Práce shrnuje autorův výzkum v oboru hašovacích funkcí v průběhu jeho doktorského studia. První část práce představuje zobecněnou teorii rovnic sestavených ze dvou základních stavebních kamenů kryptografických primitiv: modulárního sčítaní a exkluzivní disjunkce. Druhá a třetí část byly napsány po Wangové zveřejnění kolizí v MD5 a~ukazují, že drobné modifikace této hašovací funkce nefungují. Tyto dvě částí popisují kolize pro 3C a 3C+ konstrukce hashovacích funkcí, které navrhl Gauravaram, a pro tzv. “feedback ring-iterative structure” konstrukci navrženou Su a kol. Výsledky byly publikovány na konferencích ICISC 2006 a SPI 2007. Poslední část představuje nový typ kolizí pro MD5 s nově navrženými rozdíly v kolidujících zprávách. Výsledek byl publikován ve sborníku konference Indocrypt 2008.