Cryptology ePrint Archive: Report 2011/326

SGCM: The Sophie Germain Counter Mode

Markku-Juhani O. Saarinen

Abstract: Sophie Germain Counter Mode (SGCM) is an authenticated encryption mode of operation, to be used with 128-bit block ciphers such as AES. SGCM is a variant of the NIST standardized Galois / Counter Mode (GCM) which has been found to be susceptible to weak key / short cycle forgery attacks. The GCM attacks are made possible by its extremely smooth-order multiplicative group which splits into 512 subgroups. Instead of GCM's $GF(2^{128})$, we use $GF(p)$ with $p=2^{128}+12451$, where $\frac{p-1}{2}$ is also a prime. SGCM is intended for those who want a concrete, largely technically compatible alternative to GCM. In this memo we give a technical specification of SGCM, together with some elements of its implementation, security and performance analysis. Test vectors are also included.

Category / Keywords: Authenticated Encryption, GCM, Sophie Germain Counter Mode.

Date: received 16 Jun 2011, last revised 4 Nov 2011

Contact author: mjos at iki fi

Available formats: PDF | BibTeX Citation

Note: Typos corrected.

Version: 20111104:172351 (All versions of this report)

Discussion forum: Show discussion | Start new discussion