also have the following corollaries which follows from Lemmas 16 and 17 presented in the next section.

Corollary 1: NM3-CPA $\not\Rightarrow$ NM1-CCA1 □

Corollary 2: NM3-CCA1 $\not\Rightarrow$ NM1-CCA2 □

The above lemmas and corollaries clarify relations between an arbitrary pair of NMi-ATK notions. As for the relations between IND-ATK and NMi-ATK, the following two lemmas explain all the relations.

Lemma 6: NM2-CCA2 $\not\Rightarrow$ IND-CPA

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of NM2-CCA2. We will construct another cryptosystem $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ artificially so that Π' is NM2-CCA2 but not IND-CPA. For new Π', use Π' considered in Lemma 4.

```
Algorithm of $\mathcal{K}'(1^k)$
    return $(\mathcal{K}(1^k))$

Algorithm of $\mathcal{E}'_{pk}(x)$
    if $x = 0$ or $x = 1$ then return $(0||x)$
        else return $(1||\mathcal{E}_{pk}(x))$

Algorithm of $\mathcal{D}'_{sk}(c||y)$
    if $c = 0$ and $y = 0$ or 1 then return $y$
        else if $c = 0$ and $y \neq 0$ nor 1 then return $\perp$
            else return $(\mathcal{D}_{sk}(y))$
```

In the same way as in Lemma 4, the behavior of Π' is almost equivalent to Π except for two plaintexts 0 and 1. Therefore, if Π is NM2-CCA2 secure then Π' is also NM2-CCA2 secure. To show that Π' is not IND-CPA, consider an adversary which selects a predicate p so that $p(x)$ =true if and only if x is either 0 or 1. Since the encryption oracle needs to pick a plaintext from $\mathcal{M}_p = \{0, 1\}$, the challenge ciphertext for the adversary is either $\mathcal{E}'_{pk}(0)$ or $\mathcal{E}'_{pk}(1)$, and the IND-CPA adversary only need to take a last part of the encryption which is a plaintext itself, if the encryption is in the right form $(0||x)$. □

Lemma 7: IND-CCA1 $\not\Rightarrow$ NM1-CPA

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of IND-CCA1. The cryptosystem $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ constructed in the proof of Theorem 3 in [4], shown below,

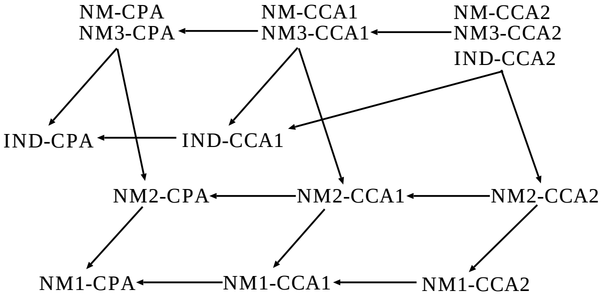

Figure 4.1. IND-ATK and NMi-ATK

is IND-CCA1 but not NM1-CPA.

```
**Algorithm** of $\mathcal{K}'(1^k)$
    return $(\mathcal{K}(1^k))$

**Algorithm** of $\mathcal{E}'_{pk}(x)$
    $y_1 \leftarrow \mathcal{E}_{pk}(x)$
    $y_2 \leftarrow \mathcal{E}_{pk}(\bar{x})$
    return $(y_1||y_2)$

**Algorithm** of $\mathcal{D}'_{sk}(y_1||y_2)$
    return $(\mathcal{D}_{sk}(y_1))$
```

In the construction of Π', $\mathcal{E}'_{pk}(x)$ returns $\mathcal{E}_{pk}(x)||\mathcal{E}_{pk}(\bar{x})$ where $\bar{x}$ denotes a bitwise complement of x. The constructed Π' is IND-CCA1, if underlying Π is IND-CCA1, but Π' is not NM1-CPA for only swapping $(y_1||y_2)$ to $(y_2||y_1)$. □

The relations shown in this section is summarized in Figure 4.1. Individual separation results are not shown in the figure, but if there is no directed path from α to β, then $\alpha \not\Rightarrow \beta$ holds.

4.4. Generalized One-wayness (OWi)

In Section 2.2.4, we reviewed the result by Goldreich and considered OW-ATK as a formal definition of one-wayness. In this section, as analogy to the discussion in the previous section, we consider other formalizations of OW-ATK.

Definition 8: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and $A = (A_1, A_2)$ be an adversary. For atk $\in$ {cpa, cca1, cca2} and $k \in \mathbf{N}$, define

$$\mathrm{Adv}^{\mathrm{ow}i\text{-}\mathrm{atk}}_{A,\Pi}(k) = |\mathrm{Succ}^{\mathrm{ow}i\text{-}\mathrm{atk}}_{A,\Pi}(k) - \mathrm{Succ}^{\mathrm{ow}i\text{-}\mathrm{atk}}_{A,\Pi,\$}(k)|$$

where

$$\begin{aligned}\mathrm{Succ}^{\mathrm{ow}i\text{-}\mathrm{atk}}_{A,\Pi}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (p, s) \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x \leftarrow \mathcal{M}_p; y \leftarrow \mathcal{E}_{pk}(x); z \leftarrow A_2^{\mathcal{O}_2}(p, s, y) : x = z],\end{aligned}$$

and

$$\begin{aligned}\mathrm{Succ}^{\mathrm{ow}i\text{-}\mathrm{atk}}_{A,\Pi,\$}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (p, s) \leftarrow A_1^{\mathcal{O}_1}(pk);\\ &x, x' \leftarrow \mathcal{M}_p; y \leftarrow \mathcal{E}_{pk}(x); z \leftarrow A_2^{\mathcal{O}_2}(p, s, y) : x' = z].\end{aligned}$$

The oracle to be used is the same as IND-ATK. It is assumed that the predicate p is polynomial-time describable. For i where $i \in \{1, 2, 3\}$, the encryption scheme Π is said to be secure in the sense of OWi-CPA, OWi-CCA1 and OWi-CCA2 if p is level-i, and if $\mathrm{Adv}^{\mathrm{ow}i\text{-}\mathrm{cpa}}_{A,\Pi}(k)$, $\mathrm{Adv}^{\mathrm{ow}i\text{-}\mathrm{cca1}}_{A,\Pi}(k)$ and $\mathrm{Adv}^{\mathrm{ow}i\text{-}\mathrm{cca2}}_{A,\Pi}(k)$ are negligible for any adversary A, respectively. □

4.5. Relation among OWi, OW and IND

We first show that OW3-ATK is equivalent to IND-ATK.

Lemma 8: IND-ATK ⇒ OW3-ATK

Proof: We asumme that encryption scheme Π is secure in the IND-ATK sense. In the similar way of Lemma 1, we construct an IND-ATK adversary $A = (A_1, A_2)$ by using a OW3-ATK adversary $B = (B_1, B_2)$. The construction is as follows.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
    $(p, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
    $\{x_0, x_1\} \leftarrow \mathcal{M}_p$
    $s' \leftarrow (p, s)$
    return $(x_0, x_1, s')$
```

```
**Algorithm** of $A_2^{\mathcal{O}_2}(x_0, x_1, s', y)$ where $s' = (p, s)$
    $z \leftarrow B_2^{\mathcal{O}_2}(p, s, y)$
    if $z = x_0$ then $c \leftarrow 0$
        else if $z = x_1$ then $c \leftarrow 1$
            else $c \leftarrow \{0, 1\}$
    return $c$
```

The predicate p defined by $B_1^{\mathcal{O}_1}(pk)$ is level-3. We need to show that $\mathrm{Adv}_{B,\Pi}^{ow3-atk}(\cdot)$ is negligible. The following proof is similar to the proof of Theorem 2 in [4] or Theorem 3.3 in [5]. □

Lemma 9: OW3-ATK ⇒ IND-ATK

Proof: Construct a OW3-ATK adversary $A = (A_1, A_2)$ by using an IND-ATK adversary $B = (B_1, B_2)$.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
    $(x_0, x_1, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
    $\mathcal{M}_p := \{x_0, x_1\}$
    $s' \leftarrow (x_0, x_1, s)$
    return $(p, s')$
```

```
**Algorithm** of $A_2^{\mathcal{O}_2}(p, s', y)$ where $s' = (x_0, x_1, s)$
    $b \leftarrow B_2^{\mathcal{O}_2}(x_0, x_1, s, y)$
    if $b = 0$ then $z = x_0$
        else $z = x_1$
    return $z$
```

We assign $\mathcal{M}_p$ as a set of two plaintexts (x_0, x_1), then the predicate p is obiously level-3. We need to show that $\mathrm{Adv}_{B,\Pi}^{ind-atk}(\cdot)$ is negligible. The following proof is similar to the proof of Theorem 1 in [4] or Theorem 3.1 in [5]. □

Similar to the discussion concerning NMi-ATK, we have the following lemmas.

Lemma 10: OW3-ATK $\Rightarrow$ OW2-ATK $\Rightarrow$ OW1-ATK □

Lemma 11: OW2-CCA2 $\not\Rightarrow$ OW3-CPA

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of OW2-CCA2. We will construct another cryptosystem $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ artificially so that Π' is OW2-CCA2 but not OW3-CPA. The construction is the same as in Lemma 4.

```
**Algorithm** of $\mathcal{K}'(1^k)$
  return $(\mathcal{K}(1^k))$

**Algorithm** of $\mathcal{E}'_{pk}(x)$
  if $x = 0$ or $x = 1$ then return $(0||x)$
    else return $(1||\mathcal{E}_{pk}(x))$

**Algorithm** of $\mathcal{D}'_{sk}(c||y)$
  if $c = 0$ and $y = 0$ or 1 then return $y$
    else if $c = 0$ and $y \neq 0$ or 1 then return $\perp$
      else return $(\mathcal{D}_{sk}(y))$
```

The behavior of Π' is almost equivalent to Π except for two plaintexts 0 and 1. Therefore, if Π is OW2-CCA2 secure then Π' is also OW2-CCA2 secure. To show that Π' is not OW3-CPA, consider an adversary which selects a predicate p so that $p(x)$ =true if and only if x is either 0 or 1. Since the encryption oracle needs to pick a plaintext from $\mathcal{M}_p = \{0, 1\}$, the challenge ciphertext for the adversary is either $\mathcal{E}'_{pk}(0)$ or $\mathcal{E}'_{pk}(1)$, and for a OW3-CPA adversary, it is easy to take the last part of $(0||x)$ to get the plaintext. □

Lemma 12: OW1-CCA2 $\not\Rightarrow$ OW2-CPA

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of NM1-CCA2. The construction of $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is the same as Lemma 5. The scheme Π' is OW1-CCA2 but not OW2-CPA.

```
**Algorithm** of $\mathcal{K}'(1^k)$
  return $(\mathcal{K}(1^k))$

**Algorithm** of $\mathcal{E}'_{pk}(x)$
  if $x \in \mathcal{M}_p$ then return $(0||x)$
    else return $(1||\mathcal{E}_{pk}(x))$

**Algorithm** of $\mathcal{D}'_{sk}(c||y)$
  if $c = 0$ and $y \in \mathcal{M}_p$ then return $y$
    else if $c = 0$ and $y \notin \mathcal{M}_p$ then return $\perp$
      else return $(\mathcal{D}_{sk}(y))$
```

The behavior of Π' is almost equivalent to Π except for some plaintexts in $\mathcal{M}_p$ (level-2). Therefore, if Π is NM1-CCA2 secure then Π' is also NM1-CCA2 secure. To show that Π' is not NM2-CPA, consider an adversary which selects a predicate p so that $p(x)$ =true if and only if x is either 0 or 1. Since the encryption oracle picks a plaintext from $\mathcal{M}_p$ with the level-2 predicate, the challenge ciphertext for the adversary is $\mathcal{E}'_{pk}(x)$ with $x \in \mathcal{M}_p$. □

The following corollaries are from Lemmas 16 and 17 presented in the next section.

Corollary 3: OW3-CPA $\not\Rightarrow$ OW1-CCA1 □

Corollary 4: OW3-CCA1 $\not\Rightarrow$ OW1-CCA2 □

The following lemmas show that OW-ATK considered in Section 2.2.4 is equivalent to OW1-ATK.

Lemma 13: OW1-ATK $\Rightarrow$ OW-ATK

Proof: We construct a OW1-ATK adversary $A = (A_1, A_2)$ using a OW-ATK adversary $B = (B_1, B_2)$. Now A_1 needs to specify a predicate, which we use a tautology (a predicate which is true for any message) in this construction.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
  $s \leftarrow B_1^{\mathcal{O}_1}(pk)$
```

```
    $p := (p(x) =$true for all $x)$
    return $(p, s)$

**Algorithm** of $A_2^{\mathcal{O}_2}(p, s, y)$
    $z \leftarrow B_2^{\mathcal{O}_2}(s, y)$
    return $z$
```

The OW-ATK adversary B_2 is expected to return a correct answer, and A_2 will success the attack. Since M contains exponential-number of messages, the predicate p defined by $A_1^{\mathcal{O}_1}$ is level-1. The rest of the proof is straightforward The adversary A_2 will succeeds the attack if B_2 does, and the probability of the challenge chosen from $\mathcal{M}_p$ is one. Therefore, $\mathrm{Adv}_{B,\Pi}^{\text{ow-atk}}(\cdot)$ is equivalent to $\mathrm{Adv}_{A,\Pi}^{\text{ow1-atk}}(\cdot)$. □

Lemma 14: OW-ATK ⇒ OW1-ATK

Proof: We construct a OW-ATK adversary $A = (A_1, A_2)$ using a OW1-ATK adversary $B = (B_1, B_2)$. The OW1-ATK adversary B_2 will succeeds the attack only if the message underlying the challenge is chosen from $\mathcal{M}_p$ where p is the predicate determined by B_1. However, the challenge to the OW-ATK adversary A_2 might be chosen from the outside of $\mathcal{M}_p$.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
    $(p, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
    $s' \leftarrow (p, s)$
    return $(s')$

**Algorithm** of $A_2^{\mathcal{O}_2}(s', y)$ where $s' = (s, p)$
    $z \leftarrow B_2^{\mathcal{O}_2}(p, s, y)$
    return $z$
```

The adversary A_2 will succeeds the attack if x with $y = \mathcal{E}_{pk}(x)$ is (fortunately) chosen from $\mathcal{M}_p$ by an encryption oracle. On the other hand, if $x \notin \mathcal{M}_p$, then A_2 has few chances to success. To show that this construction suffices, we need to evaluate $\mathrm{Adv}_{A,\Pi}^{\text{ow-atk}}(\cdot)$ precisely. First, observe that $|\mathcal{M}_p|$ is very large (beyond polynomial) in OW1-ATK, and the output of $A_2^{\mathcal{O}_2}(p, s, y)$ coincides with the randomly chosen x' with negligible probability. This means that $\mathrm{Succ}_{B,\Pi,\$}^{\text{ow1-atk}}(\cdot)$ is always negligible. Therefore, if $\mathrm{Adv}_{B,\Pi}^{\text{ow1-atk}}(\cdot)$ is not negligible, then it

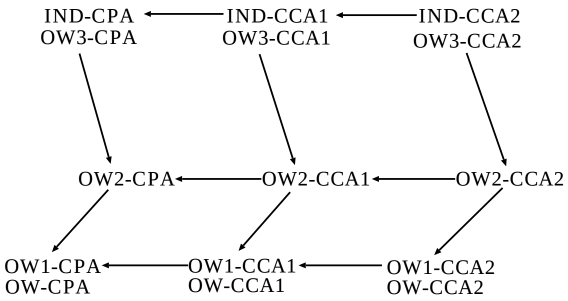

Figure 4.2. IND-ATK and OWi-ATK

means that $\mathrm{Succ}^{\text{ow1-atk}}_{B,\Pi}(\cdot)$ is not negligible.

Now observe that

$$\mathrm{Adv}^{\text{ow-atk}}_{A,\Pi}(\cdot) = \Pr[x \in \mathcal{M}_p] \cdot \mathrm{Succ}^{\text{ow1-atk}}_{B,\Pi}(\cdot) + \Pr[x \notin \mathcal{M}_p] \cdot \mathrm{Succ}^{\text{ow1-atk}}_{B,\Pi,*}(\cdot) \tag{4.1}$$

where

$$\begin{aligned}\mathrm{Succ}^{\mathrm{ow1}-atk}_{B,\Pi,*}(k) = \Pr[&(pk, sk) \leftarrow \mathcal{K}(1^k); (p, s) \leftarrow B_1^{\mathcal{O}_1}(pk);\\ &x \leftarrow \overline{\mathcal{M}_p}; y \leftarrow \mathcal{E}_{pk}(x); z \leftarrow A_2^{\mathcal{O}_2}(p, s, y) : x = z]\end{aligned}$$

where $\overline{\mathcal{M}_p}$ denotes the complement set of $\mathcal{M}_p$. Remark that $\Pr[x \in \mathcal{M}_p] = |\mathcal{M}_p|/|\mathcal{M}|$ is not negligible since p is a level-1 predicate. Thus the first term in (1) is a product of two non-negligible values and hence non-negligible if $\mathrm{Adv}^{\text{ow1-atk}}_{B,\Pi}(\cdot)$ is not negligible. Therefore, we could show that if $\mathrm{Adv}^{\text{ow1-atk}}_{B,\Pi}(\cdot)$ is not negligible, then $\mathrm{Adv}^{\text{ow-atk}}_{A,\Pi}(\cdot)$ is not negligible also. This completes the proof. □

Figure 4.2 shows the relations discussed in this section .

4.6. Relation among OWi and NMi

This section is to discuss the relation between NMi-ATK and OWi-ATK. It is rather easy to show the following lemma.

Lemma 15: NMi-ATK $\Rightarrow$ OWi-ATK for $i \in \{1, 2, 3\}$

Proof: Let $B = (B_1, B_2)$ be a OWi-ATK adversary attacking Π. We construct an NMi-ATK adversary $A = (A_1, A_2)$ attacking Π using $B = (B_1, B_2)$ so that A succeeds the attack if B does.

```
**Algorithm** of $A_1^{\mathcal{O}_1}(pk)$
  $(p, s) \leftarrow B_1^{\mathcal{O}_1}(pk)$
  return $(p, s)$
```

```
**Algorithm** of $A_2^{\mathcal{O}_2}(p, s, y)$
  $z \leftarrow B_2^{\mathcal{O}_2}(p, s, y)$
  $y' \leftarrow \mathcal{E}_{pk}(\bar{z})$
  return $(R, y')$
```

Note that R is bitwise complement, and assuming that there exists a level-i predicate p. Formally, we need to show that $\mathrm{Adv}_{A,\Pi}^{\mathrm{nm}i\text{-atk}}(\cdot)$ is not negligible if $\mathrm{Adv}_{B,\Pi}^{\mathrm{ow}i\text{-atk}}(\cdot)$ is not negligible. The proof is straightforward, and is omitted. $\square$

The following lemmas suggest that the difference in the oracles of adversaries is essential. The proofs are omitted, but remarked that we can make use of proof techniques similar to those in NM-CPA $\not\Rightarrow$ IND-CCA1 (Theorem 4 in [4]) and NM-CCA1 $\not\Rightarrow$ NM-CCA2 (Theorem 5 in [4]).

Lemma 16: NM3-CPA $\not\Rightarrow$ OW1-CCA1

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of NM1-CCA2. The construction of $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is the same as Theorem 4 in [4]. The scheme Π' is NM3-CPA but not OW1-CCA1 as follows.

```
**Algorithm** of $\mathcal{K}'(1^k)$
  $(pk, sk) \leftarrow (\mathcal{K}(1^k))$
  $u, v \leftarrow \{0, 1\}^k$
  $pk' \leftarrow pk||u$
  $sk' \leftarrow sk||u||v$
  return $(pk', sk')$

Algorithm of $\mathcal{E}'_{pk||u}(x)$
  $y \leftarrow \mathcal{E}_{pk}(x)$
  return $(0||y)$

Algorithm of $\mathcal{D}'_{sk||u||v}(b||y)$
  if $b = 0$ then return $\mathcal{D}_{sk}(y)$
    else if $y = u$ then return $v$
      else if $y = v$ return $sk$
        else return $\perp$
```

As a proof of Theorem 4 in [4] (details of probabilistic analysis is in [5]), Π is NM3-CPA secure and Π' is also NM3-CPA secure. To show that Π' is not OW-CCA1, the adversary asks $\mathcal{D}'_{sk||u||v}(\cdot)$ with $(1||u)$ to get v at first, then asks $(1||v)$ to get sk. Therefore, the adversary can compute $\mathcal{D}_{sk}(y)$ to recover the message with probability one in polynomial-time. □

Lemma 17: NM3-CCA1 $\not\Rightarrow$ OW1-CCA2

Proof: Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem secure in the sense of NM3-CCA1. The construction of $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ is the same as Theorem 5 in [4]. $F = \{F^k :\geq 1\}$ is a fixed family of pseudorandom functions. Here each $F^k = \{F_K : K \in \{0,1\}^k\}$ is a finite collection where a particular function $F_k : \{0,1\}^k \rightarrow \{0,1\}^k$ with each key $K \in \{0,1\}^k$. ε is the empty string, and the scheme Π' is NM3-CCA1 but not OW1-CCA2 as follows.

```
Algorithm of $\mathcal{K}'(1^k)$
  $(pk, sk) \leftarrow (\mathcal{K}(1^k))$
  $K \leftarrow \{0,1\}^k$
  $sk' \leftarrow sk||K$
  return $(pk, sk')$

Algorithm of $\mathcal{E}'_{pk||u}(x)$
  $y \leftarrow \mathcal{E}_{pk}(x)$
```

```
return $(0||y||\varepsilon)$

Algorithm of $\mathcal{D}'_{sk||K}(b||y||z)$
  if $b = 0 \wedge (z = \varepsilon)$ then return $\mathcal{D}_{sk}(y)$
    else if $(b = 1) \wedge (z = \varepsilon)$ then return $F_K(y)$
      else if $(b = 1) \wedge (z = F_K(y))$ return $D_{sk}(y)$
        else return $\perp$
```

As a proof of Theorem 5 in [4] (details of probabilistic analysis is in [5]). To show that Π' is not OW1-CCA2, the adversary cannot asks a challenge $(0||y||\varepsilon)$, but may asks $(1||y||\varepsilon)$ to get $F_k(y)$, and then asks $(1||y||F_k(y))$ to get the decryption of y. However, when NM3-CCA1 tries to obtain $F_k(y)$ to get $D_{sk}(y)$, the ability of the adversary is CCA1. Thus the decryption oracle is available without the challenge y in the second stage. And possibility of the adversary successfully computing F_k after getting y is very small for the pseudorandomness of F, thus computation is hard for the CCA1 adversary. $\mathcal{D}'_{sk||u||v}(\cdot)$ with $(1||u)$ to get v at first, then asks $(1||v)$ to get sk. Therefore, the adversary can compute $\mathcal{D}_{sk}(y)$ to recover the message with probability one in polynomial-time. □

Lemmas considered in the previous sections imply some relations between OWi-ATK and NMi-ATK.

Corollary 5: OW3-CCA1$\not\Rightarrow$ NM1-CPA

Proof: OW3-CCA1 and IND-CCA1 are equivalent by Lemmas 8 and 9, while IND-CCA1$\not\Rightarrow$ NM1-CPA by Lemma 7. □

It follows from the above corollary that OWi-ATK $\not\Rightarrow$ NMj-ATK' for any $i, j \in \{1, 2, 3\}$ and ATK, ATK' $\in \{\text{CPA}, \text{CCA1}\}$.

For the case of CCA2, we need another lemma.

Lemma 18: OW2-CCA2$\not\Rightarrow$ NM1-CPA

Proof: From a OW2-CCA2 secure cryptosystem $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, we construct a new cryptosystem $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is OW2-CCA2 but not NM1-CPA. The construction is shown below.

```
**Algorithm** of $\mathcal{K}'(1^k)$
  return $(pk, sk)$

**Algorithm** of $\mathcal{E}'_{pk}(x)$
  $y \leftarrow \mathcal{E}_{pk}(x)$
  return $(0||y)$

**Algorithm** of $\mathcal{D}'_{sk}(c||y)$
  if $c = 0$ then return $\mathcal{D}_{sk}(y)$
    else return $y$
```

The cryptosystem Π' is OW2-CCA2 if Π is OW2-CCA2, since a OW2-CCA2 adversary $A = (A_1, A_2)$ for Π is constructible from a OW2-CCA2 adversary $B = (B_1, B_2)$ for Π'. The construction of the adversary A is that $A_1 = B_1$ and A_2 asks B_2 to attack $0||y$ where y is the challenge presented to A_2. The algorithm A_2 needs to provide a decryption oracle of Π' (say $O_{\Pi'}$) to B_2. To simulate $O_{\Pi'}$, A_2 makes use of the decryption oracle of Π (say O_{Π}) which is available to A_2. Due to the restriction of oracles in CCA2, A_2 cannot ask O_{Π} to decrypt the challenge y itself, and in this case A_2 will fail to make correct simulation of $O_{\Pi'}$. However, this will never happen because B_2 cannot ask $O_{\Pi'}$ to decrypt $0||y$ which is the challenge for B_2. The algorithm B_2 may ask $O_{\Pi'}$ to decrypt $1||y$, but in this case A_2 does not have to consult O_{Π} because $O_{\Pi'}$ simply returns y.

To see that Π' is not NM1-CPA, let $y = 0||E_{pk}(x)$ be a challenge ciphertext and consider an adversary which outputs another ciphertext $y' = 1||E_{pk}(x)$ and a relation R such that $R(x, x')$ is true if and only if $x' = E_{pk}(x)$. The ciphertext y' will be decrypted to $E_{pk}(x)$ by D'_{sk}, and therefore, $R(D'_{sk}(y), D'_{sk}(y')) = R(x, E_{pk}(x))$ will be true with non-negligible probability. □

Thanks to the above lemma, we have OWi-ATK $\not\Rightarrow$ NMj-ATK' for any $i, j \in \{1, 2\}$ and ATK, ATK' $\in$ $\{\mathrm{CPA}, \mathrm{CCA1}, \mathrm{CCA2}\}$. Now all the relations among the OWi-ATK and NMi-ATK formalizations are clarified.

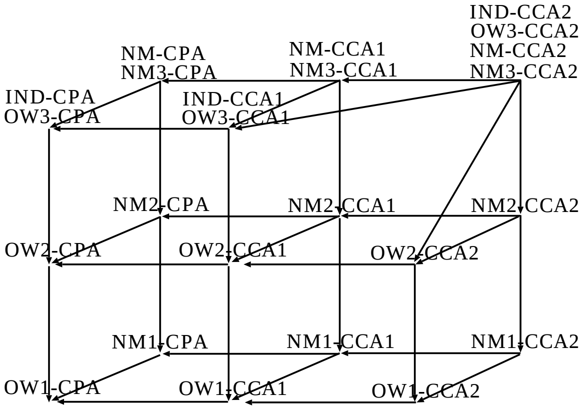

Figure 4.3. Relations among all security notions

4.7. Discussion

The relations shown in the previous sections are summarized in Figure 4.3. Separation results are not presented in the figure, but if there is not a directed path from α to β then it means that the security in the sense of α does not always imply the security in the sense of β.

Figure 4.3 shows many interesting relations among security notions. For example, it shows that OW3-ATK is equivalent to IND-ATK. This result contradicts the widely-accepted belief that one-wayness is a properly weaker security notion than indistinguishability. This fact suggests that when we consider one-wayness, we implicitly assume that the message space is beyond polynomial. That is, OW3-ATK formalizes rather irregular situation which we do not consider usually. We are not sure if the same consequence follows in the case of non-malleability, but we remark that as far as only level-3 predicates are considered, non-malleability, indistinguishability and one-wayness are all equivalent for a CCA2 adversary.

Another interesting relation is that IND-ATK does not always imply NM2-ATK. It is obvious from the definition that no deterministic cryptosystem (cryptosystem of which encryption function is deterministic) can be IND-ATK, and hence any deterministic cryptosystem cannot be NM3-ATK secure. On the other hand, our result suggests that the determinism of cryptosystems and NM2-ATK can be compatible. That is, there may exist deterministic cryptosystems which are secure in the sense of NM2-ATK. This result encourages the use of deterministic cryptosystems in some contexts. For example, consider that we want a non-malleable cryptosystem to be used in a protocol of which adversaries may wiretap the communication, but they need to consider exponentially many number of possible plaintexts (as we considered in the introduction). The required security notion in such a situation is NM2-ATK, and we may devise deterministic cryptosystems which are usually more efficient (with respect to the length of ciphertexts) than probabilistic cryptosystems.

Chapter 5

Conclusion and Future Work

Formalizations of security notions of public-key cryptosystems were discussed in this thesis. The results can be regarded as an extension of Bellare's study, and our model reflects many important practical aspects of cryptosystems.

In the first part of this thesis, formal definitions of equivalence undecidability and non-verifiability were considered. Both properties are fundamental and important for public-key cryptosystems, but formalizations for the properties have not been considered yet. We presented formal definitions of the properties according to the style of Bellare's work, and induced the formalizations of EU-ATK and NV-ATK. We also showed that both of EU-ATK and NV-ATK are equivalent to IND-ATK. This is an interesting result since equivalence undecidability and non-verifiability were considered independently from indistinguishability.

In the second part of the thesis, we considered detailed formalizations of non-malleability and one-wayness. According to the size of the message space chosen by an adversary, we considered NM1-ATK, NM2-ATK and NM3-ATK for non-malleability, and OW1-ATK, OW2-ATK and OW3-ATK for one-wayness. We also showed that NM3-ATK is equivalent to NM-ATK by Bellare et al., and that OW1-ATK is equivalent to OW-ATK by Goldreich. This suggests that our detailed formalizations are natural extensions of the previous research. The relations among the new and old formalizations were almost clarified. We could confirm theoretically that the difference of the size of message space affects the advantage of adversaries essentially. We also note that the induced formalizations well correspond to the adversaries in the real world. In the real world, it commonly happens that an adversary does not know what the plaintext underlying the challenge is, and there are an exponential number of possible plaintexts. To discuss the security under such situations, security notions with levels one and two are much appropriate.

It seems that we still have a lot of works to do in this research field. For example, there are many security properties which are not yet discussed in this theoretical framework. It will be interesting if a number of security properties are discussed in a uniform framework. Another theoretical and technical problem is the treatment of the “meaningful relation R” in NM(i)-ATK formalizations. Obviously “meaningfully related” is a too intuitive definition, and it is difficult to consider such a definition in a formal discussion. As for the future work from the practical viewpoint, we need to evaluate existing cryptosystems and classify them in the formal framework. For example, we can show that RSA is neither IND-CPA, NM1-CPA, nor OW3-CPA. It seems that RSA is OW2-CCA1 but not OW2-CCA2, though, its proof is not provided yet. Classifying many practical cryptosystems in the proposed framework is both theoretically and practically an important subject in this research topic.

References

[1] M. Abe and T. Okamoto, *Provably Secure Partially Blind Signatures*, Advances in Cryptology–CRYPTO'00 Proceedings, Lecture Notes in Computer Science Vol. 1880, pp. 271–286, 2000.

[2] O. Baudron, D. Pointcheval and J. Stern, *Extended Notions of Security for Multicast Public-key Cryptosystems*, Automata, Languages and Programming–ICALP'00 Proceedings, Lecture Notes in Computer Science Vol. 1853, pp. 499–511, 2000.

[3] M. Bellare, A. Desai, E. Jokipii and P. Rogaway, *A Concrete Security Treatment of Symmetric Encryption*, Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, pp. 394–403, 1997.

[4] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, *Relations among Notions of Security for Public-Key Encryption Schemes*, Advances in Cryptology–CRYPTO'98 Proceedings, Lecture Notes in Computer Science Vol. 1462, pp. 26–45, 1998.

[5] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, *Relations Among Notions of Security for Public-Key Encryption Schemes*, Manuscript, 1998, **http://www-cse.ucsd.edu/ucsd.edu/users/mihir/**.

[6] M. Bellare and P. Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, The first ACM Conference on Computer and Communications Security, ACM, pp. 62–73, 1993.

[7] M. Bellare and P. Rogaway, *Optimal Asymmetric Encryption*, Advances in Cryptology–EUROCRYPT'94 Proceedings, Lecture Notes in Computer Science Vol. 950, pp. 92–111, 1995.

[8] M. Bellare and A. Sahai, *Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization*, Advances in Cryptology–CRYPTO'99 Proceedings, Lecture Notes in Computer Science Vol. 1666, pp. 519–536, 1999.

[9] M. Bellare and A. Sahai, *Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization*, Manuscript, 1999, **http://www-cse.ucsd.edu/ucsd.edu/users/mihir/**.

[10] D. Bleichenbacher, *Chosen Ciphertext Attack against Protocols Based on the RSA Encryption Standard PKCS #1*, Advances in Cryptology–CRYPTO'98 Proceedings, Lecture Notes in Computer Science Vol. 1462, pp. 1–12, 1998.

[11] V. Boyko, *On the Security Properties of OAEP as an All-or Nothing Transform*, Advances in Cryptology–CRYPTO'99 Proceedings, Lecture Notes in Computer Science Vol. 1666, pp. 503–518, 1999.

[12] A. Desai, *The Security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search*, Advances in Cryptology–CRYPTO'00 Proceedings, Lecture Notes in Computer Science Vol. 1880, pp. 359–375, 2000.

[13] A. Desai, *New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen Ciphertext Attack*, Advances in Cryptology–CRYPTO'00 Proceedings, Lecture Notes in Computer Science Vol. 1880, pp. 394–412, 2000.

[14] R. Cramer and V. Shoup, *A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack*, Advances in Cryptology–CRYPTO'98 Proceedings, Lecture Notes in Computer Science Vol. 1462, pp. 13–25, 1998.

[15] D. Dolev, C. Dwork and M. Naor, *Non-Malleable Cryptography*, Proceedings of the 23rd Annual Symposium on Theory of Computing, ACM, pp. 543–522, 1991.

[16] D. Dolev, C. Dwork, and M. Naor, *Non-Malleable Cryptography*, Technical Report CS 95-27, Weizmann Institute of Science 1995.

[17] D. Dolev, C. Dwork, and M. Naor, *Non-Malleable Cryptography*, Manuscript, 1998.

[18] D. Dolev, C. Dwork, and M. Naor, *Non-Malleable Cryptography*, Manuscript, 2000, **http://www.wisdom.weizmann.ac.il/ naor/PAPERS/nmc.ps.gz**.

[19] Federal Information Processing Standards 74, *FIPS PUB 74 DES*, NIST, USA, Nov.1981, **http://www.ilt.nist.gov/fipspubs/fip74.htm**.

[20] E. Fujisaki and T. Okamoto, *Secure Integration of Asymmetric and Symmetric Encryption Schemes*, Advances in Cryptology–CRYPTO'99 Proceedings, Lecture Notes in Computer Science Vol. 1666, pp. 537–554, 1999.

[21] E. Fujisaki and T. Okamoto, *How to Enhance the Security of Public-Key Encryption at Minimum Cost*, Public Key Cryptography–PKC'99 Proceedings, Lecture Notes in Computer Science Vol. 1560, pp. 53–68, 1999.

[22] E. Fujisaki and T. Okamoto, *How to Enhance the Security of Public-Key Encryption at Minimum Cost*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Institute of Electronics, Information and Communication Engineers E83-A(1), pp. 24–32, Jan. 2000.

[23] S. Goldwasser and S. Micali, *Probabilistic Encryption*, Journal of Computer and System Sciences, 28, pp. 270–299, 1984.

[24] O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, Springer-Verlag, 1999.

[25] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC press, pp. 306–311, 1997.

[26] M. Naor and M. Yung, *Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks*, Proceedings of the 22nd Annual Symposium on Theory of Computing, pp. 427–437, ACM, 1990.

[27] T. Okamoto and S. Uchiyama, *A New Public-Key Cryptosystem as Secure as Factoring*, Advances in Cryptology–EUROCRYPT '98 Proceedings, Lecture Notes in Computer Science Vol. 1403, pp. 308–318, 1998.

[28] T. Okamoto, S. Uchiyama and E. Fujisaki, *EPOC: Efficient Probabilistic Public-Key Encryption*, Proceedings of the 1999 Symposium on Cryptography and Information Security, pp. 75–86, 1999.

[29] C. Rackoff and D. Simon, *Non-interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*, Advances in Cryptology–CRYPTO '91 Proceedings, Lecture Notes in Computer Science Vol. 576, pp. 433–444, 1998.

[30] RSA Data Security, Inc., *PKCS#1: RSA Encryption Standard, Version 1.5*, Redwood City, CA, Nov.1998, **http://www.rsa.com/rsalabs/**.

[31] H. Sakai, N. Nakamura and Y. Igarashi, *A Refined Definition of Semantic Security for Public-key Encryption Schemes*, IEICE Transactions on Information and Systems, Institute of Electronics, Information and Communication Engineers E84-D(1), pp. 34–39, Jan. 2001.

[32] SSL*Ref*, a reference implementation from Netscape Communications of the SSL protocol, **http://home.netscape.com/newsref/std/sslref.html**.