• **Claim.** Security of scheme $S_1$ under definition $D_1$ implies security of scheme $S_2$ under definition $D_2$.

• **Eq. claim.** Insecurity of scheme $S_2$ under definition $D_2$ implies insecurity of scheme $S_1$ under definition $D_1$.

• **Eq. claim.** The existence of an efficient adversary $A$ attacking scheme $S_2$ under definition $D_2$ with “not small” $d_2$-advantage implies the existence of an efficient adversary $B$ attacking scheme $S_1$ under definition $D_1$ with “not small” $d_1$-advantage.

• To prove the claim:
  • (1) Construct $B$ that uses $A$ as a subroutine. $D_1$ and $D_2$ define what “games” the adversaries play, including what oracles are they given. $B$ has to simulate the required inputs for $A$.
  • (2) Analyze $d_1$-advantage of $B$ based on $d_2$-advantage of $A$.
  • (3) Argue $B$’s efficiency based on $A$’s efficiency.