We investigate functions which can be realized using only addition, XOR and rotation (ARX). Sometimes we admit operations with constants as well (ARX+C).
We start our research from a theoretical point of view. We prove that every function can by written using only ARX+C operations and that we can even omit XOR. On the other hand, other combinations of these operations do not generate all functions. We also present an algorithm determining whether a function can be realised only by addition and XOR.
After that we present a rotational cryptanalysis, which is designed especially for ARX ciphers. We demonstrate this method on reduced variants of Threefish, TEA and XTEA ciphers and discuss for which ciphers it is suitable. The last part of this thesis deals with a modification of rotational cryptanalysis called rotational rebound attack and shows its application on Threefish.