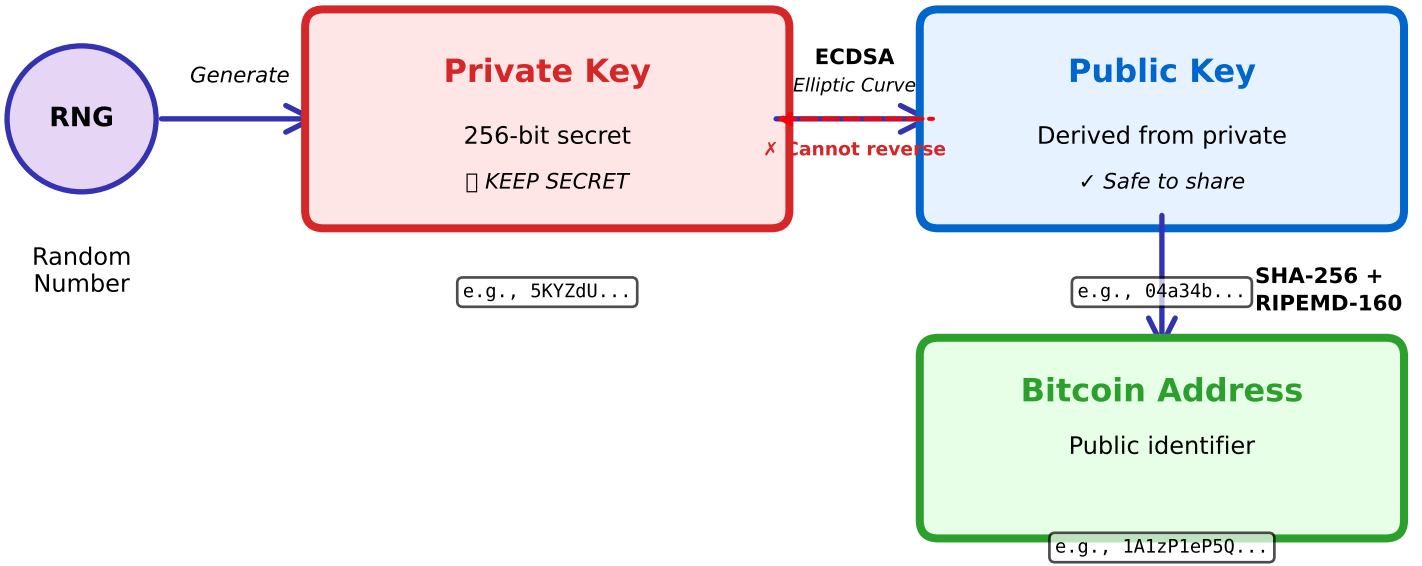
Public-Private Key Derivation

Cryptographic key hierarchy in Bitcoin



Security Properties:
- Private key must remain secret
- Public key can be freely shared
- Cannot derive private from public
- One private key → One public key

Use Cases:
- Private key: Sign transactions
- Public key: Verify signatures
- Address: Receive Bitcoin