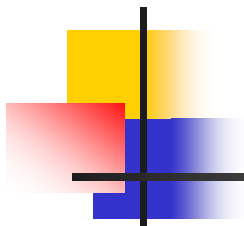




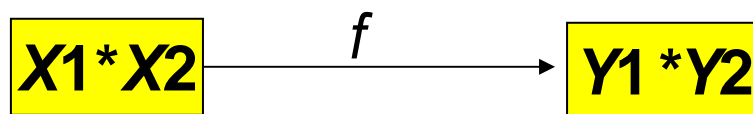
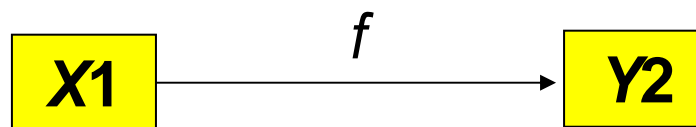
# Appendix

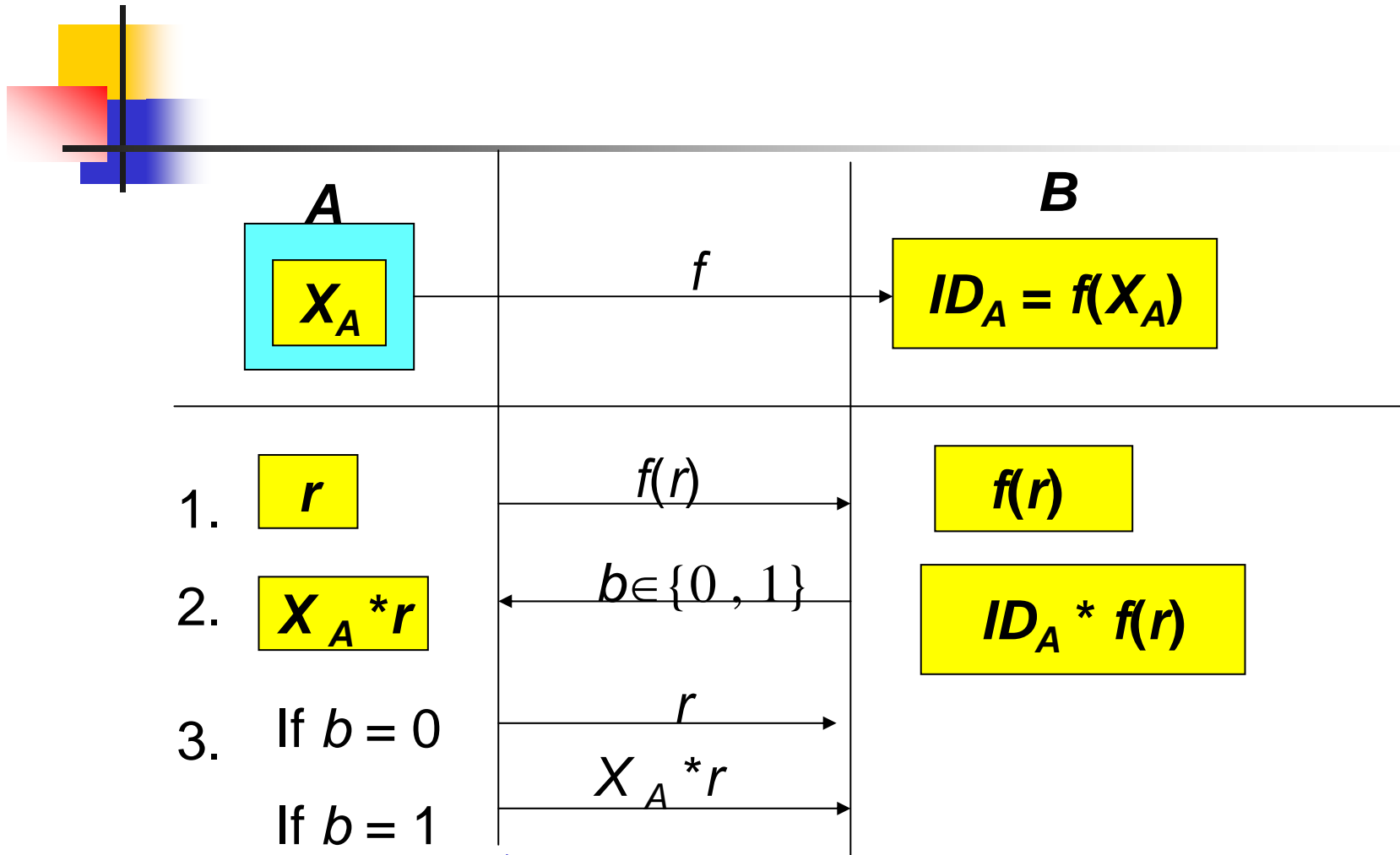
## 零資訊交換証明法 (zkIP)

邱錫彥 老師



假設某一個單向函數  $f$  具有下列特性：





知道 $X_A$ 可以每次通過測試。  
若不知道 $X_A$ 則祇有 $1/2$ 之機會通過測試。