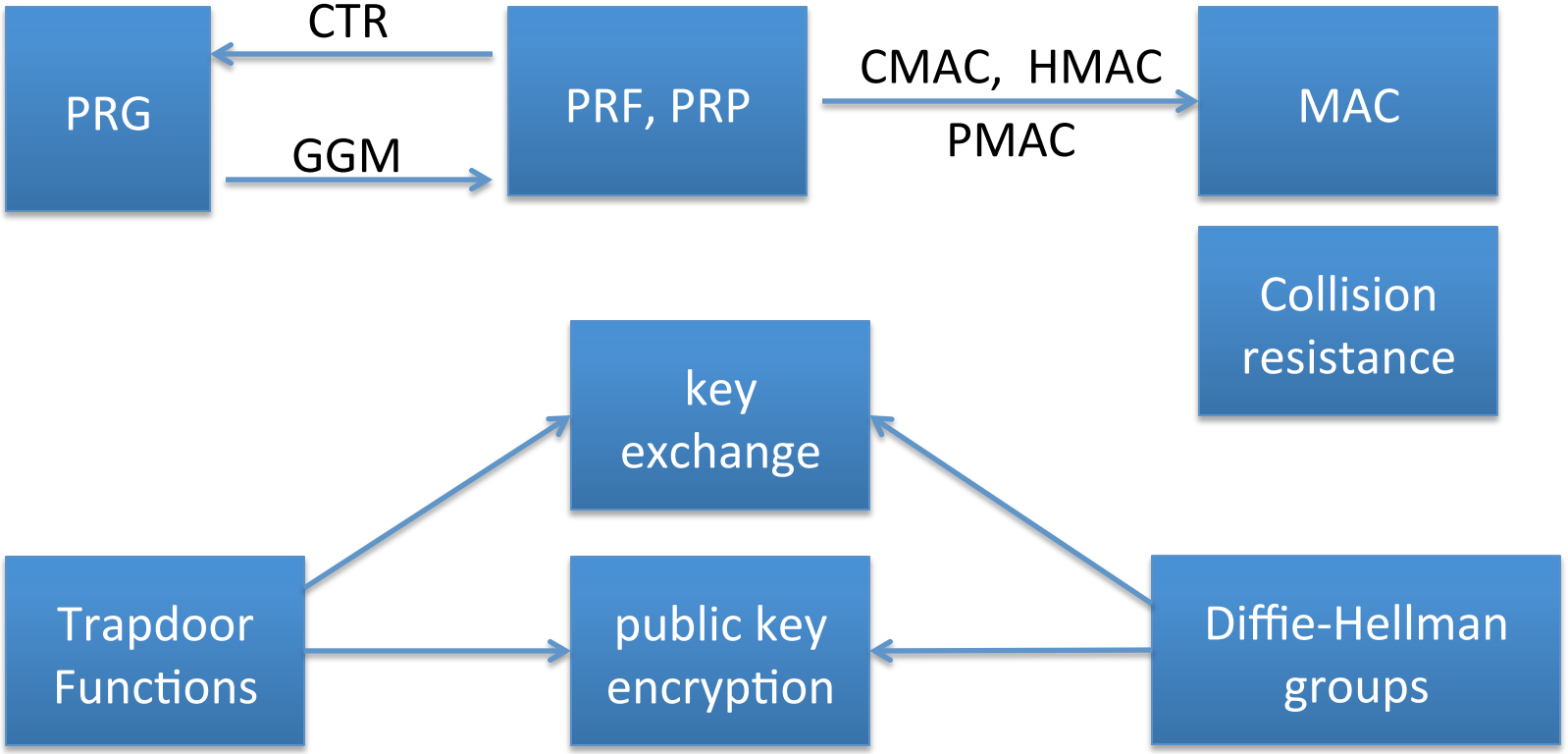
Farewell (for now)

Quick Review: primitives



Quick Review: primitives

To protect non-secret data: (data integrity)

- using small read-only storage: use collision resistant hash
- without: use MAC … requires secret key

To protect sensitive data: only use authenticated encryption

(eavesdropping security by itself is insufficient)

Session setup:

- Interactive settings: use authenticated key-exchange protocol
- When no-interaction allowed: use public-key encryption

Remaining Core Topics (part II)

- Digital signatures and certificates
- Authenticated key exchange
- User authentication:

  passwords, one-time passwords, challenge-response

- Privacy mechanisms
- Zero-knowledge protocols

Many more topics to cover …

- Elliptic Curve Crypto
- Quantum computing
- New key management paradigms:

  identity based encryption and functional encryption
- Anonymous digital cash
- Private voting and auction systems
- Computing on ciphertexts: fully homomorphic encryption
- Lattice-based crypto
- Two party and multi-party computation

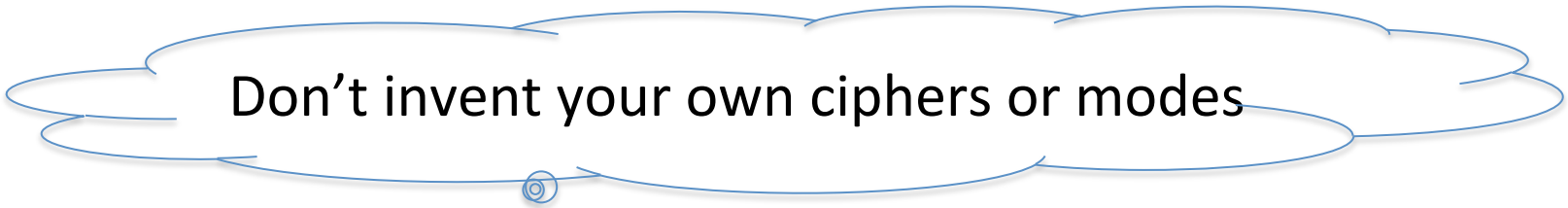
Final Words

Be careful when using crypto:

- A tremendous tool, but if incorrectly implemented:

  products will work, but may be easily attacked

Make sure to have others review your designs and code



End of part I