Game $\mathrm{G}^{\mathrm{ae}}_{\mathcal{A},\mathsf{SE}}$	$\underline{\textsc{Enc}(M_0, M_1, \ell, H)}$	$\underline{\textsc{Dec}(C, H)}$
$b \leftarrow\!\!\$\ \{0,1\}$	$u \leftarrow u + 1$	$v \leftarrow v + 1$
$u \leftarrow v \leftarrow 0$	$(C^0, \mathrm{st}_e^0) \leftarrow\!\!\$\ \mathsf{SE.Enc}(K, \ell, H, M_0, \mathrm{st}_e)$	If $b = 0$) then return $\perp$
$K \leftarrow\!\!\$\ \mathsf{SE.Kg}$	$(C^1, \mathrm{st}_e^1) \leftarrow\!\!\$\ \mathsf{SE.Enc}(K, \ell, H, M_1, \mathrm{st}_e)$	$(M, \mathrm{st}_d) \leftarrow \mathsf{SE.Dec}(K, H, C, \mathrm{st}_d)$
$(\mathrm{st}_e, \mathrm{st}_d) \leftarrow \mathsf{SE.Init}$	If $C^0 = \perp$ or $C^1 = \perp$ then return $\perp$	If $v > u$ or $C \neq C_v$ then $\mathsf{oos} \leftarrow \mathsf{true}$
$b' \leftarrow\!\!\$\ \mathcal{A}^{\textsc{Enc},\textsc{Dec}}$	$(C_u, \mathrm{st}_e) \leftarrow (C^b, \mathrm{st}_e^b)$	If not oos then return M
Return $b = b'$	Return C_u	Return $\perp$

Figure 1: Security game for stateful length-hiding encryption

3.1 Stateful Length-Hiding Authenticated Encryption

Syntax

- $K \leftarrow\!\!\$\ \mathsf{SE.Kg}$
- $(\mathrm{st}_e, \mathrm{st}_d) \leftarrow \mathsf{SE.Init}$
- $(C, \mathrm{st}_e) \leftarrow\!\!\$\ \mathsf{SE.Enc}(K, \ell, H, m, \mathrm{st}_e)\ //|C| = \ell$
- $(M, \mathrm{st}_d) \leftarrow\!\!\$\ \mathsf{SE.Dec}(K, H, C, \mathrm{st}_d)$

Security is defined by the game in Fig. 1 where $\mathsf{Adv}^{\mathsf{ae}}_{\mathsf{SE},\mathcal{A}} = 2\Pr[\mathrm{G}^{\mathrm{ae}}_{\mathcal{A},\mathsf{SE}}] - 1$. Correctness is defined in the expected way.

3.2 Key Exchange

Execution Environment We consider an environment where there are parties $P_1, \ldots, P_l$ each of which has corresponding keys $(\mathrm{pk}_i, \mathrm{sk}_i)$. Associated to a party P_i are sessions $\pi_i^1, \ldots, \pi_i^d$. Each π_i^s has access to the following variables.

- Secret key: sk_i
- Public keys: $\mathrm{pk}_1, \ldots, \mathrm{pk}_l$
- Acceptance state: $\Lambda_i^s \in \{\mathsf{accept}, \mathsf{reject}, \perp\}$
- Key: $K_i^s \in \{0,1\}^\kappa \cup \{\perp\}$
- Intended partner: $\Pi_i^s \in \{1, \ldots, l\}$
- Role: $\rho_i^s \in \{\mathrm{Client}, \mathrm{Server}\}$
- State: st_i^s

Additional bookkeeping is done with the following variables.

- Time: τ
- Transcripts: T_i^s
- Corruption time: ct_i
- Acceptance time: at_i^s
- Reveal time: rt_i^s
- Boolean: tested

$\underline{\textsc{Init}}$
$\tau \leftarrow 0$
$\mathsf{tested} \leftarrow \mathsf{false}$
For $i \in [l]$ do
  $(\mathrm{sk}_i, \mathrm{pk}_i) \leftarrow\!\!\$\ \mathsf{KE.Kg}$
  $\mathrm{ct}_i \leftarrow \infty$
  For $s \in [d]$ do
    $\Lambda_i^s \leftarrow K_i^s \leftarrow \Pi_i^s \leftarrow \rho_i^s \leftarrow \mathrm{st}_i^s \leftarrow \perp$
    $\mathrm{at}_i^s \leftarrow \mathrm{rt}_i^s \leftarrow \infty$
$\mathbf{pk} \leftarrow (\mathrm{pk}_1, \ldots, \mathrm{pk}_l)$

$\underline{\textsc{Send}(i, s, m)}$ $\tau \leftarrow \tau + 1$
If $\rho_i^s = \perp$ then
  If $m = \top$ then $\rho_i^s \leftarrow$ Client
  Else $\rho_i^s \leftarrow$ Server
$(m', \Lambda_i^s, K_i^s, \Pi_i^s, \mathrm{st}_i^s) \leftarrow\!\!\$\ \mathsf{KE}(\mathrm{sk}_i, \mathbf{pk}, \Lambda_i^s, K_i^s, \Pi_i^s, \mathrm{st}_i^s)$
$T_i^s \leftarrow T_i^s || m || m'$
Return m'

$\underline{\textsc{Reveal}(i, s)}$
$\tau \leftarrow \tau + 1$
$\mathrm{rt}_i^s \leftarrow \min\{\mathrm{rt}_i^s, \tau\}$
Return K_i^s

$\underline{\textsc{Corrupt}(i)}$
$\tau \leftarrow \tau + 1$
$\mathrm{ct}_i \leftarrow \min\{\mathrm{ct}_i, \tau\}$
Return sk_i

$\underline{\textsc{Test}(i, s)}$
$\tau \leftarrow \tau + 1$
If $\Lambda_i^s \neq \mathsf{accept}$ or tested then return $\perp$
$K_0 \leftarrow\!\!\$\ \{0,1\}^\kappa$
$K_1 \leftarrow K_i^s$
$\mathsf{tested} \leftarrow \mathsf{true}$
Return K_b

Game $\mathrm{G}^{\mathrm{corr}}_{\mathsf{KE}}$ $\textsc{Init}$
$m \leftarrow \top$
Loop
  $m \leftarrow \textsc{Send}(1, 1, m)$
  $m \leftarrow \textsc{Send}(2, 1, m)$
Return $\Lambda_1^1 = \Lambda_2^1 = \mathsf{accept}$
and $K_1^1 = K_2^1$

Game $\mathrm{G}^{\mathrm{auth}}_{\mathsf{KE},\mathcal{A}}$
$\textsc{Init}$
$\mathcal{A}^{\textsc{Send},\textsc{Reveal},\textsc{Corrupt},\textsc{Test}}$
$\mathsf{win} \leftarrow \mathsf{false}$
For all (i, s) do
  $\mathsf{win} \leftarrow \mathsf{true}$ if:
    $\Lambda_i^s = \mathsf{accept}$
    $\mathrm{at}_i^s < \mathrm{ct}_{\Pi_i^s}$
    Not $\mathsf{MATCH}(i, s, j, t)$ for exactly one $(j, t) \neq (i, s)$
Return win

$\mathsf{MATCH}(i, s, j, t)$
Return $(T_j^t \neq \perp$ and $T_j^t \sqsubset T_i^s)$
or $T_i^s = T_j^t$

Game $\mathrm{G}^{\mathrm{ke}}_{\mathsf{KE},\mathcal{A}}$
$\textsc{Init}$
$b' \leftarrow\!\!\$\ \mathcal{A}^{\textsc{Send},\textsc{Reveal},\textsc{Corrupt},\textsc{Test}}$
$(i, s) \leftarrow (i^*, s^*)$ If $\Lambda_i^s \neq \mathsf{accept}$ then return false
If $\mathrm{rt}_i^s \neq \infty$ then return false
If $\exists (j, t)$ s.t. $\mathsf{MATCH}(i, s, j, t)$ and $\mathrm{rt}_j^t \neq \infty$
  Return false
If $\mathrm{ct}_{\Pi_i^s} < \mathrm{at}_i^s$ then return false
Return $b = b'$

Figure 2: **Left:** Key exchange security environment. **Right:** KE security games and matching condition.

Correctness and security games are defined in Fig. 2. Correctness requires $\Pr[\mathrm{G}^{\mathrm{corr}}_{\mathsf{KE}}] = 1$. Authentication security advantage is given by $\mathsf{Adv}^{\mathsf{auth}}_{\mathsf{KE},\mathcal{A}} = \Pr[\mathrm{G}^{\mathrm{auth}}_{\mathcal{A},\mathsf{KE}}]$. Key privacy is given by $\mathsf{Adv}^{\mathsf{ke}}_{\mathsf{KE},\mathcal{A}} = 2\Pr[\mathrm{G}^{\mathrm{ke}}_{\mathcal{A},\mathsf{KE}}] - 1$.

$\underline{\text{INIT}}$
Same as before except for all (i, s):
$u_i^s \leftarrow v_i^s \leftarrow 0$
$b_i^s \leftarrow\!\!\$\ \{0,1\}$
$\mathsf{oos}_i^s \leftarrow \mathsf{false}$

$\underline{\text{Game } \mathrm{G}^{\mathrm{auth}}_{\mathsf{KE},\mathsf{SE},\mathcal{A}}}$
Same as before except also return false
if queried REVEAL to (i, s) or matching (j, t)

$\underline{\mathsf{MATCH}(i, s, j, t)}$
Return ($T_j^t \neq \perp$ and $T_j^t \sqsubset T_i^s$)
or $T_i^s = T_j^t$

$\underline{\text{Game } \mathrm{G}^{\mathrm{lr}}_{\mathsf{KE},\mathsf{SE},\mathcal{A}}}$
$\underline{\text{INIT}}$
$(i, s, b)\mathcal{A}^{\text{SEND,REVEAL,CORRUPT,ENC,DEC,TEST}}$
If $\Lambda_i^s \neq \mathsf{accept}$ then return false
If $\mathrm{rt}_i^s \neq \infty$ then return false
If $\exists (j, t)$ s.t. $\mathsf{MATCH}(i, s, j, t)$
  and $\mathrm{rt}_j^t \neq \infty$ then return false
If $\mathrm{ct}_{\Pi_i^s} < \mathrm{at}_i^s$ then return false
Return $b = b_i^s$

$\underline{\text{ENC}(M_0, M_1, \ell, H)}$
$u_i^s \leftarrow u_i^s + 1$
$(C^0, \mathrm{st}_e^0) \leftarrow\!\!\$\ \mathsf{SE.Enc}(K, \ell, H, M_0, \mathrm{st}_e)$
$(C^1, \mathrm{st}_e^1) \leftarrow\!\!\$\ \mathsf{SE.Enc}(K, \ell, H, M_1, \mathrm{st}_e)$
If $C^0 = \perp$ or $C^1 = \perp$ then return $\perp$
$(C_{u_i^s}, \mathrm{st}_e) \leftarrow (C^{b_i^s}, \mathrm{st}_e^{b_i^s})$
Return $C_{u_i^s}$

$\underline{\text{DEC}(C, H)}$
$v_i^s \leftarrow v_i^s + 1$
If $b = 0$ then return $\perp$
$(M, \mathrm{st}_d) \leftarrow \mathsf{SE.Dec}(K, H, C, \mathrm{st}_d)$
Let (j, t) minimize $\mathsf{MATCH}(i, s, j, t)$
If $v_i^s > u_j^t$ or $C \neq C_{v_j^t}$ then $\mathsf{oos}_i^s \leftarrow \mathsf{true}$
If not oos_i^s then return M
Return $\perp$

Figure 3: ACCE extension.