

Article Summary

November 19, 2009

Abstract

This paper aims to bridge two means to evaluate cryptographic scheme, the first is the formal approach using expressions and the second uses complexity and probability of real advantage of the attacker

1 Formal Encryption and Expression Equivalence

The representation is usual: the plaintext message is M , the cipher is $\{M\}_K$, K the key, i a bit, and the box \square an undecryptable data.

We define some rules to develop the pattern of an expression to be able to compare it with another and decide if two are equivalent or not.

One big idea is that we assume that the atomic function we use are safe in the large view. In this way, this is really easier to modelize the properties of the protocol. That's why we can assume that every box representation are equivalent in size and in distinguishability in the key and in the plaintext.

2 The Computational View: Encryption Schemes and Indistinguishability

The different parts of a symmetric encryption scheme are described first, then a definition of the security of such schemes is established.

The encryption scheme is defined as a triple of algorithms $\{K, E, D\}$ where K returns a key, E returns a ciphertext and D returns a plaintext.

The concepts of negligible functions and advantages are defined, too. It will be useful in the concept of distinguishability for a given adversary.

The different types of security for an encryption scheme are described in this section: types 0, 1 and 3. For each type of security, a definition based on a difference of probabilities to guess the key or to learn information from a ciphertext is given. Some properties of encryption schemes having given types of security are detailed in this section.

3 The Computational Soundness of Formal Equivalence

This section gives us a formal view (theorems, properties and their proofs) of encryption schemes when we consider both views of cryptography.

In a given encryption scheme, an association between an ensemble and an expression is proposed. After that, we show that a relation of equivalence between expressions implies indistinguishability in ensembles. This theory (that unifies both views of cryptography) is based on transformations related to patterns presented in the first sections and presents some algorithms and properties related to the description of an encryption scheme Π in the formal theory and in the computational theory.

In the end, a link is made with the security levels defined in section 3.