General Distinguishing Attack on NMAC and HMAC with Birthday Attack Complexity

Donghoon Chang[1] and Mridul Nandi[2]

[1] Center for Information Security Technologies(CIST), Korea University, Korea
dhchang@cist.korea.ac.kr
[2] David R. Cheriton School of Computer Science, University of Waterloo, Canada
m2nandi@cs.uwaterloo.ca

Abstract. Kim *et al.* [3] and Contini *et al.* [2] studied on the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1. Especially, they considered the distinguishing attacks. However, they did not describe a generic distinguishing attack on NMAC and HMAC. In this paper, we describe the generic distinguisher to distinguish NMAC and HMAC based on any hash function from the random function with the birthday attack complexity. This result supports Bellare's results on NMAC and HMAC [1].

Keywords : NMAC, HMAC, Distinguishing Attack, Birthday Attack.

1 Introduction.

Since MD4-style hash functions were broken, evaluations on the security of HMAC and NMAC have been required. Kim *et al.* [3] and Contini *et al.* [2] showed the security analyses on them. However, Kim *et al.*' distinguishing attack complexity is far from the birthday attack complexity. Contini *et al.* also suggested 2^{84} as the distinguishing attack complexity of NMAC and HMAC on the reduced SHA-1, which is bigger than the birthday attack complexity. In this paper, we describe the generic distinguisher to distinguish NMAC and HMAC based on any hash function from the random function with the birthday attack complexity. This result supports Bellare's results on NMAC and HMAC [1].

2 NMAC and HMAC

Fig. 1 and 2 show NMAC and HMAC based on a compression function f from $\{0,1\}^n \times \{0,1\}^b$ to $\{0,1\}^n$. K_1 and K_2 are n bits. $\overline{K} = K||0^{b-n}$ where K is n bits. opad is formed by repeating the byte '0x36' as many times as needed to get a b-bit block, and ipad is defined similarly using the byte '0x5c'.

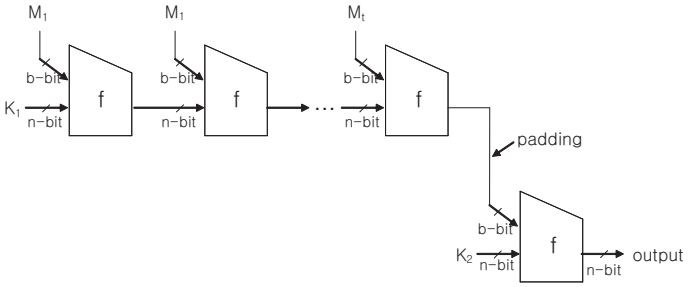

Fig. 1. NMAC

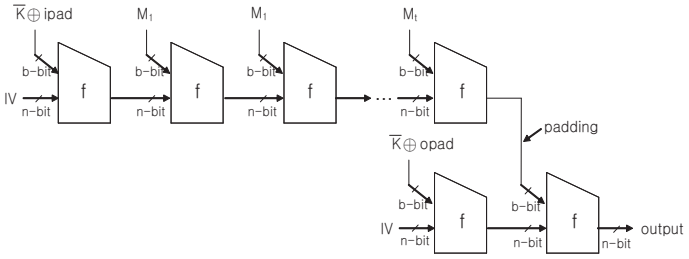

Fig. 2. HMAC

3 General Distinguishing Attack On NMAC and HMAC

See Fig. 3. Distinguisher A choose the padded message $2^{n/2}$ l-block queries such i-th query is $X_i||X||X||\cdots||X$ where only first message block is different and X is a fixed value. We know that there is an internal collision pair in (1) with high probability. Then automatically the pair becomes also an internal collision pair in from (2) to (l). Except the pair, we also know that there exist an internal collision pair in (2) with high probability. By this logic, we can get l internal collision pairs in (l). In case of NMAC and HMAC, since the value in (l) is applied to f once more, we can get about l+1 collision pairs of NMAC and HMAC. On the other hand, in case of random function, we can get only one collision pair on average with high probability. Then, distinguisher A says NMAC (or HMAC) if there are $l/2$ collision pair at least. Otherwise A says the random function. So, with high probability A can distinguish NMAC and HMAC from the random function.

4 Conclusion

In this paper, we described a generic distinguishing attack on NMAC and HMAC where a compression function f is used iteratively and the size of the internal

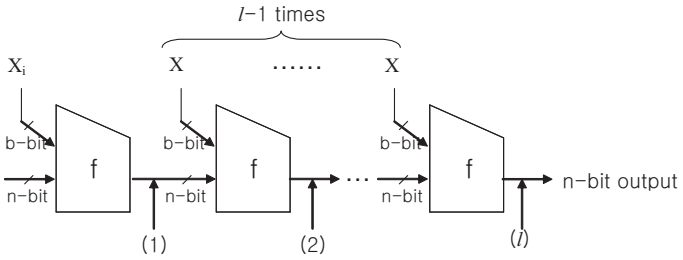

Fig. 3. queries for Distinguishing Attack

state is same as that of the hash output. Therefore, we can know that the security bound of NMAC and HMAC is the birthday attack complexity in case that the size of the internal state is same as that of the hash output.

References

1. M. Bellare, *New Proofs for NMAC and HMAC: Security without Collision-Resistance*, Advances in Cryptology - CRYPTO'06, LNCS ??, Springer-Verlag, pp. ??-??, ??.
2. S. Contini and Y. L. Yin, *Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions*, Advances in Cryptology - Asiacrypt'06, LNCS 4284, Springer-Verlag, pp. 37-53, 2006.
3. J. Kim, A. Biryukov, B. Preneel, and S. Hong, *On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1*, SCN'06, to appear. (http://eprint.iacr.org/2006/187).