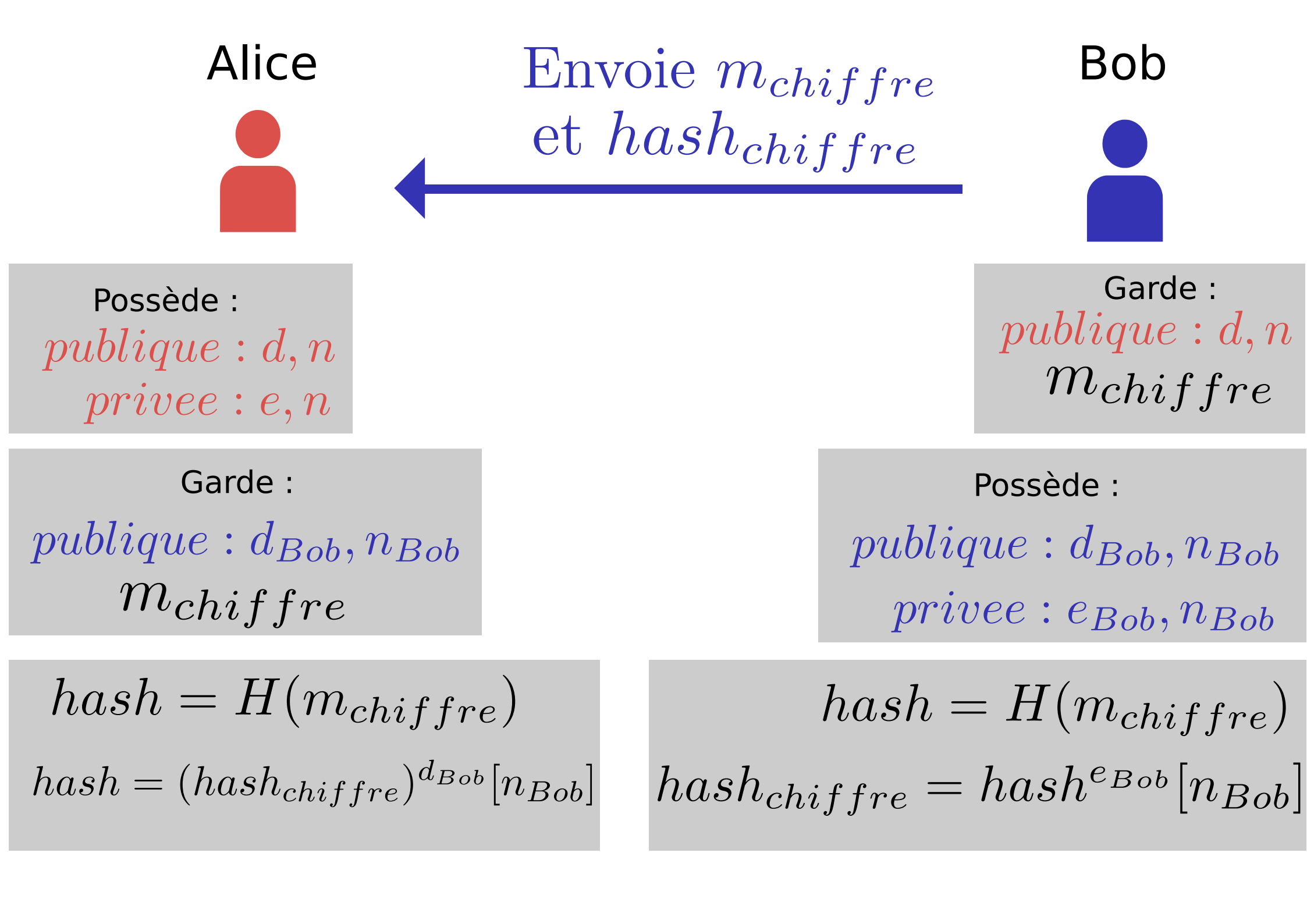
Alice
Envoie $m_{chiffre}$ et $hash_{chiffre}$
Bob
Possède :
$publique : d, n$
$privee : e, n$
Garde :
$publique : d, n$
$m_{chiffre}$
Garde :
$publique : d_{Bob}, n_{Bob}$
$m_{chiffre}$
Possède :
$publique : d_{Bob}, n_{Bob}$
$privee : e_{Bob}, n_{Bob}$
$hash = H(m_{chiffre})$
$hash = (hash_{chiffre})^{d_{Bob}}[n_{Bob}]$
$hash = H(m_{chiffre})$
$hash_{chiffre} = hash^{e_{Bob}}[n_{Bob}]$