

# EC - Diffie-Hellman (ECDH)

Alice  $E, p, G$  Bob

$a \in [2, |E|-1]$   
geheim

$b \in [2, |E|-1]$   
geheim

$a \cdot G$

$b \cdot G$

$a \cdot (b \cdot G)$

$b \cdot (a \cdot G)$

$= (a \cdot b) \cdot G$

$(a \cdot b) \cdot G$

x-Koordinate

ist gemeinsamer  
geheimer Schlüssel