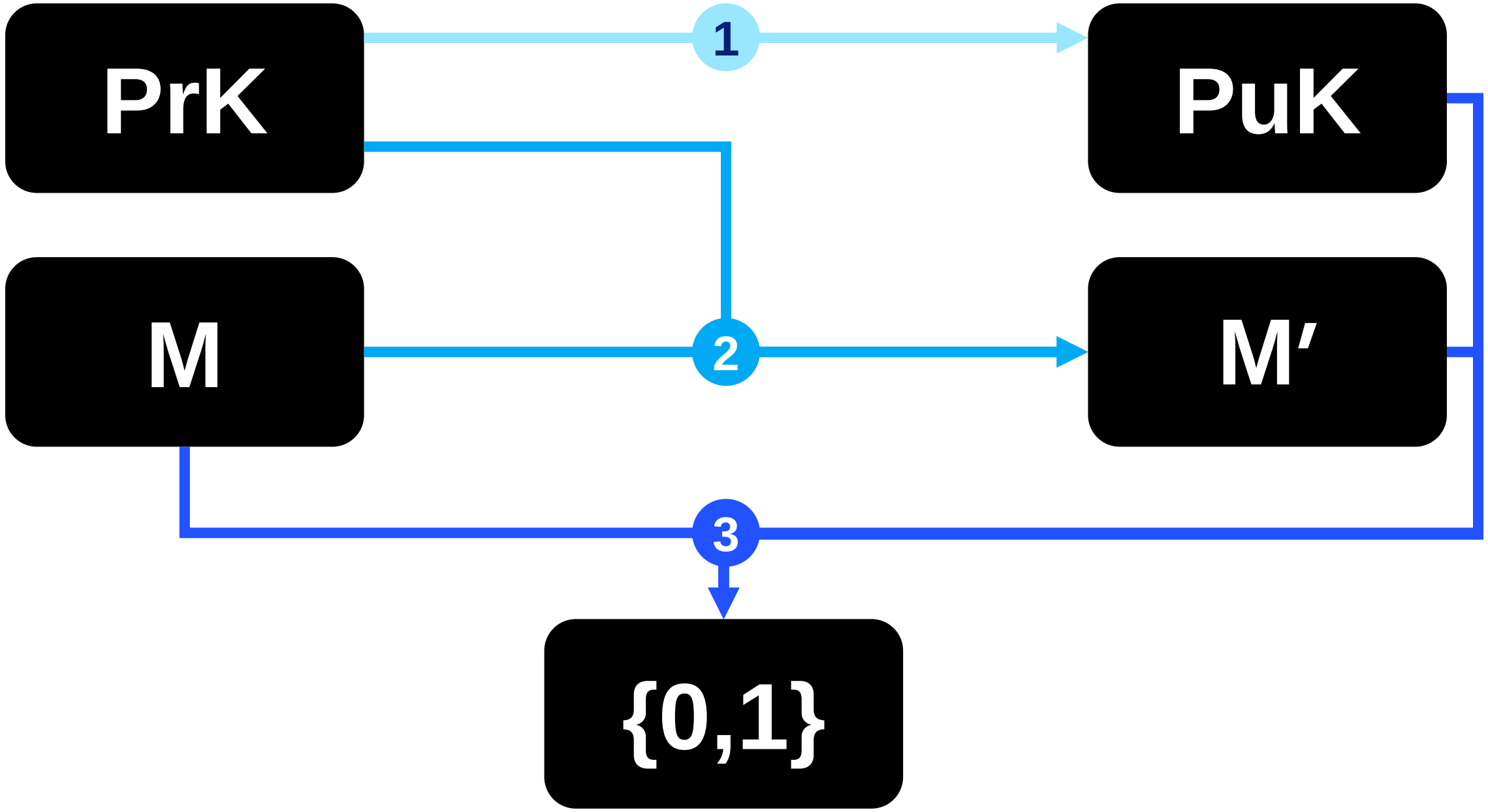
PrK
1
PuK
M
2
M′
3
{0,1}