Improving Key Recovery Attacks on Block Ciphers using Sbox Decision Trees

No Author Given

No Institute Given

Abstract

In the cryptanalysis of block ciphers, the key recovery attack is one of the most common templates, which applies to many well-known families, such as differential, linear, integral, or meet-in-the-middle attacks. Broadly speaking, in a key recovery attack a part of the key is guessed so that a distinguisher can be applied to a reduced version of the cipher. In general, we want to minimise the size of this guess in order to save both time and memory.

In this work, we introduce a general technique which applies to block cipher constructions which employ Sboxes, such as SPNs. By describing the desired output(s) of an Sbox as a decision tree which branches according to linear combinations of the inputs, we can provide efficient guessing strategies for the key.

We provide two metrics for the efficiency of these trees, numberLeaves and domsize. We briefly discuss an algorithm which finds trees which finds a tree which provides the minimum value of numberLeaves, minLeaves and the minimum value of domsize, domopt.

We then illustrate how this technique can be applied to two of the most widely-used cryptanalysis families: differential cryptanalysis and linear cryptanalysis. In the case of differential cryptanalysis, we discuss how to minimise the key guess required to guarantee the desired difference between two plaintexts at the output of an Sbox. In the case of linear cryptanalysis, we discuss which of our tree-based techniques can be used in each type of linear key recovery algorithm.

This technique has been applied in attacks on reduced-round NOEKEON (linear attack), RECTANGLE (differential attack), GIFT (boomerang/rectangle attack), Serpent (differential-linear attack) and PRESENT (meet-in-the-middle attack).

Main References

1. Broll, M., Canale, F., David, N., Flórez-Gutiérrez, A., Leander, G., Naya-Plasencia, M., Todo, Y.: Further improving differential-linear attacks: Applications to chaskey and serpent. IACR Cryptol. ePrint Arch. p. 820 (2021), https://eprint.iacr.org/2021/820
2. Broll, M., Canale, F., Flórez-Gutiérrez, A., Leander, G., Naya-Plasencia, M.: Generic framework for key-guessing improvements. In: Advances in Cryptology – ASIACRYPT 2021 (2021)