CORR 2000-28

Montgomery Multiplier and Squarer in $GF(2^m)$

Huapeng Wu

Abstract Montgomery multiplication in $GF(2^M)$ is defined by $a(x)b(x)r^{-1}(x) \bmod f(x)$, where the field is generated by irreducible polynomial $f(x)$, $a(x)$ and $b(x)$ are two field elements in $GF(2^m)$, and $r(x)$ is a fixed field element in $GF(2^m)$. In this paper, first we present a generalized Montgomery multiplication algorithm in $GF(2^m)$. Then by choosing $r(X)$ according to $f(x)$, we show that efficient architecture for bit-parallel Montgomery multiplier and squarer can be obtained for the fields generated with irreducible trinomials. Complexities in terms of gate counts and time propagation delay of the circuits are investigated and found to be comparable to or better than that of polynomial basis or weakly dual basis multiplier for the same class of fields.