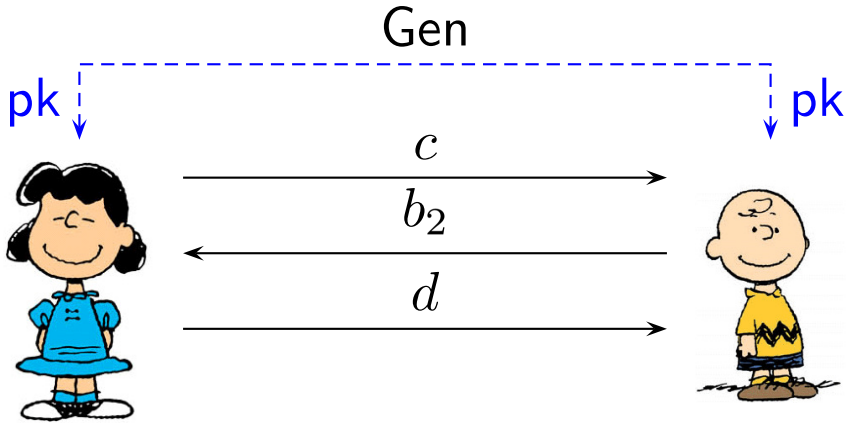
$b_1 \xleftarrow{u} \{0,1\}$

$(c,d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(b_1)$

return $b_1 \oplus b_2$




$b_2 \xleftarrow{u} \{0,1\}$

$b_1 \leftarrow \mathsf{Open}_{\mathsf{pk}}(c,d)$

return $b_1 \oplus b_2$