Title: **Security of NMAC and HMAC Based on Non-malleability**

Author: **Fischlin, M.**

Published in: *Topics in Cryptology - CT-RSA 2008, Lecture Notes in Comput. Sci.*, **4964**, 138–154, (2008)

Review by: Mario Forcinito

The security of Nested Message Authentication Code (NMAC) and Hashed Message Authentication Code (HMAC) protocols is a very active research field (see the references below), specially after several attacks were reported on MD5 and SHA1 hash functions.

In this paper the author give a security proof for NMAC and HMAC when they are used as message authentication code based on the assumption of non-malleability and unpredictability of the compression function. This is a somewhat weaker assumption than previous security analysis in which the pseudorandomness of the compression function was required.

Non-malleability is understood as the property by which the knowledge of images of the iterated compression function does not lend any additional power to create another hash value. Unpredictability is the property by which is infeasible to predict the output of the iterated compression function.

The relation among security notions is also analyzed.

See also:

1. J. An and M. Bellare, Constructing VIL-MACs from FIL-MACs: Message authentication under weakened assumptions
`http://cseweb.ucsd.edu/~mihir/papers/fv-mac.html`

2. M. Bellare, New Proofs for NMAC and HMAC: Security without Collision-Resistance
`http://cseweb.ucsd.edu/~mihir/papers/hmac-new.html`

3. H. Krawczyk, M. Bellare and R. Canetti, HMAC: Keyed-Hashing for Message Authentication
`http://cseweb.ucsd.edu/~mihir/papers/rfc2104.txt`

4. P. A. Fouque, G. Leurent and P. Q. Nguyen, Full Key-Recovery Attacks on HMAC NMAC-MD4 and NMAC-MD5
http://www.di.ens.fr/∼leurent/files/HMAC_CR07.pdf