1 IND-CCA2

For each of two games respectively evaluating data and nonce confidentialities, CryptoVerif reduces the advantage of every adversary $A$

- making $q_G$ queries to $Gen^{E(k_{src}, \cdot)}(\cdot)$, $q_V$ queries to $Verif^{E^{-1}(k_{src}, \cdot)}(\cdot)$, and $q_H$ queries to $H(\cdot)$ in the game, and
- running the game in $T_A$ time units,

to an expression depending on the advantage of an adversary $B$

- making $q_G + 1$ queries to the encryption oracle $E(k_{src}, \cdot)$ and $q_V$ queries to the decryption oracle $E^{-1}(k_{src}, \cdot)$ in an IND-CCA2 game, and
- running a IND-CCA2 game in $T_B$ time units with $T_B = T_A + P_1(q_G, q_V, s)$ time units, where $P_1(q_G, q_V, s)$ is polynomial in $q_G$, $q_V$, and the message size $s$.

We now evaluate the IND-CCA2 advantage of such an adversary $B$ when using our encryption scheme.

By Theorem 3.2 in [4], there exist two adversaries $C$ and $D$ such that

$$\text{Adv}^{\text{IND-CCA2}}_{\text{AES-CBC, HMAC-SHA-256\_trunc}}(B) \leq 2 \times \text{Adv}^{\text{INT-CTXT}}_{\text{AES-CBC, HMAC-SHA-256\_trunc}}(C) + \text{Adv}^{\text{IND-CPA}}_{\text{AES-CBC, HMAC-SHA-256\_trunc}}(D)$$

and

- $C$ and $D$ run in time $O(T_B)$,
- $C$ makes $q_G + 1$ queries to the encryption oracle $E(k_{src}, \cdot)$ and $q_V$ queries to $Verif^{E^{-1}(k_{src}, \cdot)}(\cdot)$, and
- $D$ makes $q_G + 1$ queries to the left-right oracle $LR(k_{src}, \cdot)$.

By Theorems 4.3 and 4.4 in [4], there exist two adversaries $F$ and $G$ such that

$$\text{Adv}^{\text{IND-CCA2}}_{\text{AES-CBC, HMAC-SHA-256\_trunc}}(B) \leq 2 \times \text{Adv}^{\text{SUF-CMA}}_{\text{HMAC-SHA-256\_trunc}}(F) + \text{Adv}^{\text{IND-CPA}}_{\text{AES-CBC}}(G)$$

and

- $F$ (resp. $G$) uses the same resources as $C$ (resp. $D$), except that
- each tag query of $F$ is 128 bits longer than that of $C$.

By Theorem 4.8.1 in [1], there exists an adversary $I$ such that

$$\text{Adv}^{\text{IND-CCA2}}_{\text{AES-CBC, HMAC-SHA-256\_trunc}}(B) \leq 2 \times \text{Adv}^{\text{SUF-CMA}}_{\text{HMAC-SHA-256\_trunc}}(F) + 2 \times \text{Adv}^{\text{PRF}}_{\text{AES}}(I) + \frac{(14 \times (q_G + 1))^2}{2^{128}}$$

and

- $I$ runs in time $O(T_B)$ and

---

1 We instantiate the parameter $\ell$ in Theorem 4.4 with 128, because the difference between the length of the ciphertext and the plaintext in our implementation of AES-CBC is 1 block of 128 bits.

2 In Theorem 4.8.1, we instantiate $n$ by 128 because we use AES-128, moreover the parameter $\sigma$ is instantiated as follows: $\sigma$ is the total number of 128 bits blocks generated by the $q_G + 1$ queries to the encryption oracle $E(k_{src}, \cdot)$ made by $F$. In our case $\sigma = 14 \times (q_G + 1)$. 

---
makes $14 \times (q_G + 1)$ queries to the encryption oracle modeling the encryption function of AES.

By Proposition 2.7 of [3], there exists an adversary $J$ such that

$$\text{Adv}^{\text{IND-CCA2}}_{\text{AES-CBC,HMAC-SHA-256})} (B) \leq 2 \times (\text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256}} (J) + \frac{q_V}{2^{72}}) + 2 \times \text{Adv}^{\text{PRF}}_{\text{AES}} (I) + \frac{196 \times (q_G + 1)^2}{2^{128}}$$

and

- $J$ runs in time $O(T_B)$
- makes $q_V$ queries to the verification oracle of HMAC-SHA-256.

Now, for any function $f$, $\text{Adv}^{\text{PRF}}_{\text{f}} (A) \leq \text{Adv}^{\text{PRF}}_{\text{f}} (B)$ with $A$ and $B$ two attackers making the same queries and running the same time.

Hence, there exists an adversary $L$ which runs in time $O(T_B)$ and makes $q_V$ queries to the verification oracle of HMAC-SHA-256, such that $\text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256}} (J) \leq \text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256}} (L)$

We note $\text{comp-SHA-256}$ (resp. $\text{comp-SHA-256}^*$) the compression function used in SHA-256 (resp. its dual function). Using Lemma 5.2 from [2], we obtain

$$\text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256}} (L) \leq \text{Adv}^{\text{RKA}}_{\text{comp-SHA-256}} (M) + \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (N)$$

where $M$ is a related key adversary that performs two oracle queries and has time $O(T_B)$.

By Theorem 3.3 of [2], there exist two adversaries $N$ and $O$ such that

$$\text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256}} (L) \leq \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (N) + \frac{(q_V - 1)q_V}{2m} \times (8 \times \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (O) + \frac{1}{2^{256}})$$

and $m = 4$ is number of blocks per query of $L$. $N$ makes $q_V$ queries and runs in $O(T_B)$ time, $O$ makes 2 queries and run in $O(T)$, $T$ being the time for one computation of $\text{comp-SHA-256}$.

So,

$$\text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256}} (L) \leq \text{Adv}^{\text{RKA}}_{\text{comp-SHA-256}} (M) + \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (N) + \frac{(q_V - 1)q_V}{2} \times (8 \times \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (O) + \frac{1}{2^{256}})$$

Consequently,

$$\text{Adv}^{\text{IND-CCA2}}_{\text{AES-CBC,HMAC-SHA-256})} (B) \leq 2 \times \text{Adv}^{\text{RKA}}_{\text{comp-SHA-256}} (M) + 2 \times \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (N) + \frac{(q_V - 1)q_V}{2} \times (8 \times \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (O) + \frac{1}{2^{256}}) + \frac{q_V}{2^{71}} + 2 \times \text{Adv}^{\text{PRF}}_{\text{AES}} (I) + \frac{196 \times (q_G + 1)^2}{2^{128}}$$

**Estimation.** Here, we assume $q_V = 2^{20}$ and $q_G = 2^{30}$. We now bound the strength of the adversaries using estimations based on the current best attacks on AES ($2^{126.1}$) and comp-SHA-256 ($2^{256}$):

- $\text{Adv}^{\text{RKA}}_{\text{comp-SHA-256}} (M)$
- $\text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}} (N)$
- $\text{Adv}^{\text{PRF}}_{\text{AES}} (I)$

---

3Here, we truncate from $d = 256$ bits (HMAC-SHA-256) to $s = 72$ bits. Moreover, $O(256 + 72) = O(1)$.

4The input of SHA-256 is $14 \times 16$ bytes $= 3.5 \times 512$ bits, now each block in SHA-256 is of size 512 bits, so we need 4 blocks.
For AES, if the attacker can make $N_{AES}$ queries, its advantage can be estimated by $N_{AES}^2 2^{126}$. For SHA-256, if the attacker can make $N_{SHA}$ queries to the compression function, then the advantage of the attacker can be estimated by $N_{SHA}^2 2^{256}$.

Here, we assume $N_{AES} \leq 2^{70}$ and $N_{SHA} \leq 2^{100}$. So,

$$\text{Adv}^{PRF}_{AES}(I) \leq 2^{-56.1} \quad \text{Adv}^{RKA}_{comp-SHA-256}(M) \leq 2^{-156}$$

$$\text{Adv}^{PRF}_{comp-SHA-256}(N) \leq 2^{-156} \quad \text{Adv}^{PRF}_{comp-SHA-256}(O) \leq 2^{-156}$$

Hence, we obtain the following estimations:

$$\text{Adv}^{PRF}_{HMAC-SHA-256\_trunc}(L) \leq 2^{-156} + 2^{-156} + 2^{30} (2^{32} - 156 + 2^{-256}) \leq 2^{-113}$$

$$\text{Adv}^{IND-CCA2}_{AES-CBC,HMAC-SHA-256\_trunc}(B) \leq 2^{-156} + 2^{256} + 2^{40} (2^{32} - 156 + 2^{-256}) + 2^{-51} + 2^{-56.1} + 2^{-59}$$

$$\leq 2^{-50}$$

2 Data Confidentiality

Below, we first recall the result from CryptoVerif.

For all adversaries $A$

- making $q_G$ queries to $Gen^{E(k_{src}, \cdot)}(\cdot)$, $q_V$ queries to $Verif^{E^{-1}(k_{src}, \cdot)}(\cdot)$, and $q_H$ queries to $H(\cdot)$ in the $FG$ game, and
- running the $FG$-game in $T_A$ time units,

there exists an adversary $B$

- making $q_G + 1$ queries to the encryption oracle $E(k_{src}, \cdot)$ and $q_V$ queries to the decryption oracle $E^{-1}(k_{src}, \cdot)$ in the $IND-CCA2$ game, and
- running the $IND-CCA2$ game in $T_B$ time units with $T_B = T_A + P_1(q_G, q_V, s)$ time units, where $P_1(q_G, q_V, s)$ is polynomial in $q_G, q_V$, and the message size $s$

such that

$$\text{Adv}^{FG}_{AES-CBC,HMAC-SHA-256\_trunc}(A) \leq 2 \times \text{Adv}^{IND-CCA2}_{AES-CBC,HMAC-SHA-256\_trunc}(B)$$

From Section 1, we can deduce that

$$\text{Adv}^{FG}_{AES-CBC,HMAC-SHA-256\_trunc}(A) \leq 4 \times \text{Adv}^{RKA}_{comp-SHA-256}(M) + 4 \times \text{Adv}^{PRF}_{comp-SHA-256}(N) + 2(q_V - 1)q_V \times \left( 8 \times \text{Adv}^{PRF}_{comp-SHA-256}(O) + \frac{1}{2^{256}} \right) + \frac{q_V}{2^{70}} + 4 \times \text{Adv}^{AES}_{AES}(I) + \frac{196 \times (q_G + 1)^2}{2^{127}}$$

where $N$ makes $q_V$ queries and runs in $O(T_B) \text{ time}$, $O$ makes 2 queries and run in $O(T)$, $T$ being the time for one computation of $comp-SHA-256$.

Estimation. To obtain an estimation, we use the same values as in Section 1. We obtain:

$$\text{Adv}^{FG}_{AES-CBC,HMAC-SHA-256\_trunc}(A) \leq 2 \times 2^{-50} \leq 2^{-49}$$
3 Nonce Confidentiality

Below, we first recall the result from CryptoVerif.

For all adversaries $A$:
- making $q_G$ queries to $Gen^E(k_{src}, \cdot)$, $q_V$ queries to $Verif^{E^{-1}(k_{src}, \cdot)}(\cdot)$, $q_H$ queries to $H(\cdot)$, and $nb_A$ tries in the $N$–$conf$ game, and
- running the $N$–$conf$ game in $T_A$ times units,

there exists an adversary $B$:
- making $q_G + 1$ queries to $E(k_{src}, \cdot)$ and $q_V$ queries to $E^{-1}(k_{src}, \cdot)$ in the $IND$–$CCA2$ game, and
- running the $IND$–$CCA2$ game in $T_B$ time units with $T_B = T_A + P_2(q_G, q_V, s)$ time units, where $P_2(q_G, q_V, s)$ is polynomial in $q_G, q_V$, and the message size $s$

such that:

$$Adv_{N-conf}^{AES$–$CBC, HMAC$–$SHA$–$256_{trunc}}(A) \leq \frac{nb_A + q_H + q_G}{2^{n_n}} + Adv_{IND$–$CCA2}^{AES$–$CBC, HMAC$–$SHA$–$256_{trunc}}(B)$$

From Section 1, we can deduce that

$$Adv_{N-conf}^{AES$–$CBC, HMAC$–$SHA$–$256_{trunc}}(A) \leq \frac{nb_A + q_H + q_G}{2^{n_n}} + 2 \times Adv_{comp-SHA$–$256}^{RKA}(M) + 2 \times Adv_{comp-SHA$–$256}^{PRF}(N) + (q_V - 1)q_V \times (8 \times Adv_{comp-SHA$–$256}^{PRF}(O) + \frac{1}{2^{256}}) + \frac{q_V}{2^{71}} + 2 \times Adv_{AES}^{PRF}(I) + \frac{196 \times (q_G + 1)^2}{2^{128}}$$

and $N$ makes $q_V$ queries and runs in $O(T_B)$ time, $O$ makes 2 queries and run in $O(T)$, $T$ being the time for one computation of $comp$–$SHA$–$256$.

**Estimation.** To obtain an estimation, we use the same values as in Section 1 and we assume $nb_A = q_V = 2^{20}$ and $q_H = 2^{40}$. Moreover, in our case, $n_n = 96$. We obtain:

$$Adv_{N-conf}^{AES$–$CBC, HMAC$–$SHA$–$256_{trunc}}(A) \leq 2^{-55} + 2^{-50} \leq 2^{-49}$$

4 Unforgeability

Below, we first recall the result from CryptoVerif. For all adversaries $A$:
- making $q_G$ queries to $Gen^E(k_{src}, \cdot)$, $q_V$ queries to $Verif^{E^{-1}(k_{src}, \cdot)}(\cdot)$, $q_H$ queries to $H(\cdot)$ in the $UF$–$CMVA$ game, and
- running the $UF$–$CMVA$ game in $T_A$ time units,

there exists an adversary $B$:
- making $q_G$ queries to $E(k_{src}, \cdot)$ and $q_V + 1$ queries to $E^{-1}(k_{src}, \cdot)$ in the $INT$–$PTXT$ game, and
running the INT-PTXT game in $T_B$ time units with $T_B = T_A + P_3(q_G, q_V, s)$ time units, where $P_3(q_G, q_V, s)$ is polynomial in $q_G, q_V,$ and the message size $s$ such that:

$$\text{Adv}^{\text{UF-CMVA}}_{\text{AES-CBC, HMAC-SHA-256, trunc}}(A) \leq \text{Adv}^{\text{INT-PTXT}}_{\text{AES-CBC, HMAC-SHA-256, trunc}}(B)$$

By Theorems 4.3 in [4], there exists an $C$ such that

$$\text{Adv}^{\text{UF-CMVA}}_{\text{AES-CBC, HMAC-SHA-256, trunc}}(A) \leq \text{Adv}^{\text{WUF-CMA}}_{\text{HMAC-SHA-256, trunc}}(C)$$

and

- $C$ uses the same resources as $A$, except that
- each tag query of $C$ is 128 bits longer than that of $A$.

By Proposition 2.7 of [3], there exists an adversary $D$ such that

$$\text{Adv}^{\text{UF-CMVA}}_{\text{AES-CBC, HMAC-SHA-256, trunc}}(A) \leq \text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256, trunc}}(D) + \frac{q_V}{2^{72}}$$

and

- $D$ runs in time $O(T_B)$ and
- makes $q_V$ queries to the verification oracle of HMAC-SHA-256$_{\text{trunc}}$.

Now, from Section 1, there exists adversaries $M', N', O'$ such that

$$\text{Adv}^{\text{PRF}}_{\text{HMAC-SHA-256, trunc}}(D) \leq \text{Adv}^{\text{RKA}}_{\text{comp-SHA-256}}(M') + \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}}(N') + \frac{(q_V - 1)q_V}{2} \times (8 \times \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}}(O') + \frac{1}{2^{256}})$$

and $M'$ is a related key adversary that performs two oracles queries and has time $O(T_B)$, $N'$ makes $q_V$ queries and runs in $O(T_B)$ time, $O'$ makes 2 queries and run in $O(T)$, $T$ being the time for one computation of comp-SHA-256.

So,

$$\text{Adv}^{\text{UF-CMVA}}_{\text{AES-CBC, HMAC-SHA-256, trunc}}(A) \leq \text{Adv}^{\text{RKA}}_{\text{comp-SHA-256}}(M') + \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}}(N') + \frac{(q_V - 1)q_V}{2} \times (8 \times \text{Adv}^{\text{PRF}}_{\text{comp-SHA-256}}(O') + \frac{1}{2^{256}}) + \frac{q_V}{2^{72}}$$

Estimation. Using the same value and estimation again, we obtain:

$$\text{Adv}^{\text{UF-CMVA}}_{\text{AES-CBC, HMAC-SHA-256, trunc}}(A) \leq 2^{-113} + 2^{-52} \leq 2^{-51}$$
References


