Cryptology ePrint Archive: Report 2013/136

2048XKS-F & 4096XKS-F - Two Software Oriented High Security Block Ciphers

Dieter Schmidt

Abstract: 2048XKS-F (eXtended Key Schedule - Feistel) is a Feistel cipher with a block length of 2048 bit and a key size of 4096 bit or 8192 bit, respectively. It uses the round function of the Subtitution-Permutation-Networks (SPN)1024 [11] and 1024XKS [12]as the f-function. 4096XKS-F is a Feistel cipher with a block length of 4096 bit and a key size of 8192 bit or 16384 bit, respectively. It uses the round function of the Substitution-Permutation-Network (SPN) 2048XKS as the f-function. Both 2048XKS-F and 4096XKS-F have 32 rounds. Additionally, there are #define statements in the reference implementation tocontrol which of the functions are compiled first, e.g. the diffusion layer or the s-box layer. In total, there are 6 #define statements in each reference implementation, making up 64 different ciphers. 2048XKS-F and 4096XKS-F are designed for 32 bit microprocessors with an integer hardware multiplier.

Category / Keywords: secret-key cryptography / Feistel cipher, Substituion-Permutation-Network (SPN)

Date: received 7 Mar 2013

Contact author: dieterschmidt at usa com