1 IND-CCA2

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

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

to an expression depending on the advantage of an adversary $\mathcal{B}$

- making $q_G + 1$ queries to the encryption oracle $\mathcal{E}(k_{src},\cdot)$ and q_V queries to the decryption oracle $\mathcal{E}^{-1}(k_{src},\cdot)$ in a *IND-CCA2* game, and
- running a *IND-CCA2* game in $T_{\mathcal{B}}$ time units with $T_{\mathcal{B}} = T_{\mathcal{A}} + P_1(q_G, q_V, s)$ 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 $\mathcal{B}$ when using our encryption scheme.

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

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

and

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

By Theorems 4.3 and 4.4 in [4][1], there exist two adversaries $\mathcal{F}$ and $\mathcal{G}$ such that

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

and

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

By Theorem 4.8.1 in [1][2], there exists an adversary $\mathcal{I}$ such that

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

and

- $\mathcal{I}$ runs in time $O(T_{\mathcal{B}})$ and

[1] We instantiate the parameter ℓ 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 σ is instantiated as follows: σ is the total number of 128 bits blocks generated by the $q_G + 1$ queries to the encryption oracle $\mathcal{E}(k_{src},\cdot)$ made by $\mathcal{F}$. 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][3] , there exists an adversary $\mathcal{J}$ such that

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

and

- $\mathcal{J}$ runs in time $O(T_{\mathcal{B}})$ and
- makes q_V queries to the verification oracle of HMAC-SHA-256$_{trunc}$.

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

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

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

$$\mathbf{Adv}^{\mathit{PRF}}_{\mathtt{HMAC\text{-}SHA\text{-}256}}(\mathcal{L}) \leq \mathbf{Adv}^{\mathit{RKA}}_{\mathtt{comp\text{-}SHA\text{-}256}^*}(\mathcal{M}) + \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{NMAC\text{-}SHA\text{-}256}}(\mathcal{L})$$

where $\mathcal{M}$ is a related key adversary that performs two oracle queries and has time $O(T_{\mathcal{B}})$.
By Theorem 3.3 of [2], there exists two adversaries $\mathcal{N}$ and $\mathcal{O}$ such that

$$\mathbf{Adv}^{\mathit{PRF}}_{\mathtt{NMAC\text{-}SHA\text{-}256}}(\mathcal{L}) \leq \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{comp\text{-}SHA\text{-}256}}(\mathcal{N}) + \frac{(q_V-1)q_V}{2} \times \big(2m \times \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{comp\text{-}SHA\text{-}256}}(\mathcal{O}) + \frac{1}{2^{256}}\big)$$

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

$$\begin{aligned}\mathbf{Adv}^{\mathit{PRF}}_{\mathtt{HMAC\text{-}SHA\text{-}256}_{trunc}}(\mathcal{L}) \quad \leq \quad & \mathbf{Adv}^{\mathit{RKA}}_{\mathtt{comp\text{-}SHA\text{-}256}^*}(\mathcal{M}) + \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{comp\text{-}SHA\text{-}256}}(\mathcal{N}) + \\ & \frac{(q_V-1)q_V}{2} \times \big(8 \times \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{comp\text{-}SHA\text{-}256}}(\mathcal{O}) + \frac{1}{2^{256}}\big)\end{aligned}$$

Consequently,

$$\begin{aligned}\mathbf{Adv}^{\mathit{IND\text{–}CCA2}}_{\mathtt{AES\text{-}CBC},\mathtt{HMAC\text{-}SHA\text{-}256}_{trunc}}(\mathcal{B}) \quad \leq \quad & 2 \times \mathbf{Adv}^{\mathit{RKA}}_{\mathtt{comp\text{-}SHA\text{-}256}^*}(\mathcal{M}) + 2 \times \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{comp\text{-}SHA\text{-}256}}(\mathcal{N}) + \\ & (q_V-1)q_V \times \big(8 \times \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{comp\text{-}SHA\text{-}256}}(\mathcal{O}) + \frac{1}{2^{256}}\big) + \\ & \frac{q_V}{2^{71}} + 2 \times \mathbf{Adv}^{\mathit{PRF}}_{\mathtt{AES}}(\mathcal{I}) + \frac{196\times(q_G+1)^2}{2^{128}}\end{aligned}$$

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}):

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

[4]The input of `SHA-256` is $14 * 16$ bytes $= 3.5 * 512$ bits, now each block in `SHA-256` is of size 512 bits, so we need 4 blocks.

For AES, if the attacker can make $N_{\texttt{AES}}$ queries, its advantage can be estimated by $\frac{N_{\texttt{AES}}}{2^{126.1}}$. For SHA-256, if the attacker can make $N_{\texttt{SHA}}$ queries to the compression function, then the advantage of the attacker can be estimated by $\frac{N_{\texttt{SHA}}}{2^{256}}$.

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

$$\mathbf{Adv}^{PRF}_{\texttt{AES}}(\mathcal{I}) \leq 2^{-56.1} \qquad \mathbf{Adv}^{RKA}_{\texttt{comp-SHA-256}^*}(\mathcal{M}) \leq 2^{-156}$$
$$\mathbf{Adv}^{PRF}_{\texttt{comp-SHA-256}}(\mathcal{N}) \leq 2^{-156} \qquad \mathbf{Adv}^{PRF}_{\texttt{comp-SHA-256}}(\mathcal{O}) \leq 2^{-156}$$

Hence, we obtain the following estimations:

$$\begin{array}{rcl} \mathbf{Adv}^{PRF}_{\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{L}) & \leq & 2^{-156} + 2^{-156} + 2^{39}\left(2^3 2^{-156} + 2^{-256}\right) \leq 2^{-113} \\ \mathbf{Adv}^{IND\text{–}CCA2}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{B}) & \leq & 2.2^{-156} + 2.2^{-156} + 2^{40}\left(2^3 2^{-156} + 2^{-256}\right) + 2^{-51} + 2.2^{-56.1} + 2^{-59} \\ & \leq & 2^{-50} \end{array}$$

2 Data Confidentiality

Below, we first recall the result from *CryptoVerif.*

For all adversaries $\mathcal{A}$

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

there exists an adversary $\mathcal{B}$

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

such that

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

From Section 1, we can deduce that

$$\begin{array}{rcl} \mathbf{Adv}^{FG}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{A}) & \leq & 4 \times \mathbf{Adv}^{RKA}_{\texttt{comp-SHA-256}^*}(\mathcal{M}) + \\ & & 4 \times \mathbf{Adv}^{PRF}_{\texttt{comp-SHA-256}}(\mathcal{N}) + \\ & & 2(q_V - 1)q_V \times \left(8 \times \mathbf{Adv}^{PRF}_{\texttt{comp-SHA-256}}(\mathcal{O}) + \dfrac{1}{2^{256}}\right) + \\ & & \dfrac{q_V}{2^{70}} + 4 \times \mathbf{Adv}^{PRF}_{\texttt{AES}}(\mathcal{I}) + \dfrac{196 \times (q_G + 1)^2}{2^{127}} \end{array}$$

where $\mathcal{N}$ makes q_V queries and runs in $O(T_{\mathcal{B}})$ time, $\mathcal{O}$ 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:

$$\mathbf{Adv}^{FG}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{A}) \quad \leq \quad 2 \times 2^{-50} \leq 2^{-49}$$

3 Nonce Confidentiality

Below, we first recall the result from *CryptoVerif*.

For all adversaries $\mathcal{A}$:

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

there exists an adversary $\mathcal{B}$:

- making $q_G + 1$ queries to $\mathcal{E}(k_{src},\cdot)$ and q_V queries to $\mathcal{E}^{-1}(k_{src},\cdot)$ in the *IND-CCA2* game, and
- running the *IND-CCA2* game in $T_{\mathcal{B}}$ time units with $T_{\mathcal{B}} = T_{\mathcal{A}} + P_2(q_G, q_V, s)$ time units, where $P_2(q_G, q_V, s)$ is polynomial in q_G, q_V, and the message size s

such that:

$$\mathbf{Adv}^{N\text{–}conf}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{A}) \leq \frac{nb_A + q_H + q_G}{2^{\eta_n}} + \mathbf{Adv}^{IND\text{–}CCA2}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{B})$$

From Section 1, we can deduce that

$$\begin{aligned}
\mathbf{Adv}^{N\text{–}conf}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{A}) \quad \leq \quad & \frac{nb_A + q_H + q_G}{2^{\eta_n}} + 2 \times \mathbf{Adv}^{RKA}_{\texttt{comp-SHA-256}^*}(\mathcal{M}) + \\
& 2 \times \mathbf{Adv}^{PRF}_{\texttt{comp-SHA-256}}(\mathcal{N}) + \\
& (q_V - 1)q_V \times \left(8 \times \mathbf{Adv}^{PRF}_{\texttt{comp-SHA-256}}(\mathcal{O}) + \frac{1}{2^{256}}\right) + \\
& \frac{q_V}{2^{71}} + 2 \times \mathbf{Adv}^{PRF}_{\texttt{AES}}(\mathcal{I}) + \frac{196 \times (q_G + 1)^2}{2^{128}}
\end{aligned}$$

and $\mathcal{N}$ makes q_V queries and runs in $O(T_{\mathcal{B}})$ time, $\mathcal{O}$ 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, $\eta_n = 96$. We obtain:

$$\mathbf{Adv}^{N\text{–}conf}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{A}) \quad \leq \quad 2^{-55} + 2^{-50} \leq 2^{-49}$$

4 Unforgeability

Below, we first recall the result from *CryptoVerif*. For all adversaries $\mathcal{A}$:

- making q_G queries to $Gen^{\mathcal{E}(k_{src},\cdot)}(\cdot)$, q_V queries to $Verif^{\mathcal{E}^{-1}(k_{src},\cdot)}(\cdot)$, q_H queries to $\mathcal{H}(\cdot)$ in the *UF–CMVA* game, and
- running the *UF–CMVA* game in $T_{\mathcal{A}}$ time units,

there exists an adversary $\mathcal{B}$:

- making q_G queries to $\mathcal{E}(k_{src},\cdot)$ and $q_V + 1$ queries to $\mathcal{E}^{-1}(k_{src},\cdot)$ in the *INT-PTXT* game, and

- running the *INT-PTXT* game in $T_{\mathcal{B}}$ time units with $T_{\mathcal{B}} = T_{\mathcal{A}} + P_3(q_G, q_V, s)$ time units, where $P_3(q_G, q_V, s)$ is polynomial in q_G, q_V, and the message size s

such that:

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

By Theorems 4.3 in [4], there exists an $\mathcal{C}$ such that

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

and

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

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

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

and

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

Now, from Section 1, there exists adversaries $\mathcal{M}', \mathcal{N}', \mathcal{O}'$ such that

$$\begin{aligned}\mathbf{Adv}^{\mathit{PRF}}_{\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{D}) \quad \leq \quad & \mathbf{Adv}^{\mathit{RKA}}_{\texttt{comp-SHA-256}^*}(\mathcal{M}') + \mathbf{Adv}^{\mathit{PRF}}_{\texttt{comp-SHA-256}}(\mathcal{N}') + \\ & \frac{(q_V-1)q_V}{2} \times \big(8 \times \mathbf{Adv}^{\mathit{PRF}}_{\texttt{comp-SHA-256}}(\mathcal{O}') + \frac{1}{2^{256}}\big)\end{aligned}$$

and $\mathcal{M}'$ is a related key adversary that performs two oracle queries and has time $O(T_{\mathcal{B}})$, $\mathcal{N}'$ makes q_V queries and runs in $O(T_{\mathcal{B}})$ time, $\mathcal{O}'$ makes 2 queries and run in $O(T)$, T being the time for one computation of `comp-SHA-256`.

So,

$$\begin{aligned}\mathbf{Adv}^{\mathit{UF\text{–}CMVA}}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{A}) \quad \leq \quad & \mathbf{Adv}^{\mathit{RKA}}_{\texttt{comp-SHA-256}^*}(\mathcal{M}') + \mathbf{Adv}^{\mathit{PRF}}_{\texttt{comp-SHA-256}}(\mathcal{N}') + \\ & \frac{(q_V-1)q_V}{2} \times \big(8 \times \mathbf{Adv}^{\mathit{PRF}}_{\texttt{comp-SHA-256}}(\mathcal{O}') + \frac{1}{2^{256}}\big) + \frac{q_V}{2^{72}}\end{aligned}$$

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

$$\mathbf{Adv}^{\mathit{UF\text{–}CMVA}}_{\texttt{AES-CBC},\texttt{HMAC-SHA-256}_{trunc}}(\mathcal{A}) \quad \leq \quad 2^{-113} + 2^{-52} \leq 2^{-51}$$

References

[1] Bellare, M.: Symmetric encryption. `https://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf`

[2] Bellare, M.: New proofs for nmac and hmac: Security without collision-resistance (2006). URL `https://cseweb.ucsd.edu/~mihir/papers/hmac-new.html`. An extended abstract of this paper appeared in Advances in Cryptology - Crypto 2006 Proceedings, Lecture Notes in Computer Science Vol. 4117, C. Dwork ed, Springer-Verlag, 2006.

[3] Bellare, M., Kilian, J., Rogaway, P.: The security of the cipher block chaining message authentication code. J. Comput. Syst. Sci. **61**(3), 362–399 (2000). DOI 10.1006/jcss.1999.1694. URL `http://dx.doi.org/10.1006/jcss.1999.1694`

[4] Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. J. Cryptol. **21**(4), 469–491 (2008). DOI 10.1007/s00145-008-9026-x. URL `http://dx.doi.org/10.1007/s00145-008-9026-x`