Using MRHS to Attack Block Ciphers

Kenneth Matheis
Florida Atlantic University

Abstract. In 2007-2008, Raddum and Semaev proposed a new algorithm called Multiple Right Hand Sides, or MRHS, to attack block ciphers, and it can be directly applied to AES, PRESENT, and DES. Though it is guaranteed to terminate producing the key given just one plaintext/ciphertext pair, the computation resources required are nontrivial. The available resources will determine the time complexity of the algorithm, but we do not yet have meaningful statements about the complexity. Still, MRHS is considered to be another tool in the cryptographer’s toolkit, and in some cases it is preferable to a Groebner basis approach.

An overview of MRHS will be presented, and variants on this approach will be discussed, along with their benefits and drawbacks. In addition, software and hardware implementations will be explored.

Keywords. MRHS, algebraic attack.