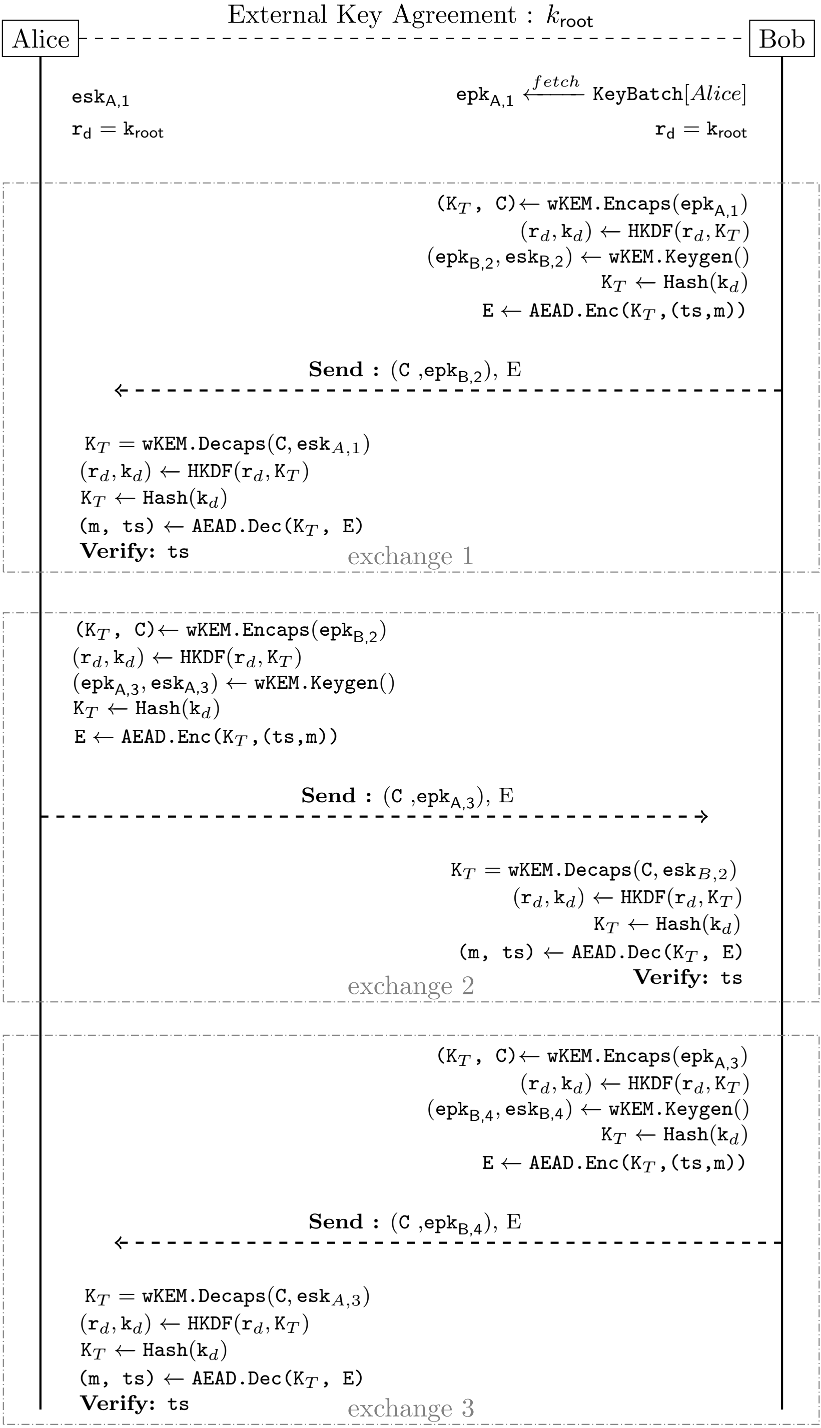

External Key Agreement : k_{root}

$\mathtt{esk}_{\mathsf{A,1}}$

$\mathtt{r}_{\mathsf{d}} = \mathtt{k}_{\mathsf{root}}$

$\mathtt{epk}_{\mathsf{A,1}} \xleftarrow{fetch} \mathtt{KeyBatch}[Alice]$

$\mathtt{r}_{\mathsf{d}} = \mathtt{k}_{\mathsf{root}}$

$(\mathtt{K}_T\mathtt{,\ C}) \leftarrow \mathtt{wKEM.Encaps}(\mathtt{epk}_{\mathsf{A,1}})$

$(\mathtt{r}_d, \mathtt{k}_d) \leftarrow \mathtt{HKDF}(\mathtt{r}_d, \mathtt{K}_T)$

$(\mathtt{epk}_{\mathsf{B,2}}, \mathtt{esk}_{\mathsf{B,2}}) \leftarrow \mathtt{wKEM.Keygen}()$

$\mathtt{K}_T \leftarrow \mathtt{Hash}(\mathtt{k}_d)$

$\mathtt{E} \leftarrow \mathtt{AEAD.Enc(K}_T\mathtt{,(ts,m))}$

Send : ($\mathtt{C}$,$\mathtt{epk}_{\mathsf{B,2}}$), E

$\mathtt{K}_T = \mathtt{wKEM.Decaps}(\mathtt{C}, \mathtt{esk}_{A,1})$

$(\mathtt{r}_d, \mathtt{k}_d) \leftarrow \mathtt{HKDF}(\mathtt{r}_d, \mathtt{K}_T)$

$\mathtt{K}_T \leftarrow \mathtt{Hash}(\mathtt{k}_d)$

$\mathtt{(m,\ ts)} \leftarrow \mathtt{AEAD.Dec(K}_T\mathtt{,\ E)}$

Verify: $\mathtt{ts}$

$(\mathtt{K}_T\mathtt{,\ C}) \leftarrow \mathtt{wKEM.Encaps}(\mathtt{epk}_{\mathsf{B,2}})$

$(\mathtt{r}_d, \mathtt{k}_d) \leftarrow \mathtt{HKDF}(\mathtt{r}_d, \mathtt{K}_T)$

$(\mathtt{epk}_{\mathsf{A,3}}, \mathtt{esk}_{\mathsf{A,3}}) \leftarrow \mathtt{wKEM.Keygen}()$

$\mathtt{K}_T \leftarrow \mathtt{Hash}(\mathtt{k}_d)$

$\mathtt{E} \leftarrow \mathtt{AEAD.Enc(K}_T\mathtt{,(ts,m))}$

Send : ($\mathtt{C}$,$\mathtt{epk}_{\mathsf{A,3}}$), E

$\mathtt{K}_T = \mathtt{wKEM.Decaps}(\mathtt{C}, \mathtt{esk}_{B,2})$

$(\mathtt{r}_d, \mathtt{k}_d) \leftarrow \mathtt{HKDF}(\mathtt{r}_d, \mathtt{K}_T)$

$\mathtt{K}_T \leftarrow \mathtt{Hash}(\mathtt{k}_d)$

$\mathtt{(m,\ ts)} \leftarrow \mathtt{AEAD.Dec(K}_T\mathtt{,\ E)}$

Verify: $\mathtt{ts}$

$(\mathtt{K}_T\mathtt{,\ C}) \leftarrow \mathtt{wKEM.Encaps}(\mathtt{epk}_{\mathsf{A,3}})$

$(\mathtt{r}_d, \mathtt{k}_d) \leftarrow \mathtt{HKDF}(\mathtt{r}_d, \mathtt{K}_T)$

$(\mathtt{epk}_{\mathsf{B,4}}, \mathtt{esk}_{\mathsf{B,4}}) \leftarrow \mathtt{wKEM.Keygen}()$

$\mathtt{K}_T \leftarrow \mathtt{Hash}(\mathtt{k}_d)$

$\mathtt{E} \leftarrow \mathtt{AEAD.Enc(K}_T\mathtt{,(ts,m))}$

Send : ($\mathtt{C}$,$\mathtt{epk}_{\mathsf{B,4}}$), E

$\mathtt{K}_T = \mathtt{wKEM.Decaps}(\mathtt{C}, \mathtt{esk}_{A,3})$

$(\mathtt{r}_d, \mathtt{k}_d) \leftarrow \mathtt{HKDF}(\mathtt{r}_d, \mathtt{K}_T)$

$\mathtt{K}_T \leftarrow \mathtt{Hash}(\mathtt{k}_d)$

$\mathtt{(m,\ ts)} \leftarrow \mathtt{AEAD.Dec(K}_T\mathtt{,\ E)}$

Verify: $\mathtt{ts}$