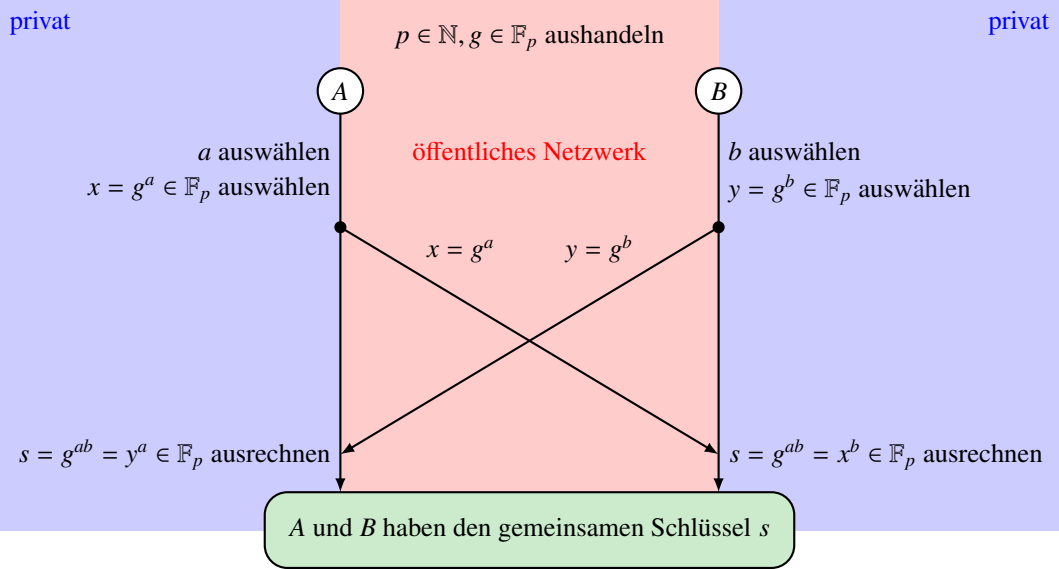
privat
privat
$p \in \mathbb{N}, g \in \mathbb{F}_p$ aushandeln
A
B
a auswählen
$x = g^a \in \mathbb{F}_p$ auswählen
öffentliches Netzwerk
b auswählen
$y = g^b \in \mathbb{F}_p$ auswählen
$x = g^a$
$y = g^b$
$s = g^{ab} = y^a \in \mathbb{F}_p$ ausrechnen
$s = g^{ab} = x^b \in \mathbb{F}_p$ ausrechnen
A und B haben den gemeinsamen Schlüssel s