The aim of this thesis is to describe a general MQ Problem with a focus on its variant called HFE, outline several attacks on a basic scheme based on HFE and describe a new attack on HFEz, a cryptosystem based on special polynomials over finite fields with a modification, which discards a portion of the output from the initial transformation. This ensures a dependency on more variables while keeping the same size of the field. The attack starts with a translation of HFE into HFE with branches, followed by a branch separating algorithm described in [Fel06]. The separation algorithm uses the public key to derive an operation, which induces (with addition) a non-associative algebra. Utilising some properties of non-associative algebras, a matrix, which can separate variables into distinct sets according to branches, is calculated. This leads to stripping off the HFEz modification and thus allowing us to attack directly the HFE polynomial.