Twisted Polynomials and Forgery Attacks on GCM