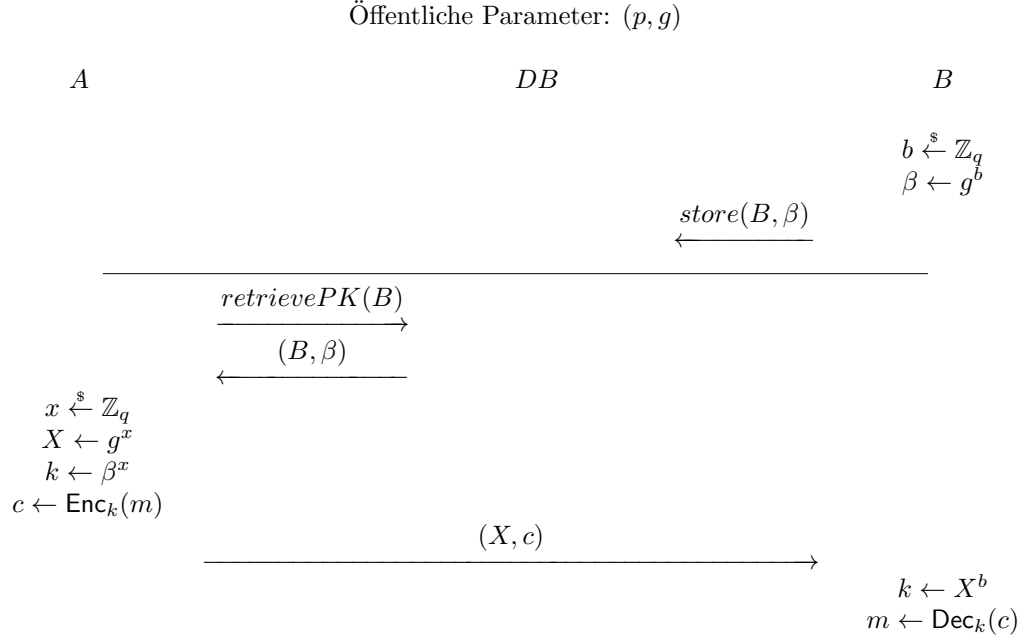
Öffentliche Parameter: (p, g)
A
DB
B
$b \xleftarrow{\$} \mathbb{Z}_q$
$\beta \leftarrow g^b$
$store(B, \beta)$
$retrievePK(B)$
(B, β)
$x \xleftarrow{\$} \mathbb{Z}_q$
$X \leftarrow g^x$
$k \leftarrow \beta^x$
$c \leftarrow \mathsf{Enc}_k(m)$
(X, c)
$k \leftarrow X^b$
$m \leftarrow \mathsf{Dec}_k(c)$