Review of Il-Whan Park, Seok-Won Jung, Hee-Jean Kim, Jong-In Lim, “Fast operation method in $\mathrm{GF}(2^n)$ using a modified optimal normal basis,” Commun. Korean Math. Soc. **12** (1997), 531–538

D. J. Bernstein

1999.08.06

The field $\mathrm{GF}(q^n)$ may be written as $\mathrm{GF}(q)[x]/(x^n + x^{n-1} + \cdots + 1)$ if q has order n modulo $n+1$. The $\mathrm{GF}(q)$-basis $\{x, x^2, \ldots, x^n\}$ of this field allows very simple calculations, for two reasons: first, the qth power of any basis element is a basis element; second, the product of two basis elements is a linear combination of only $2 - 1/n$ basis elements on average.

R. C. Mullin et al. [Discrete Appl. Math. 22 (1988/89), no. 2, 149–161; MR 90c:11092] made the observations above (for q prime); exhibited a second class of field extensions having normal bases with the $2-1/n$ property; showed that $2-1/n$ is optimal; and suggested using optimal normal bases in computations. Shuhong Gao and Hendrik W. Lenstra, Jr. [Des. Codes Cryptogr. 2 (1992), no. 4, 315–323; MR 93j:12003] subsequently gave a complete classification of optimal normal bases.

There are no new ideas in the paper under review. For certain values of q and n, the paper constructs an optimal normal $\mathrm{GF}(q)$-basis of $\mathrm{GF}(q^n)$, and suggests using this basis to perform computations in $\mathrm{GF}(q^n)$.