

Abstract In 1999, Jerome Solinas introduced families of moduli called the generalized Mersenne numbers [8]. The generalized Mersenne numbers are expressed in a polynomial form, $p = f(t)$, where t is a power of 2. It is shown that such p 's lead to fast modular reduction methods which use only a few integer additions and subtractions. We further generalize this idea by allowing any integer for t . We show that more generalized Mersenne numbers still lead to a significant improvement over well-known modular multiplication techniques. While each generalized Mersenne number requires a dedicated implementation, more generalized Mersenne numbers allow flexible implementations that work for more than one modulus. We also show that it is possible to perform long integer modular arithmetic without using multiple precision operations when t is chosen properly. Moreover, based on our results, we propose efficient arithmetic methods for XTR cryptosystem.