General Distinguishing Attacks 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.* [4] and Contini *et al.* [3] 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 generic distinguishing attacks on NMAC and HMAC. In this paper, we describe the generic distinguishers to distinguish NMAC and HMAC with the birthday attack complexity and we prove the security bound when the underlying compression function is the random oracle.

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.* [4] and Contini *et al.* [3] 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 distinguishers to distinguish NMAC and HMAC with the birthday attack complexity and we prove the security bound when the underlying compression function is the random oracle.

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'. $H : \{IV\} \times (\{0,1\}^b)^* \to \{0,1\}^n$ is the iterated hash function. H is defined as follows : $H(IV, x_1||x_2||\cdots||x_t) = f(\cdots f(f(IV, x_1), x_2)\cdots, x_t)$ where x_i is b bits. Let g be a padding method. $g(x) = x||10^t||\mathsf{bin}_{64}(x)$ where t is smallest non-negative integer such that $g(x)$ is a multiple of b and $\mathsf{bin}_i(x)$ is the i-bit binary representation of x. Then, NMAC and HMAC are defined as follows.

$$\mathrm{NMAC}_{K_1,K_2}(M) = H(K_2, g(H(K_1, g(M))))$$
$$\mathrm{HMAC}_K(M) = H(IV, g(\overline{K} \oplus \mathsf{opad}||H(IV, g(\overline{K} \oplus \mathsf{ipad}||M)))).$$

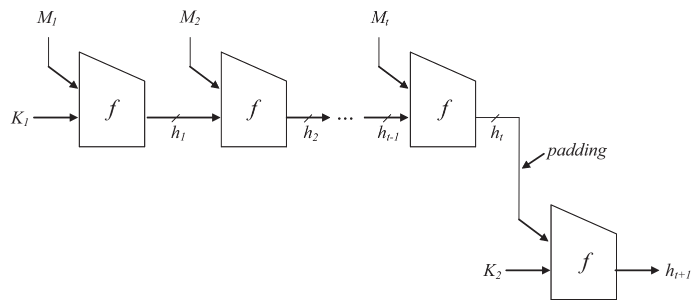

Fig. 1. NMAC ($g(M) = M_1||M_2|| \cdots ||M_t$)

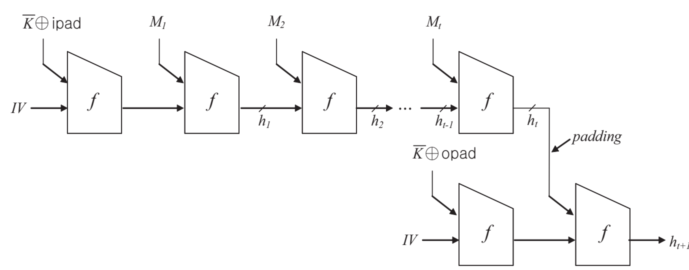

Fig. 2. HMAC ($g(\overline{K} \oplus \mathsf{ipad}||M) = \overline{K} \oplus \mathsf{ipad}||M_1||M_2|| \cdots ||M_t$)

3 General Distinguishing Attack On NMAC and HMAC

Here, we describe three types of distinguishers A_1, A_2 and A_3. In case of A_1 and A_2, we will prove the lower bound of A_1's advantage. On the other hand, A_3 distinguishes heuristically without proving exact proof of security bound. Practically, A_3 is reasonable. For all distinguishers, queries are same as follows. Let q is the number of queries such that t is a fixed value ($t \geqslant 2$) in Fig. 1 and 2. Since g is applied two times in NMAC and HMAC, $t \geqslant 2$ means that the added information of the first padding is different from that of the secoond padding.

Each block is b bits and $c = \lceil \log_2 t \rceil$. In NMAC, $A = K_1$ and $B = K_2$ in Fig. 3. In HMAC, $A = f(IV, \overline{K} \oplus \mathsf{ipad})$ and $B = f(IV, \overline{K} \oplus \mathsf{opad})$ in Fig. 3. For NMAC and HMAC, i-th query is $X_i||0^{64}||\mathsf{bin}_c(1)||0^{b-c}||\cdots||\mathsf{bin}_c(t-2)||0^{b-c}||\mathsf{bin}_c(t-1)$ where each X_i is $b-64$ bits and $X_i \neq X_j$ for any $i \neq j$ and $X_i||0^{64} \neq \mathsf{bin}_c(j)||0^{b-c}$ for any i and j such that $1 \leqslant j \leqslant t-2$. These kinds of messages enable us to prove the security bound in the random oracle model. When we prove the security bound, we will explain in detail.

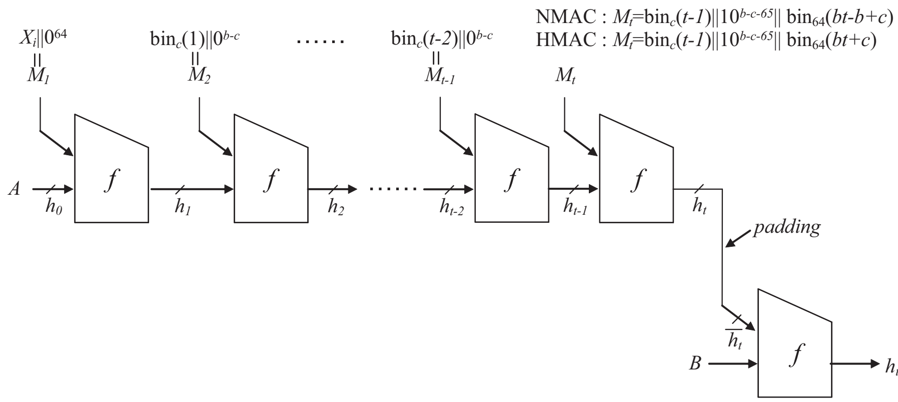

Fig. 3. Attack Strategy. In NMAC, $A = K_1$ and $B = K_2$. In HMAC, $A = f(IV, \overline{K} \oplus \mathsf{ipad})$ and $B = f(IV, \overline{K} \oplus \mathsf{opad})$.

In Fig. 3, for i-query, we denote the values of $h_1 \sim h_{t+1}$ by $h_{1,i} \sim h_{t+1,i}$. Then we define $\mathsf{Pr}[C_m]$ denotes the probability that there exist $h_{m,i} = h_{m,j}$ such that $1 \leqslant i \neq j \leqslant q$. Note that if C_i occurs, then C_j $(i+1 \leqslant j \leqslant t+1)$ also occurs. Therefore, $\mathsf{Pr}[C_{t+1}] = \mathsf{Pr}[C_1 \vee C_1 \vee \cdots \vee C_{t+1}]$. In other words, $\mathsf{Pr}[\neg C_{t+1}] = \mathsf{Pr}[\neg C_1 \wedge \neg C_1 \wedge \cdots \wedge \neg C_{t+1}]$. And $\mathsf{Pr}[C_{t+1}] = 1 - \mathsf{Pr}[\neg C_1 \wedge \neg C_1 \wedge \cdots \wedge \neg C_{t+1}]$.

Distinguisher A_1

A_1 has an access to oracle $\mathcal{O}$ which is NMAC (or HMAC) or the random function from $\{0,1\}^* \rightarrow \{0,1\}^n$. A_1 makes q queries as described above. Then A_1 outputs '1' if there is a collision among q queries, otherwise outputs '0'. We want to compute the bound of the advantage of A_1. For this, we compute the probability that there is a collision for both NMAC (or HMAC) and the random function. In case of the random function, we denote $\mathsf{Pr}_r[C]$ by the probability that there exist a collsion of the random function. Let $N = 2^n$. Let $x_{i,j} = h_{i-1}||M_i$ in Fig. 3. Then $\mathsf{Pr}[\neg C_1] = \frac{N(N-1)\cdots(N-q+1)}{N^q}$ because all X_i $(1 \leqslant i \leqslant q)$ are different. When C_1 does not occur, $x_{1,i} \neq x_{2,j}$ for all i and j. So, $\mathsf{Pr}[\neg C_2|\neg C_1] = \mathsf{Pr}[\neg C_2] = \mathsf{Pr}[\neg C_1] = \frac{N(N-1)\cdots(N-q+1)}{N^q}$. So, $\mathsf{Pr}[\neg C_1 \wedge \neg C_2] = (\mathsf{Pr}[\neg C_1])^2 = (\frac{N(N-1)\cdots(N-q+1)}{N^q})^2$. Similarly, we can know $\mathsf{Pr}[\neg C_1 \wedge$

$\cdots \wedge \neg C_{t+1}] = (\mathsf{Pr}[\neg C_1])^{t+1} = (\frac{N(N-1)\cdots(N-q+1)}{N^q})^{t+1}$. Therefore, $\mathsf{Pr}[C_{t+1}] = 1-(\frac{N(N-1)\cdots(N-q+1)}{N^q})^{t+1}$. On the other hand, in case of the random function, $\mathsf{Pr}_r[C] = 1-\frac{N(N-1)\cdots(N-q+1)}{N^q}$.

$$\begin{aligned}\mathsf{Adv}_{A_1}(q) &= |\mathsf{Pr}[A_1^{\text{HMAC or NMAC}} = 1] - \mathsf{Pr}[A_1^{\text{Rand}} = 1]| \\ &= |\frac{N(N-1)\cdots(N-q+1)}{N^q} - (\frac{N(N-1)\cdots(N-q+1)}{N^q})^{t+1}|\end{aligned}$$

With using $1-x \leqslant e^{-x}$ for $x \leqslant 1$, $\frac{N(N-1)\cdots(N-q+1)}{N^q} = (1-\frac{1}{N})(1-\frac{2}{N})\cdots(1-\frac{q-1}{N}) \leqslant e^{\frac{1}{N}+\frac{2}{N}+\cdots+\frac{q-1}{N}} = e^{-\frac{q(q-1)}{2N}}$. If $q \leqslant \sqrt{2N}$ then $\frac{q(q-1)}{2N} \leqslant 1$. With using $e^{-x} \leqslant 1-(1-e^{-1})x$ for $x \leqslant 1$ [1], we know that $e^{-\frac{q(q-1)}{2N}} \leqslant 1-(1-e^{-1})\frac{q(q-1)}{2N}$. Since $1-e^{-1} > 0.632$, $e^{-\frac{q(q-1)}{2N}} < 1-0.632\cdot\frac{q(q-1)}{2N}$. And $\frac{N(N-1)\cdots(N-q+1)}{N^q} \geqslant 1-\frac{q(q-1)}{2N}$ by the result of [1]. Therefore, $1-\frac{q(q-1)}{2N} \leqslant \frac{N(N-1)\cdots(N-q+1)}{N^q} < 1-0.632\cdot\frac{q(q-1)}{2N}$. Finally,

$$\mathsf{Adv}_{A_1}(q) \geqslant |(1-\frac{q(q-1)}{2N}) - (1-0.632\cdot\frac{q(q-1)}{2N})^{t+1}|$$

In case of $q = \sqrt{N}$, $\mathsf{Adv}_{A_1}(q) \approx |\frac{1}{2} - 0.684^{t+1}|$. When $t = 11$, $\mathsf{Adv}_{A_1}(q) \approx 0.49$.

Distinguisher A_2

A_2 has an access to oracle $\mathcal{O}$ which is NMAC (or HMAC) or the random function from $\{0,1\}^* \rightarrow \{0,1\}^n$.

- A_2 makes q queries as described above.
- If there is no collision among outputs of q queries, return 0.
- If there is a collision (M, M') among q queries,
  - When comparing with NMAC, A_2 makes new queries T and T' such that $T = M||10^{b-c-65}||\mathsf{bin}_{64}(bt-b+c)$ and $T' = M||10^{b-c-65}||\mathsf{bin}_{64}(bt-b+c)$.
  - When comparing with HMAC, A_2 makes new queries T and T' such that $T = M||10^{b-c-65}||\mathsf{bin}_{64}(bt+c)$ and $T' = M||10^{b-c-65}||\mathsf{bin}_{64}(bt+c)$.
- If $\mathcal{O}(T) = \mathcal{O}(T')$, then return 1 otherwise 0.

We know that $\mathsf{Pr}[C_t] = 1-(\frac{N(N-1)\cdots(N-q+1)}{N^q})^t$. We want to compute $\mathsf{Pr}[|\{h_{t,i}\}_{i\leqslant q}| = |\{h_{t+1,j}\}_{j\leqslant q}| \mid C_t]$. This probability means that there is no collision which do not collide in h_t. Since the size of $\{h_{t,i}\}_{i\leqslant q}$ is q at most and $\{h_{t,i}||x_{t+1}\}_{i\leqslant q} \cap \{h_{j,i}||x_{j+1}\}_{i\leqslant q, j\leqslant t-1} = \emptyset$, $\mathsf{Pr}[|\{h_{t,i}\}_{i\leqslant q}| = |\{h_{t+1,j}\}_{j\leqslant q}| \mid C_t] \geqslant \frac{N(N-1)\cdots(N-q+1)}{N^q}$. Therefore, $\mathsf{Pr}[|\{h_{t,i}\}_{i\leqslant q}| = |\{h_{t+1,j}\}_{j\leqslant q}| \wedge C_t] \geqslant (\frac{N(N-1)\cdots(N-q+1)}{N^q})(1-(\frac{N(N-1)\cdots(N-q+1)}{N^q})^t)$.

$$\begin{aligned}
\mathsf{Adv}_{A_2}(q) &= |\mathsf{Pr}[A_2^{\text{HMAC or NMAC}} = 1] - \mathsf{Pr}[A_2^{\text{Rand}} = 1]| \\
&\geqslant |\mathsf{Pr}[|\{h_{t,i}\}_{i \leqslant q}| = |\{h_{t+1,j}\}_{j \leqslant q}| \ \wedge \ C_t] - N^{-1}| \\
&\geqslant |\frac{N(N-1)\cdots(N-q+1)}{N^q} - (\frac{N(N-1)\cdots(N-q+1)}{N^q})^{t+1} - N^{-1}| \\
&\geqslant |(1 - \frac{q(q-1)}{2N}) - (1 - 0.632 \cdot \frac{q(q-1)}{2N})^{t+1} - N^{-1}|
\end{aligned}$$

In case of $q = \sqrt{N}$, $\mathsf{Adv}_{A_2}(q) \approx |\frac{1}{2} - 0.684^{t+1}|$. When $t = 11$, $\mathsf{Adv}_{A_2}(q) \approx 0.49$.

Distinguisher A_3

See Fig. 3. We know that there is an internal collision pair in h_1 with about the following probability.

$$\binom{2^{n/2}}{2} \cdot 2^{-n} = \frac{1}{2} - 2^{(2-n)/2}$$

Then automatically the pair becomes also an internal collision pair in from h_2 to h_{t+1} in Fig. 3. Except the pair, we also know that there exist an internal collision pair which is collided in h_2 with above probability. By this logic, we can get t internal collision pairs in h_t. In case of NMAC and HMAC, since the value in h_t is applied to f once more, we can get $(t+1) \cdot (\frac{1}{2} - 2^{(2-n)/2})$ collision pairs of NMAC and HMAC on average. On the other hand, in case of random function, we can get about $(\frac{1}{2} - 2^{(2-n)/2})$ collision pairs.

	NMAC or HMAC	Random Function
Average	$(t+1) \cdot (\frac{1}{2} - 2^{(2-n)/2}) \approx \frac{t+1}{2}$	$(\frac{1}{2} - 2^{(2-n)/2}) \approx \frac{1}{2}$
Standard Deviation	$\approx \sqrt{2}/2$	$\approx \sqrt{2 \cdot (t+1)}/2$

Then, distinguisher A_3 says '1' (NMAC or HMAC) if there are $\frac{t+1}{2} - \sqrt{2(t+1)}$ collision pairs at least. Otherwise A_3 says '0' (random function). So, with high probability A_3 can distinguish NMAC and HMAC from the random function. In case $t = 31$, Advantage of A_3 is

$$\begin{aligned}
\mathsf{Adv}_{A_3}(2^{n/2}) &= |\mathsf{Pr}[A_3^{\text{NMAC or HMAC}} = 1] - \mathsf{Pr}[A_3^{Rand} = 1]| \\
&\approx |0.977 - 0| = 0.977.
\end{aligned}$$

4 Conclusion

In this paper, we described generic distinguishing attacks on NMAC and HMAC where a compression function f is used iteratively and the size of the internal 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, J. Kilian, and P. Rogaway, *The Security of the Cipher Block Chaining Message Authentication Code*, Appears in Journal of Computer and System Sciences, Vol. 61, No. 3, Dec 2000, pp. 362-399.
2. M. Bellare, *New Proofs for NMAC and HMAC: Security without Collision-Resistance*, Advances in Cryptology - CRYPTO'06, LNCS ??, Springer-Verlag, pp. ??-??, ??.
3. 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.
4. 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).