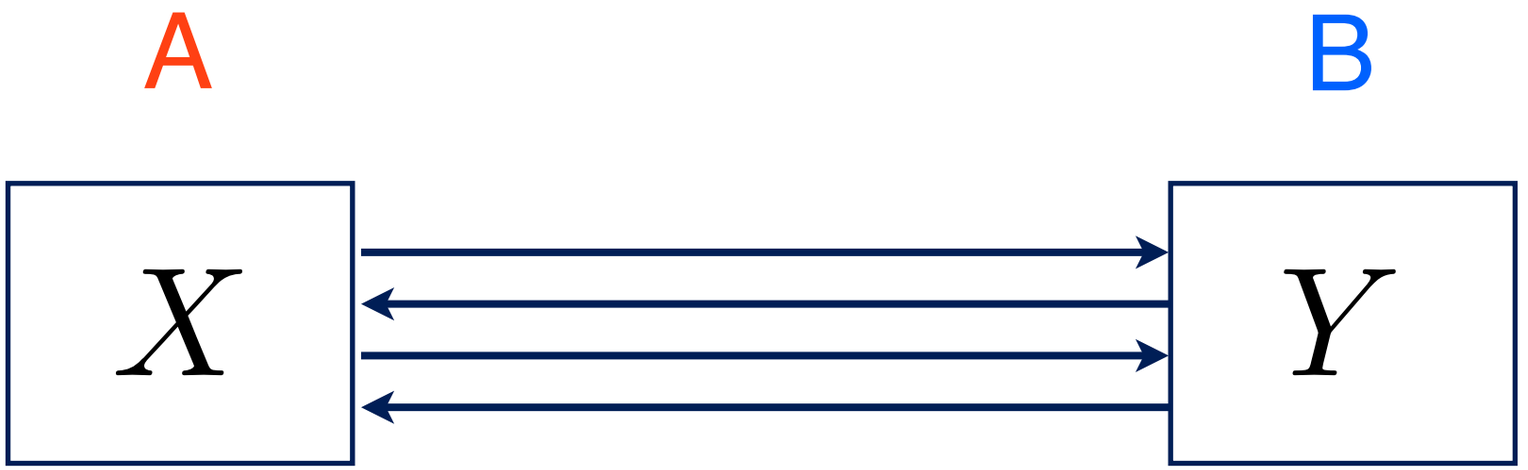
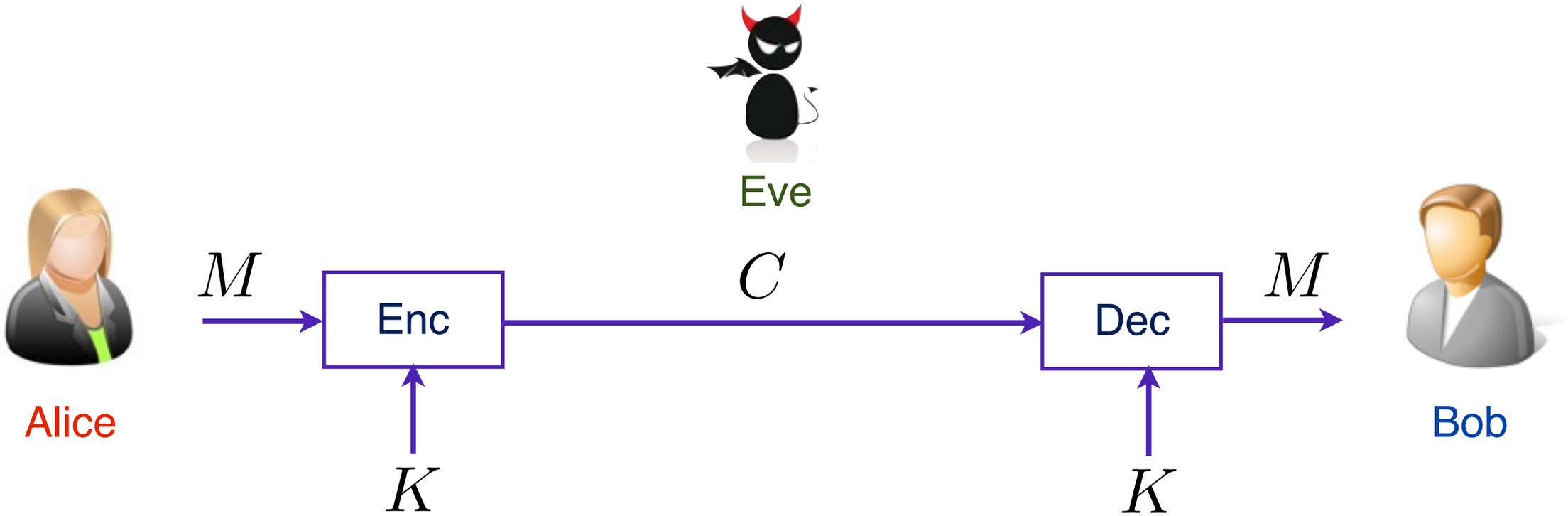



$f(X, Y)$

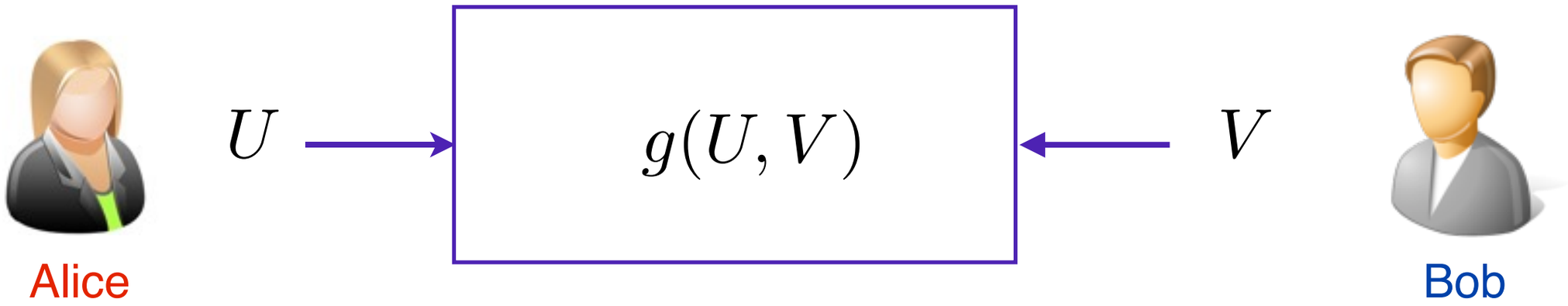
$$\mathrm{H}(\mathrm{X}) = \sum_{\mathrm{x}} \mathrm{p}(\mathrm{x}) \log \frac{1}{\mathrm{p}(\mathrm{x})}$$

# 秘密通信と鍵共有(Key Agreement)




- 現代暗号では暗号化アルゴリズム等は公開
- 秘密通信の問題は鍵共有に帰着される

# 秘匿計算 (Secure Computing)




Millionaire Problem:

$U$ :Aliceの財産

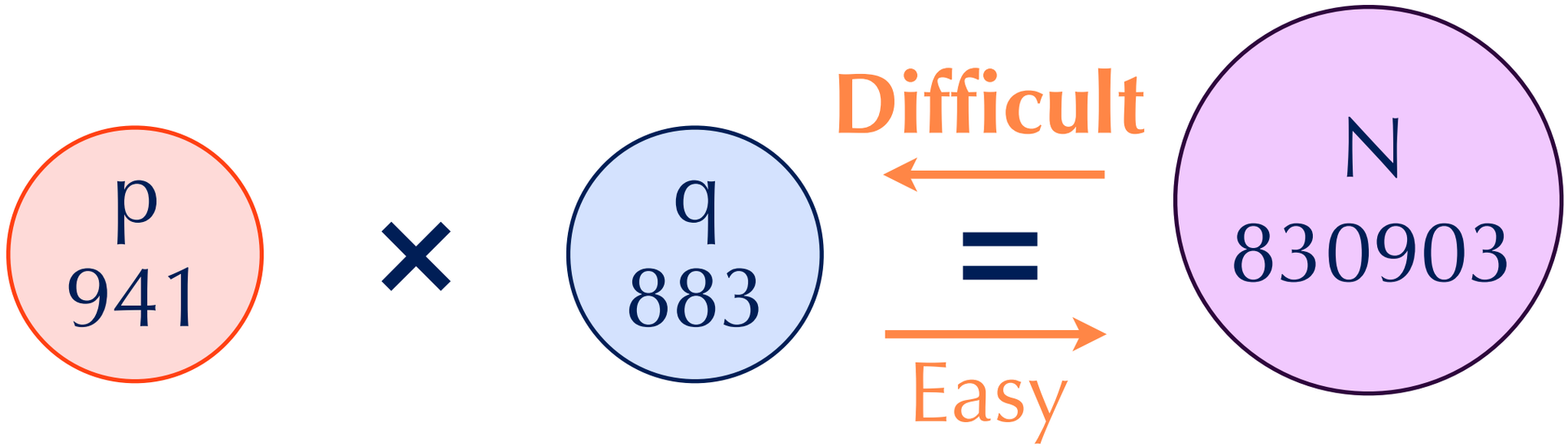
$V$ :Bobの財産

$g$ :大小比較

仲介者を介さずにダブルオークション等を実現

# 安全性の種類

- 計算量的安全性




- 情報理論的安全性