Cryptology ePrint Archive: Report 2013/144

On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes

Gordon Procter and Carlos Cid

Abstract: Universal hash functions are commonly used primitives for fast and secure message authentication in the form of Message Authentication Codes (MACs) or Authenticated Encryption with Associated Data (AEAD) schemes. These schemes are widely used and standardised, the most well known being McGrew and Viega's Galois/Counter Mode (GCM). In this paper we identify some properties of hash functions based on polynomial evaluation that arise from the underlying algebraic structure. As a result we are able to describe a general forgery attack, of which Saarinen's cycling attack from FSE 2012 is a special case. Our attack removes the requirement for long messages and applies regardless of the eld in which the hash function is evaluated. Furthermore we provide a common description of all published attacks against GCM, by showing that the existing attacks are the result of these algebraic properties of the polynomial-based hash function. Finally, we greatly expand the number of known weak GCM keys and show that almost every subset of the keyspace is a weak key class.

Category / Keywords: secret-key cryptography / Universal Hashing, MAC, Galois/Counter Mode, Cycling Attacks, Weak Keys

Publication Info: A short version of this paper was presented at Fast Software Encryption 2013

Date: received 9 Mar 2013

Contact author: gordon procter 2011 at rhul ac uk