

Abstract. This paper investigates the number of trace-one elements in a polynomial basis for \mathbb{F}_{2^n} . A polynomial basis with a small number of trace-one elements is desirable because it results in an efficient and low-cost implementation of the trace function. We focus on the case where the reduction polynomial is a trinomial or a pentanomial, in which case field multiplication can also be efficiently implemented.