CORR 2000-27

On complexity of Squaring Using Polynomial Basis in $GF(2^m)$

Huapeng Wu

Abstract In this paper, the complexity of a squaring operation using polynomial basis (PB) in a class of finite fields $GF(2^m)$ is evaluated. The main results are as follows:

1. When the field is generated with an irreducible trinomial $f(x) = x^m + x^k + 1,\ 1 \leq k \leq \frac{m}{2}$, where both m and k are odd, a PB squaring operation requires $\frac{m-1}{2}$ bit operations.

2. When the field is generated with an irreducible trinomial $f(x) = x^m + x^k + 1,\ 1 \leq k \leq \frac{m}{2}$, where $m + k$ is odd and $k \neq \frac{m}{2}$, a PB squaring operation requires $\frac{m+k-1}{2}$ bit operations.

3. When the field is generated with an irreducible trinomial $f(x) = x^m + x^{\frac{m}{2}} + 1$, a PB squaring operation requires $\frac{m+2}{4}$ bit operations.