

## Summary of the paper Relations Among Notions of Security for Public-Key Encryption Schemes

M. Bellare - A. Desaiy - D. Pointchevalz - P. Rogawayx

In this paper they compare the relative strengths of popular notions of security for public-key encryption schemes. The goal of this paper is to consider the *indistinguishability* (IND) and *non-malleability* (NM), each under *chosen-plaintext attack* (CPA) and two kinds of *chosen-ciphertext attack* (CCA1, CCA2). For each of the resulting pairs of definitions they prove either an implication or a separation. Also they did the same to the *plaintext awareness* (PA), a notion of security in the random *oracle model* (RO). Also, in this paper the authors produced a new definition of non-malleability which is simpler than the previous one.

This paper is divided into four sections Introduction, Definition of security, Relating IND and NM and finally the Result on Plaintext Awareness.

In the introduction they introduced the notation of encryption scheme security. Also, they gave an explanation of some security aspect. Finally, they talked about the motivation and some related work.

In the second section they talked about the definition of security and the framework. Also in this section they talked about indistinguishability of encryptions and non-malleability

The third section was about relation IND and NM to the three different Attacks which mentioned above. In this section they give proves for each of the resulting pairs either an implication or a separation

List of the proves that they provided in this paper:

- |            |     |          |
|------------|-----|----------|
| ➤ NM-ATK   | ==> | IND-ATK  |
| ➤ IND-CCA2 | ==> | NM-CCA2  |
| ➤ IND-CCA1 | ≠>  | NM-CPA   |
| ➤ NM-CPA   | ≠>  | IND-CCA1 |
| ➤ NM-CCA1  | ==> | NM-CCA2  |

The last section is focusing on **Plaintext Awareness**. It explains its definition and then it shows the result by proves. In this section they proved that:

- |           |     |          |
|-----------|-----|----------|
| ➤ PA      | ==> | IND-CCA2 |
| ➤ IND-CCA | ≠>  | PA       |