Cryptology ePrint Archive: Report 2011/202

Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes

Markku-Juhani O. Saarinen

Abstract: The Galois/Counter Mode (GCM) of operation has been standardized by NIST to provide single-pass authenticated encryption. The GHASH authentication component of GCM belongs to a class of Wegman-Carter polynomial hashes that operate in the field $\mathrm{GF}(2^{128})$. We present message forgery attacks that are made possible by its extremely smooth-order multiplicative group which splits into 512 subgroups. GCM uses the same block cipher key K to both encrypt data and to derive the generator H of the authentication polynomial for GHASH. In present literature, only the trivial weak key $H=0$ has been considered. We show that GHASH has much wider classes of weak keys in its 512 multiplicative subgroups, analyze some of their properties, and give experimental results on AES-GCM weak key search. Our attacks can be used not only to bypass message authentication with garbage but also to target specific plaintext bits if a polynomial MAC is used in conjunction with a stream cipher. These attacks can also be applied with varying efficiency to other polynomial hashes and MACs, depending on their field properties. Our findings show that especially the use of short polynomial-evaluation MACs should be avoided if the underlying field has a smooth multiplicative order.

Category / Keywords: Cryptanalysis, Galois/Counter Mode, AES-GCM, Cycling Attacks, Weak Keys.

Publication Info: FSE 2012

Date: received 20 Apr 2011, last revised 16 Mar 2012

Contact author: mjos at iki fi