Cryptology ePrint Archive: Report 2013/061

On the Indifferentiability of Key-Alternating Ciphers

Elena Andreeva and Andrey Bogdanov and Yevgeniy Dodis and Bart Mennink and John P. Steinberger

Abstract: The Advanced Encryption Standard (AES) is the most widely used block cipher. The high level structure of AES can be viewed as a (10-round) key-alternating cipher, where a t-round key-alternating cipher KA_t consists of a small number t of fixed permutations P_i on n bits, separated by key addition:

KA_t(K,m)= k_t + P_t(... k_2 + P_2(k_1 + P_1(k_0 + m))...),

where (k_0,...,k_t) are obtained from the master key K using some key derivation function.

For t=1, KA_1 collapses to the well-known Even-Mansour cipher, which is known to be indistinguishable from a (secret) random permutation, if P_1 is modeled as a (public) random permutation. In this work we seek for stronger security of key-alternating ciphers --- indifferentiability from an ideal cipher --- and ask the question under which conditions on the key derivation function and for how many rounds t is the key-alternating cipher KA_t indifferentiable from the ideal cipher, assuming P_1,...,P_t are (public) random permutations?

As our main result, we give an affirmative answer for t=5, showing that the 5-round key-alternating cipher KA_5 is indifferentiable from an ideal cipher, assuming P_1,...,P_5 are five independent random permutations, and the key derivation function sets all rounds keys k_i=f(K), where 0<= i<= 5 and f is modeled as a random oracle. Moreover, when |K|=|m|, we show we can set f(K)=P_0(K)+K, giving an n-bit block cipher with an n-bit key, making only six calls to n-bit permutations P_0,P_1,P_2,P_3,P_4,P_5.

Category / Keywords: foundations / Even-Mansour, ideal cipher, key alternating cipher, indifferentiability

Date: received 6 Feb 2013, last revised 19 Feb 2013

Contact author: elena andreeva at esat kuleuven be,a bogdanov@mat dtu dk,dodis@cs nyu edu,bart mennink@esat kuleuven be,jpsteinb@gmail com