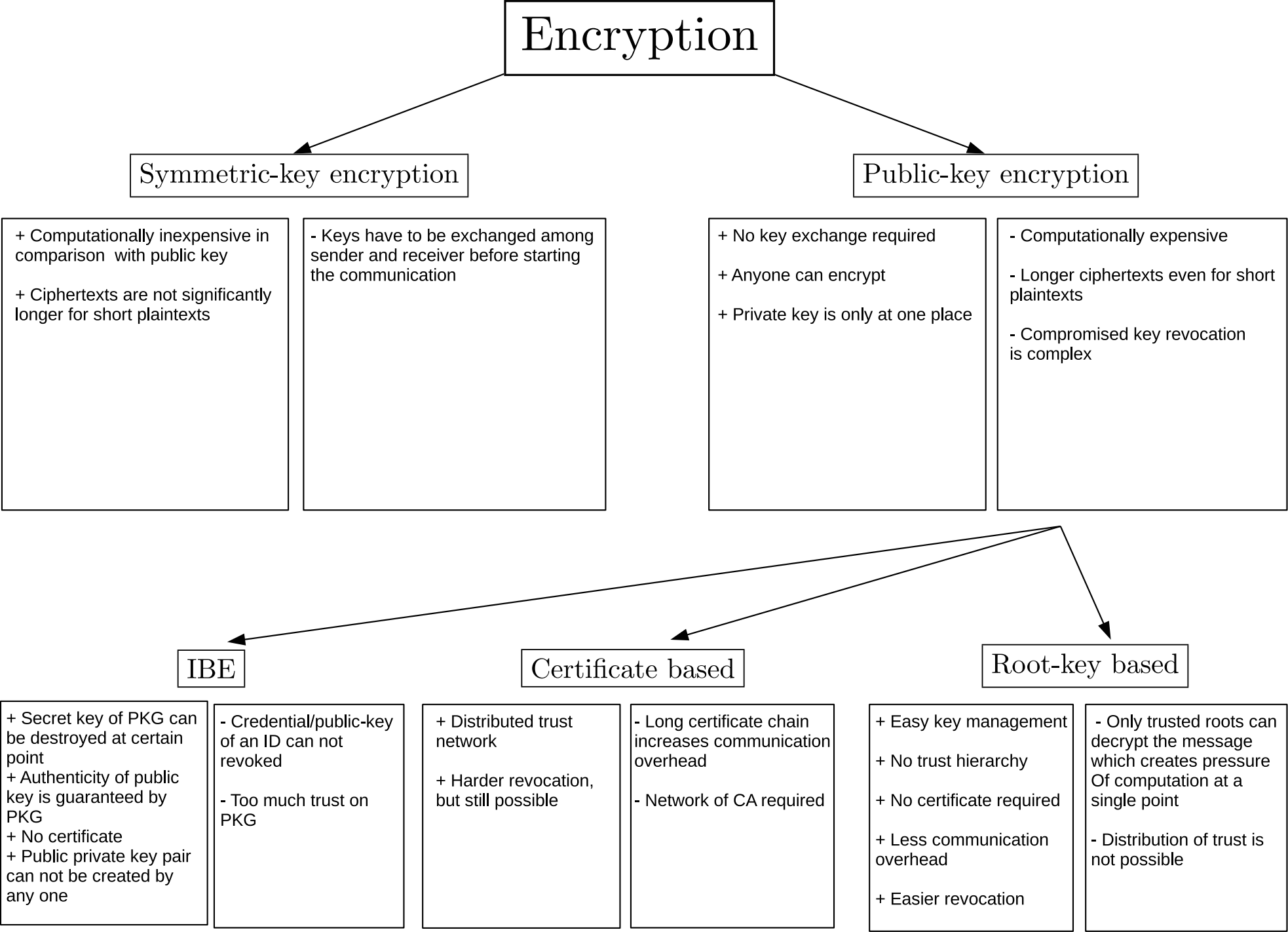
Encryption
Symmetric-key encryption
Public-key encryption
+ Computationally inexpensive in comparison with public key
+ Ciphertexts are not significantly longer for short plaintexts
- Keys have to be exchanged among sender and receiver before starting the communication
+ No key exchange required
+ Anyone can encrypt
+ Private key is only at one place
- Computationally expensive
- Longer ciphertexts even for short plaintexts
- Compromised key revocation is complex
IBE
Certificate based
Root-key based
+ Secret key of PKG can be destroyed at certain point
+ Authenticity of public key is guaranteed by PKG
+ No certificate
+ Public private key pair can not be created by any one
- Credential/public-key of an ID can not revoked
- Too much trust on PKG
+ Distributed trust network
+ Harder revocation, but still possible
- Long certificate chain increases communication overhead
- Network of CA required
+ Easy key management
+ No trust hierarchy
+ No certificate required
+ Less communication overhead
+ Easier revocation
- Only trusted roots can decrypt the message which creates pressure Of computation at a single point
- Distribution of trust is not possible