

This work surveys and studies the most practical attacks on round reduced versions of the cipher PRINCE. Specifically, concepts of integral cryptanalysis and meet-in-the-middle attacks are discussed. A new 4.5-round integral distinguisher with lower time and data complexity is presented. A new meet-in-the-middle attack on seven rounds of the cipher with low data complexity is proposed. A Python 3 reference implementation of the cipher as well as of some of the integral attacks is provided.