

Hardware Architecture for Time/Memory Trade-off Cryptanalysis

Dr. Sourav Mukhopadhyay, Switching & Systems Laboratory, RINCE, DCU

Abstract

The basic goal of a cryptanalytic attack is to recover the secret key from publicly available information. Very often a successful attack exploits weakness in the design of the specific algorithm being considered. For example, linear and differential attacks try to find the linear and differential characteristic between the plaintext and the ciphertext for a given encryption algorithms. A generic approach for cryptanalysis views the encryption function as a black box, i.e., it does not utilize information about how the function is constructed. A simplest generic attack is to try every possible key until the correct one is found. This is called an exhaustive search attack. The importance of such an approach arises from the fact that if a cryptographic algorithm is not secure against exhaustive search, then it cannot be considered secure at all. The main disadvantage of using exhaustive search is that it has to be repeated separately for each target. To address this problem, Hellman introduced time/memory trade-off (TMTO) attack that enables one to perform an exhaustive search once in an offline precomputation phase. The actual attack, i.e., finding the key corresponding to a target is done in an online phase with table lookup and is significantly faster than exhaustive search. Also, one can repeat the attack on different targets without going through the pre-computation each time. A TMTO attack is a generic attack which can be carried out against any one-way function. The online target consists of an image y and the goal of the attack is to find a x , such that $f(x)=y$, x being the secret key (pre-image) from a key space of size N corresponding to the target y .