Cryptology ePrint Archive: Report 2013/212

A Closer Look at HMAC

Krzysztof Pietrzak

Abstract: Bellare, Canetti and Krawczyk~\cite{FOCS:BelCanKra96} show that cascading an $\eps$-secure (fixed input length) PRF gives an $O(\eps n q)$-secure (variable input length) PRF when making at most q prefix-free queries of length n blocks. We observe that this translates to the same bound for NMAC (which is the cascade without the prefix-free requirement but an additional application of the PRF at the end), and give a matching attack, showing this bound is tight. This contradicts the $O(\eps n)$ bound claimed by Koblitz and Menezes~\cite{KobMen12}.

Category / Keywords: secret-key cryptography / HMAC, cascade

Publication Info: unpublished manuscript

Date: received 12 Apr 2013

Contact author: krzpie at gmail com

Available format(s): PDF | BibTeX Citation

Version: 20130414:153904 (All versions of this report)

Discussion forum: Show discussion | Start new discussion