Cryptology ePrint Archive: Report 2011/649

On the Security of NMAC and Its Variants

Fanbao Liu and Changxiang Shen and Tao Xie and Dengguo Feng

Abstract: We first propose a general equivalent key recovery attack to a H^2-MAC variant NMAC$_1$, which is also provable secure, by applying a generalized birthday attack. Our result shows that NMAC$_1$, even instantiated with a secure Merkle-Damg{\aa}rd hash function, is not secure. We further show that this equivalent key recovery attack to NMAC$_1$ is also applicable to NMAC for recovering the equivalent inner key of NMAC, in a related key setting. We propose and analyze a series of NMAC variants with different secret approaches and key distributions, we find that a variant NMAC-E, with secret envelop approach, can withstand most of the known attacks in this paper. However, all variants including NMAC itself, are vulnerable to on-line birthday attack for verifiable forgery. Hence, the underlying cryptographic hash functions, based on Merkle-Damg{\aa}rd construction, should be re-evaluated seriously.

Category / Keywords: NMAC, Keying Hash Function, Equivalent Key Recovery, Verifiable Forgery, Birthday Attack.

Date: received 2 Dec 2011

Contact author: liufanbao at gmail com