Abstract

Finite fields have been used for many applications in electronic communications. In the case of extension fields, the nature of computation depends heavily on the choice of basis used to represent the extension over the base field. The most common choices of basis are polynomial bases although optimal normal bases or some variant of these have also been used despite the fact that such bases exist in only a limited set of cases. Building on these, we develop an alternative class of bases that exist for any extension field. We provide hardware models based on the notion of shift registers for computing with respect to such bases, and investigate some of the properties of these models.