Summary: Many cryptographic systems which involve hash functions have proof of their security in a so-called random oracle model. Behavior of hash functions used in such cryptographic systems should be as close as possible to the behavior of a random function. There are several properties of hash functions dealing with a random behavior. A hash function is pseudo-random oracle if it is indifferentiable from a random oracle. However, it is well known that hash functions based on the popular Merkle-Damgård domain extension transform do not satisfy the pseudo-random oracle property. On the other hand no attack is known for many concrete applications utilizing Merkle-Damgård hash functions. Hence, a weakened notion called public-use pseudo random oracle was introduced. The property can be met by the Merkle-Damgård construction and is sufficient for several important applications. A hash function is public use pseudo-random oracle if it is indifferentiable from a random oracle with public messages (i.e., all messages hashed so far are available to all parties). This is the case of most hash based signature schemes. In this paper we analyze relationship between the property pseudo-random oracle and its variant public image pseudo-random oracle. Roughly, a hash function is public image pseudo-random oracle if it is indifferentiable from a random oracle with public images (i.e., all images of messages hashed so far are available to all parties, messages are kept secret). We prove that the properties are equivalent.

MSC:

94A60 Cryptography

Keywords:

random oracle; cryptographic hash function; pseudo-random oracle

Full Text: Link