Cílem této bakalářské práce je popsat obecný MQ problém, především jeho variantu zvanou HFE, nastínit některé útoky na základní schéma založené na HFE a následně popsat nový útok na HFEz, systém vzniklý modifikací HFE, kdy se část výstupů z úvodní transformace opomene. Modifikace HFEz zajistí závislost vstupu do HFE polynomu na větším množství proměnných při zachování velikosti rozšíření tělesa. Útok na tuto modifikaci spočívá v překladu HFEz na HFE s větvením a následné aplikaci algoritmu pro separaci jednotlivých větví navrženého v [Fel06]. Separační algoritmus přes veřejný klíč vytvoří operaci, která společně se sčítáním tvoří komutativní, neasociativní algebru. Následně se aplikací několika poznatků o neasociativních algebrách za pomoci této operace spočte matice, která umožní separovat proměnné do několika sad odpovídajících jednotlivým větvím. Díky tomuto převodu můžeme následně provést útok přímo na HFE polynom neovlivněného modifikací HFEz.