# OAEP Improvements

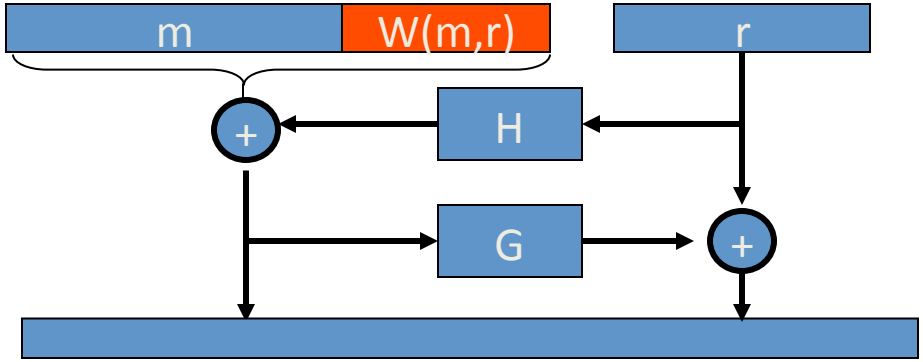
**OAEP+**: [Shoup'01]

∀ trap-door permutation F

F-OAEP+ is CCA secure when

H,G,W are *random oracles*.

During decryption validate W(m,r) field.




**SAEP+**: [B'01]

RSA (e=3) is a trap-door perm ⇒

RSA-SAEP+ is CCA secure when

H,W are *random oracle*.