BIBLIOGRAPHY


[82] Adan Abdul, Azaz Gutub, "New hardware algorithms and designs for Montgomery Modular inverse Computation in Galois Fields GF(p) and GF(2^1)", CHES'02, USA, June 11, 2002.
