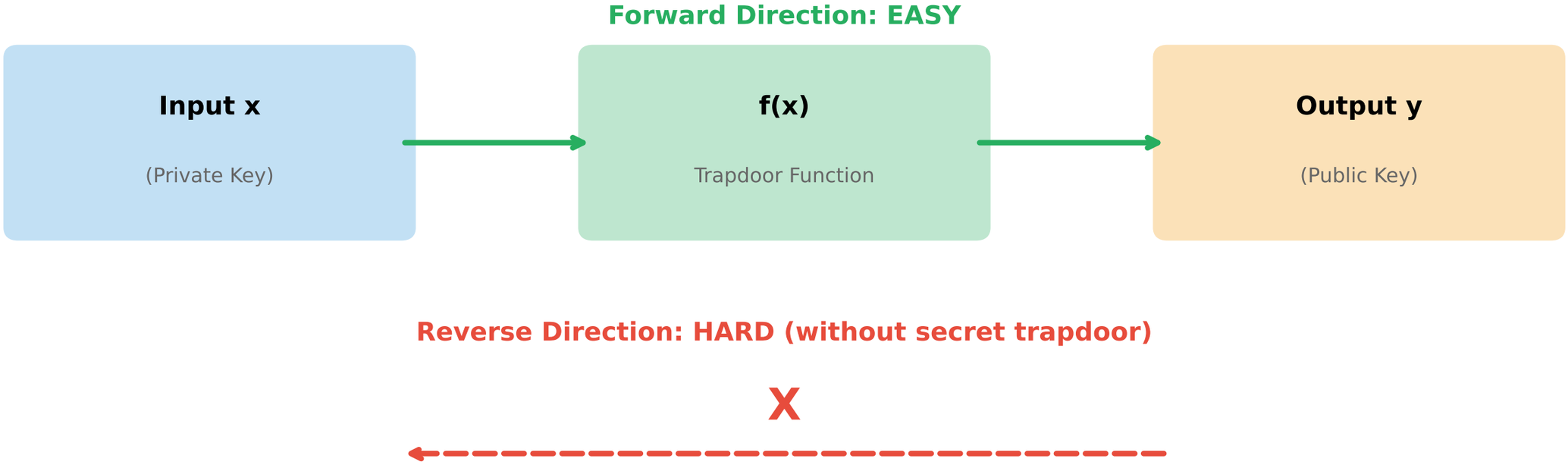
Trapdoor Functions: The Foundation of Public Key Crypto



Common Trapdoor Functions in Cryptography

Multiplication	ECC	Discrete Log
Easy: 17 x 23 = 391	Easy: K = k * G	Easy: g^x mod p
Hard: Factor 391 = ?	Hard: Find k from K	Hard: Find x from g^x

Trapdoor = Secret info (private key) that makes reverse computation easy

Source: Diffie & Hellman, "New Directions in Cryptography" (1976)