Abstract

Keccak Hash Function is the winner of SHA3 competition. Hash function collision has become one of the fundamental problem in Keccak Hash Function. One of the attack which is based on collision has been proposed by Plasencia, et.al. They proposed the practical analysis of reduced round Keccak Hash Function, such that the collision will be found in the second round of Keccak-224. For preventing Keccak Hash Function against Plasencia attack, denying collision in the second round is necessary. Denying the collision of Keccak Hash Function has become one challenge. Since the attacker used free bit for finding the collision, then for preventing against the attack the free bit camouflaging should be conducted. Therefore, for denying the collision in the second round of Keccak Hash Function, free bit camouflaging is proposed.

Free bits are used to find the original message that is caused by the collision. For denying the collision, the proposed method modifies the input message by using reverse interleaving scheme. This scheme introduces inverse double mirror image sequence of a message to prevent the attacker in obtaining the original free bits. Based on the experiment, it has been proven that using reverse interleaving, the attacker obtained the camouflaged free bit instead of the original one. The camouflaged free bit will increase the difficulty for finding the collision such that the collision could not be found in the second round. This condition will prevent the attacker for finding the original message. The larger the difference would increase the complexity of attack on Keccak Hash Function in obtaining the original message.

Keywords: Keccak, Hash Function, Reverse Interleaving, free bit, collision, attack, camouflaging free bit