Software Engineering
at the
University of Oxford

SSL Message Exchange.

Msg. 1 $C \to S$: n_c, id, cs, cm.

Msg. 2 $S \to C$: n_s, id, cs', cm'.

Msg. 3 $S \to C$: $pk(s)$

Msg. 4

Msg. 5 $C \to S$: $\{k\}_{pk(s)}$

Msg. 6

Msg. 7

⋮

Msg. n $C \to S$: $\{d_n\}_k$
$S \to C$: $\{d_m\}_k$

<u>MODIFICATION</u>

Msg. 3 : $S \to C$: S, $pk(S)$, $\{h(S, pk(S))\}_{sk(CA)}$ ~~$pk(CA)$~~