Tato práce za zabývá funkcemi, které lze vyjádřit pomocí sčítání, XORu a rotace (ARX). Případně ještě povolíme přičtení či XOR konstanty (ARX+C).
Nejprve zkoumáme tyto funkce z teoretického pohledu. Ukážeme, že pomocí operací ARX+C umíme zapsat každou funkci. Můžeme si dokonce dovolit vypustit operaci XOR. Naopak pomocí jiných kombinací zkoumaných operací všechny funkce nezískáme. Nabízíme též jednoduchý algoritmus určující, jestli lze funkci zapsat pomocí sčítání a XORu.
Následně prezentujeme metodu rotační kryptoanalýzy určenou právě pro ARX funkce. Ukážeme její podobu na zjednodušených variantách šifer Threefish, TEA a XTEA a diskutujeme, pro které šifry je metoda vhodná. Zabýváme se též úpravou metody v podobě rotačního rozpínavého útoku, jehož užití opět demonstrujeme na Threefish.