Alice (Caller) **Server (WhatsApp)** **Bob (Callee)**

$\mathrm{HKDF} : (\mathit{Key}, \mathit{Info}, \mathit{Salt}, i) \rightarrow \{0,1\}^{i \times 8}$

$\mathrm{Enc}_k : (m) \rightarrow \mathrm{AES\text{-}128\text{-}ICM}_k(m)$

$\mathrm{Auth}_{ak} : (m, j) \rightarrow \mathrm{HMAC\text{-}SHA1}_{ak}(m) \in \{0,1\}^{j \times 8}$

$\mathrm{StreamInit} : (\mathit{Key}, \mathit{IV}, \mathit{Nonce}) \rightarrow \mathit{StreamContext}$

$ms \leftarrow_\$ \{0,1\}^{256}$

$id_{call} \leftarrow_\$ \{0,1\}^{256}$

$$\xrightarrow{\mathrm{Noise}(id_{call}, id_A, id_B, \mathrm{Signal}(ms))}$$

$$\xrightarrow{\mathrm{Noise}(id_{call}, id_A, id_B, \mathrm{Signal}(ms))}$$

$k_{A0}, s_{A0} \leftarrow \mathrm{HKDF}(ms, id_A, 0, 46)$ $\qquad\qquad k_{A0}, s_{A0} \leftarrow \mathrm{HKDF}(ms, id_A, 0, 46)$

$k_{A1}, s_{A1} \leftarrow ?$ $\qquad\qquad k_{A1}, s_{A1} \leftarrow ?$

$k_{A2}, s_{A2} \leftarrow ?$ $\qquad\qquad k_{A2}, s_{A2} \leftarrow ?$

$n_{A0} \leftarrow \mathrm{HKDF}(id_{call}, id_A, 0, 4)$ $\qquad\qquad n_{A0} \leftarrow \mathrm{HKDF}(id_{call}, id_A, 0, 4)$

$n_{A1} \leftarrow \mathrm{HKDF}(id_{call}, id_A, 1, 4)$ $\qquad\qquad n_{A1} \leftarrow \mathrm{HKDF}(id_{call}, id_A, 1, 4)$

$n_{A2} \leftarrow \mathrm{HKDF}(id_{call}, id_A, 4, 4)$ $\qquad\qquad n_{A2} \leftarrow \mathrm{HKDF}(id_{call}, id_A, 4, 4)$

$ak_{A0} \leftarrow ?$ $\qquad\qquad ak_{A0} \leftarrow ?$

$ak_{A1} \leftarrow ?$ $\qquad\qquad ak_{A1} \leftarrow ?$

$ak_{A2} \leftarrow ?$ $\qquad\qquad ak_{A2} \leftarrow ?$

$c_{Ai} \leftarrow \mathrm{Enc}_{k_{Ai}}(m_{Ai})$

$srtpHeader_{Ai} \leftarrow ssrc_{Ai}, seq_{Ai}, t$

$auth_{A0} \leftarrow \mathrm{Auth}_{ak_{A0}}(0, 4)$

$auth_{A1} \leftarrow \mathrm{Auth}_{ak_{A1}}(0, 4)$

$auth_{A2} \leftarrow \mathrm{Auth}_{ak_{A2}}(srtpHeader_{A2} | c_{A2}, 10)$

$stream_{Ai} \leftarrow \mathrm{StreamInit}(k_{Ai}, s_{Ai}, n_{Ai})$ $\qquad\qquad stream_{Ai} \leftarrow \mathrm{StreamInit}(k_{Ai}, s_{Ai}, n_{Ai})$

$$\xrightarrow{srtpHeader_{Ai}, c_{Ai}, auth_{Ai}}$$

$k_{B0}, s_{B0} \leftarrow \mathrm{HKDF}(ms, id_B, 0, 46)$ $\qquad\qquad k_{B0}, s_{B0} \leftarrow \mathrm{HKDF}(ms, id_B, 0, 46)$

$k_{B1}, s_{B1} \leftarrow ?$ $\qquad\qquad k_{B1}, s_{B1} \leftarrow ?$

$k_{B2}, s_{B2} \leftarrow ?$ $\qquad\qquad k_{B2}, s_{B2} \leftarrow ?$

$n_{B0} \leftarrow \mathrm{HKDF}(id_{call}, id_B, 0, 4)$ $\qquad\qquad n_{B0} \leftarrow \mathrm{HKDF}(id_{call}, id_B, 0, 4)$

$n_{B1} \leftarrow \mathrm{HKDF}(id_{call}, id_B, 1, 4)$ $\qquad\qquad n_{B1} \leftarrow \mathrm{HKDF}(id_{call}, id_B, 1, 4)$

$n_{B2} \leftarrow \mathrm{HKDF}(id_{call}, id_B, 4, 4)$ $\qquad\qquad n_{B2} \leftarrow \mathrm{HKDF}(id_{call}, id_B, 4, 4)$

$ak_{B0} \leftarrow ?$ $\qquad\qquad ak_{B0} \leftarrow ?$

$ak_{B1} \leftarrow ?$ $\qquad\qquad ak_{B1} \leftarrow ?$

$ak_{B2} \leftarrow ?$ $\qquad\qquad ak_{B2} \leftarrow ?$

$c_{Bi} \leftarrow \mathrm{Enc}_{k_{Bi}}(m_{Bi})$

$srtpHeader_{Bi} \leftarrow ssrc_{Bi}, seq_{Bi}, t$

$auth_{B0} \leftarrow \mathrm{Auth}_{ak_{B0}}(0, 4)$

$auth_{B1} \leftarrow \mathrm{Auth}_{ak_{B1}}(0, 4)$

$auth_{B2} \leftarrow \mathrm{Auth}_{ak_{B2}}(srtpHeader_{B2} | c_{B2}, 10)$

$stream_{Bi} \leftarrow \mathrm{StreamInit}(k_{Bi}, s_{Bi}, n_{Bi})$ $\qquad\qquad stream_{Bi} \leftarrow \mathrm{StreamInit}(k_{Bi}, s_{Bi}, n_{Bi})$

$$\xleftarrow{srtpHeader_{Bi}, c_{Bi}, auth_{Bi}}$$

Figure 6.1: WhatsApp VoIP Protocol