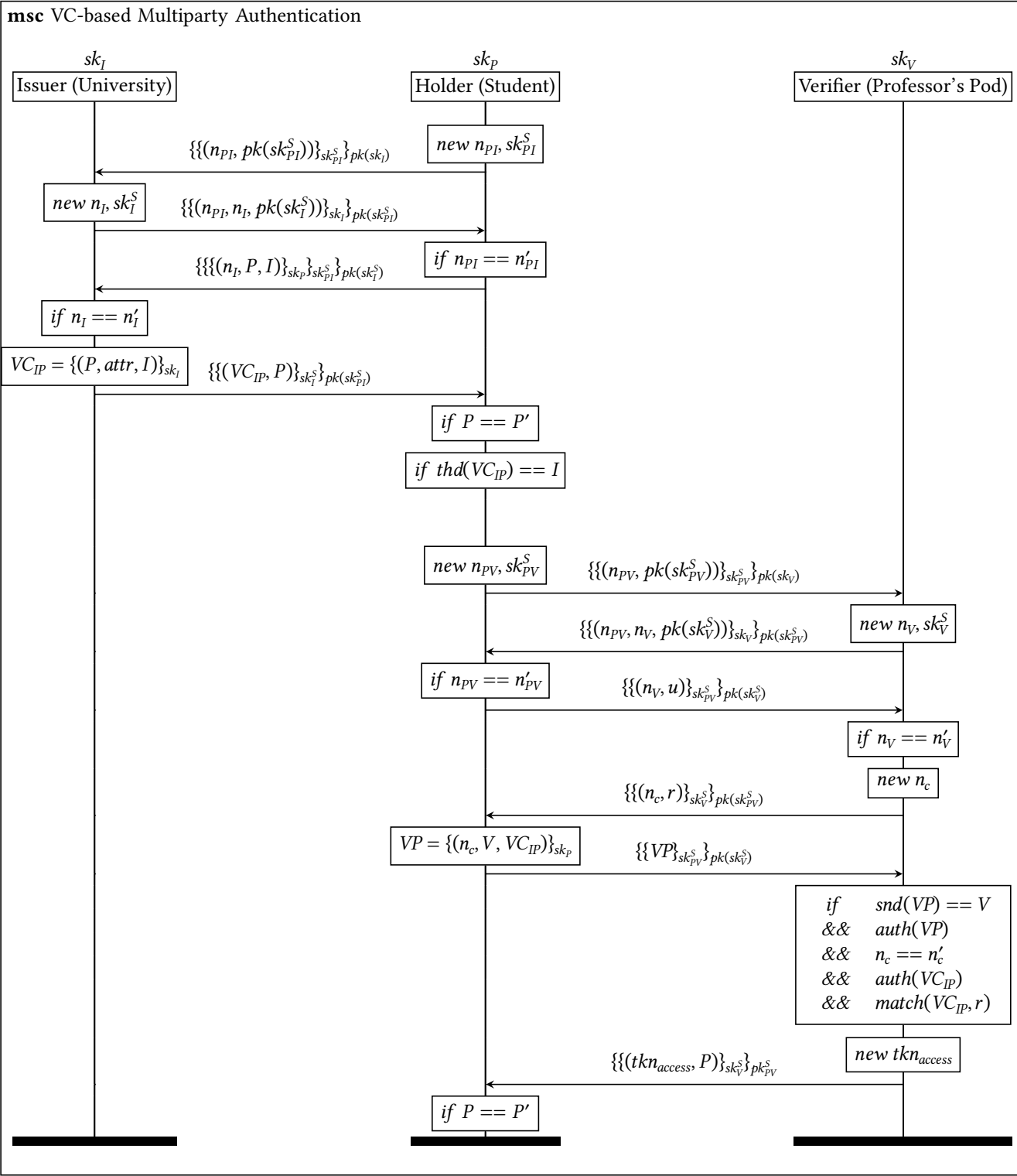
msc VC-based Multiparty Authentication
sk_I
Issuer (University)
sk_P
Holder (Student)
sk_V
Verifier (Professor's Pod)
new n_{PI}, sk^S_{PI}
$\{\{(n_{PI}, pk(sk^S_{PI}))\}_{sk^S_{PI}}\}_{pk(sk_I)}$
new n_I, sk^S_I
$\{\{(n_{PI}, n_I, pk(sk^S_I))\}_{sk_I}\}_{pk(sk^S_{PI})}$
if $n_{PI} == n'_{PI}$
$\{\{\{(n_I, P, I)\}_{sk_P}\}_{sk^S_{PI}}\}_{pk(sk^S_I)}$
if $n_I == n'_I$
$VC_{IP} = \{(P, attr, I)\}_{sk_I}$
$\{\{(VC_{IP}, P)\}_{sk^S_I}\}_{pk(sk^S_{PI})}$
if $P == P'$
if $thd(VC_{IP}) == I$
new n_{PV}, sk^S_{PV}
$\{\{(n_{PV}, pk(sk^S_{PV}))\}_{sk^S_{PV}}\}_{pk(sk_V)}$
new n_V, sk^S_V
$\{\{(n_{PV}, n_V, pk(sk^S_V))\}_{sk_V}\}_{pk(sk^S_{PV})}$
if $n_{PV} == n'_{PV}$
$\{\{(n_V, u)\}_{sk^S_{PV}}\}_{pk(sk^S_V)}$
if $n_V == n'_V$
new n_c
$\{\{(n_c, r)\}_{sk^S_V}\}_{pk(sk^S_{PV})}$
$VP = \{(n_c, V, VC_{IP})\}_{sk_P}$
$\{\{VP\}_{sk^S_{PV}}\}_{pk(sk^S_V)}$
if $snd(VP) == V$
&& $auth(VP)$
&& $n_c == n'_c$
&& $auth(VC_{IP})$
&& $match(VC_{IP}, r)$
new tkn_{access}
$\{\{(tkn_{access}, P)\}_{sk^S_V}\}_{pk^S_{PV}}$
if $P == P'$