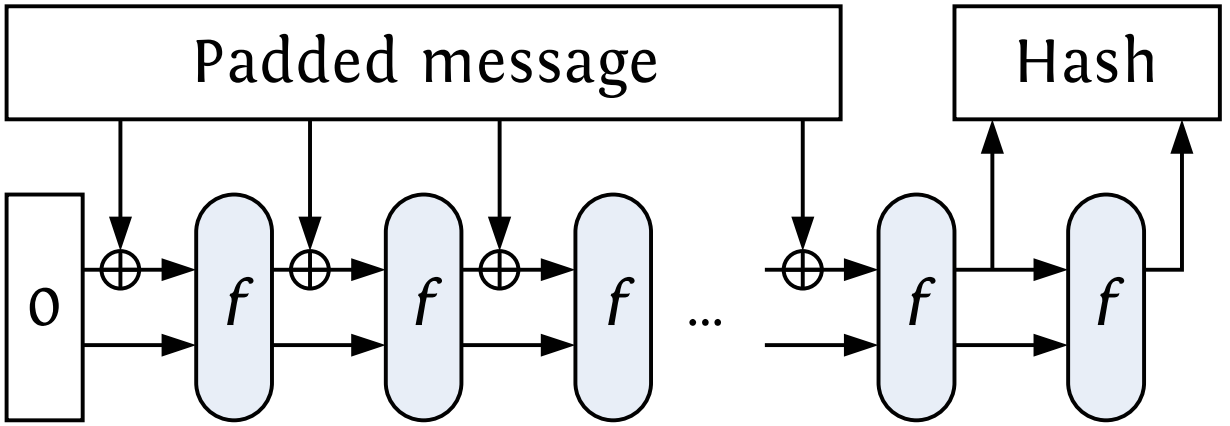
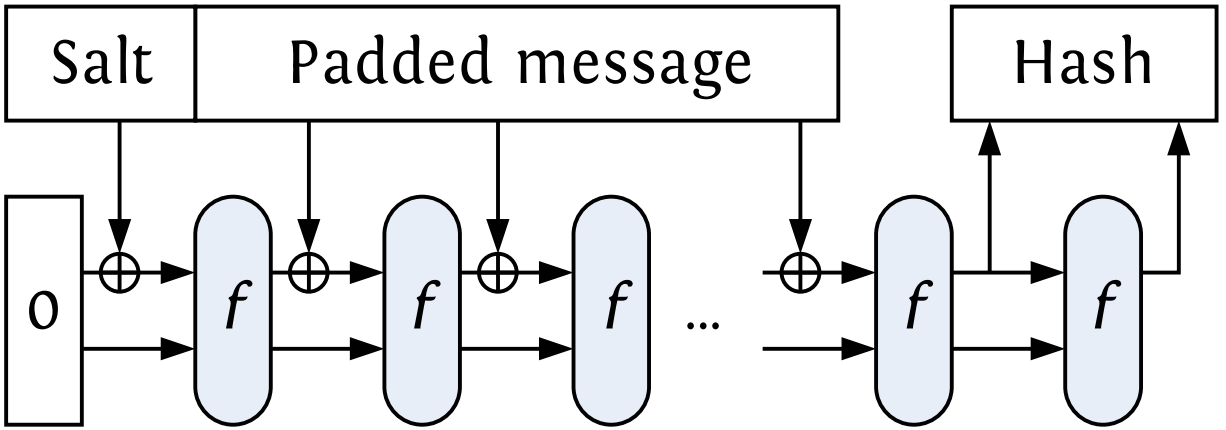
Regular hashing



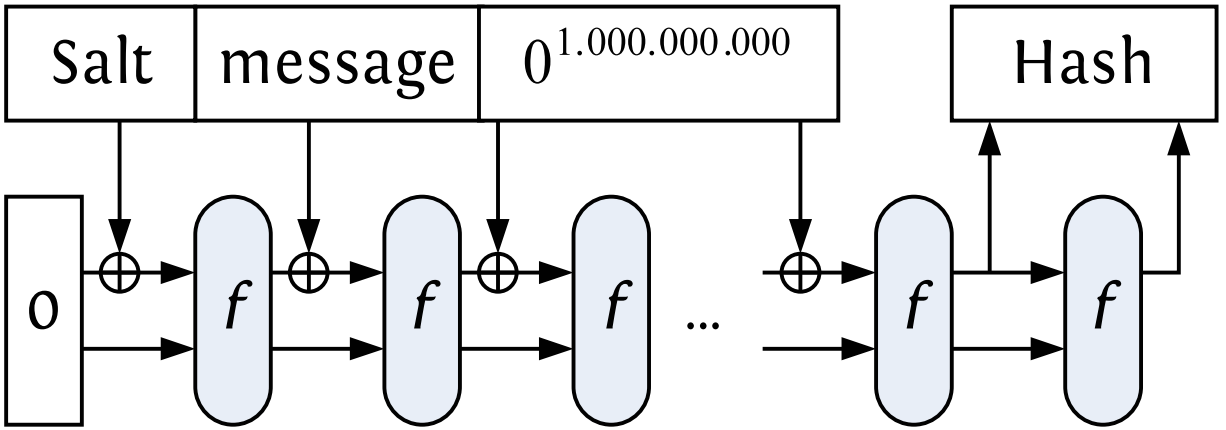
- Electronic signatures
- Data integrity (*shaXsum* ...)
- Data identifier (*Git, online anti-virus, peer-2-peer* ...)

Salted hashing



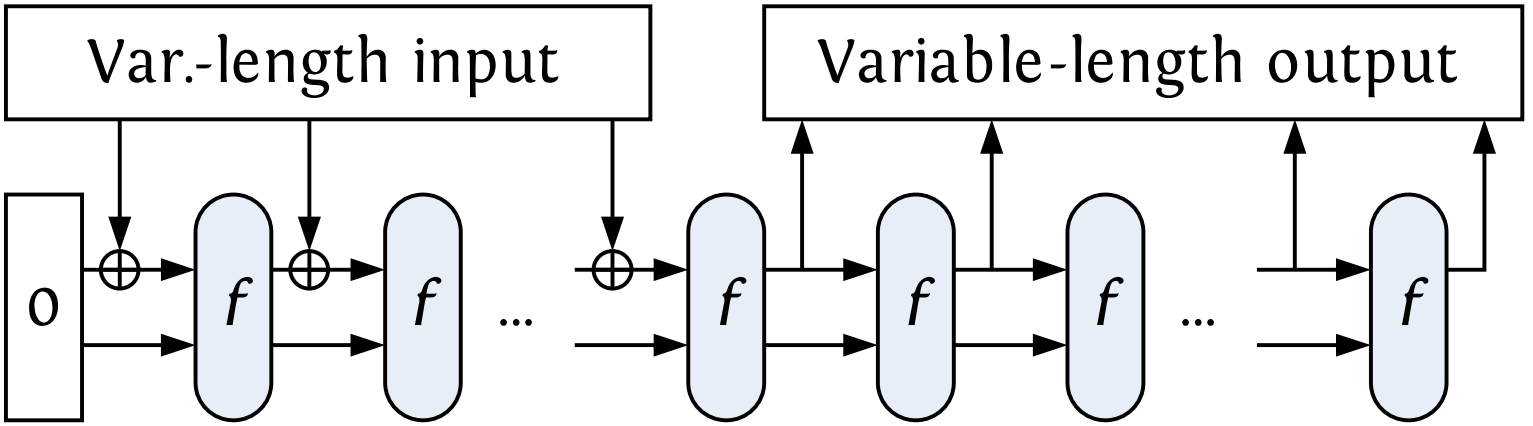
- Randomized hashing (RSASSA-PSS)
- Password storage and verification (*Kerberos*, /etc/shadow)

Salted hashing



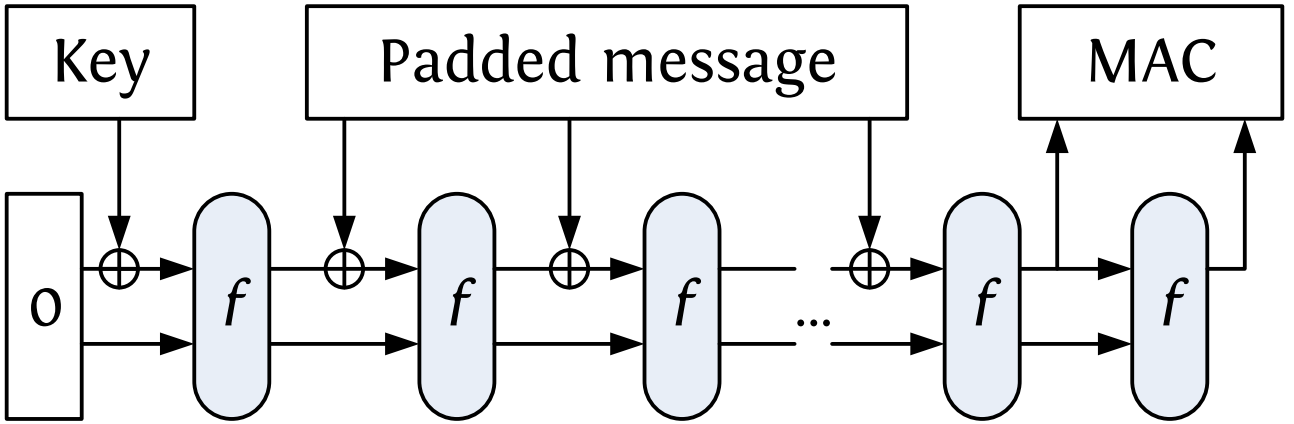
- Randomized hashing (RSASSA-PSS)
- Password storage and verification (*Kerberos*, /etc/shadow)
  - ...Can be as slow as you like it!

Mask generation function



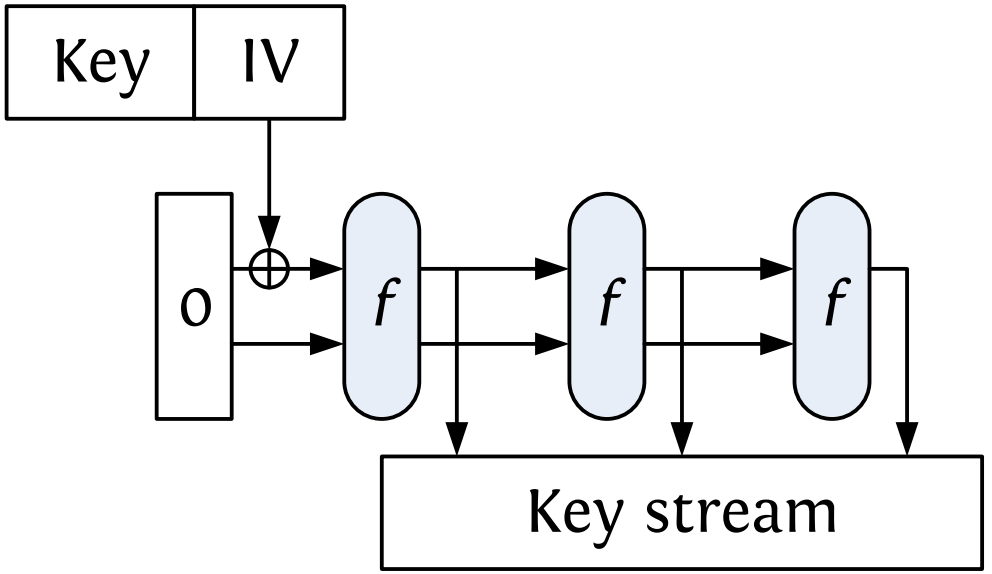
- Key derivation function in SSL, TLS
- Full-domain hashing in public key cryptography
  - electronic signatures RSASSA-PSS [PKCS#1]
  - encryption RSAES-OAEP [PKCS#1]
  - key encapsulation methods (KEM)

Message authentication codes



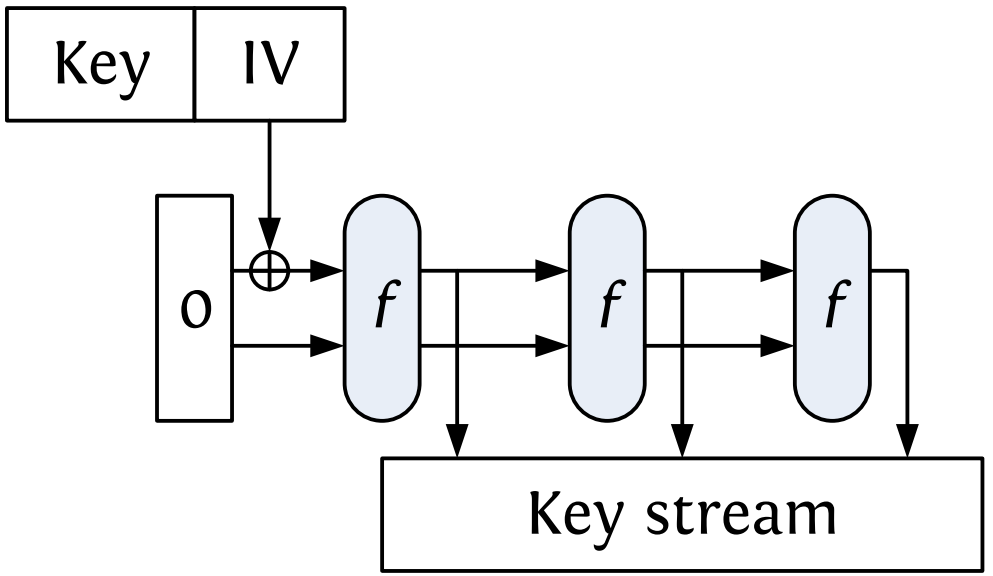
- As a message authentication code
- Simpler than HMAC [FIPS 198]
  - Required for SHA-1, SHA-2 due to length extension property
  - No longer needed for sponge

Stream encryption



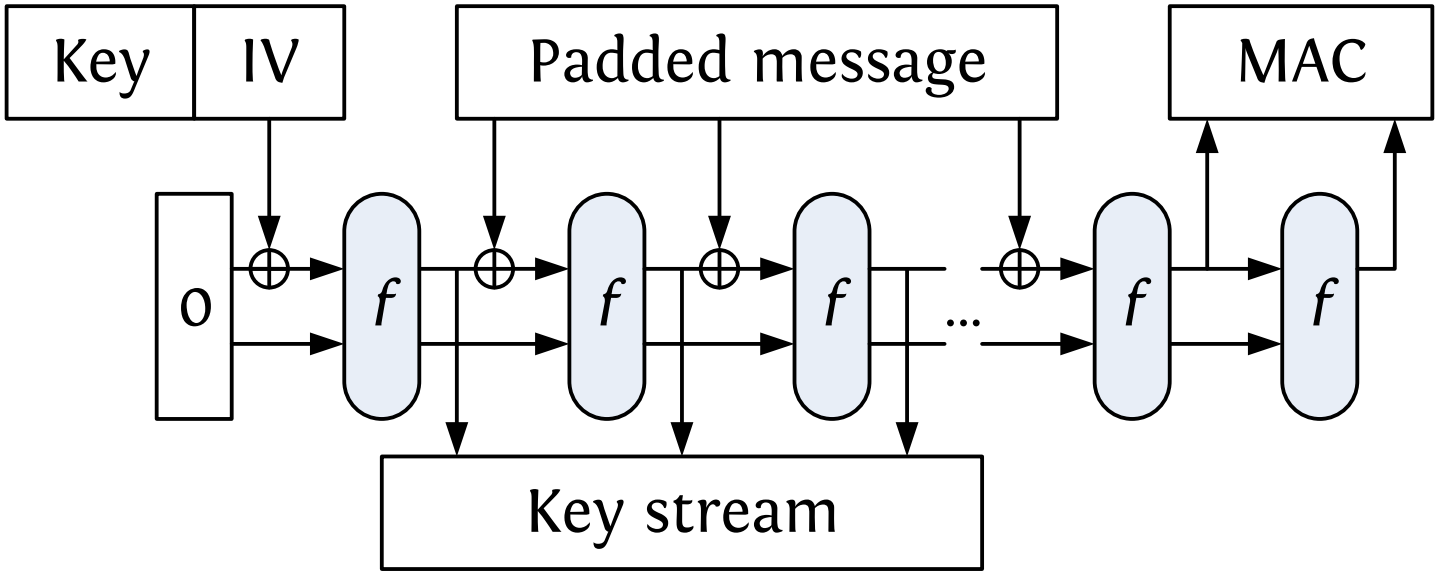
- As a stream cipher
  - Long output stream per IV: similar to OFB mode
  - Short output stream per IV: similar to counter mode

Use Sponge for (stream) encryption



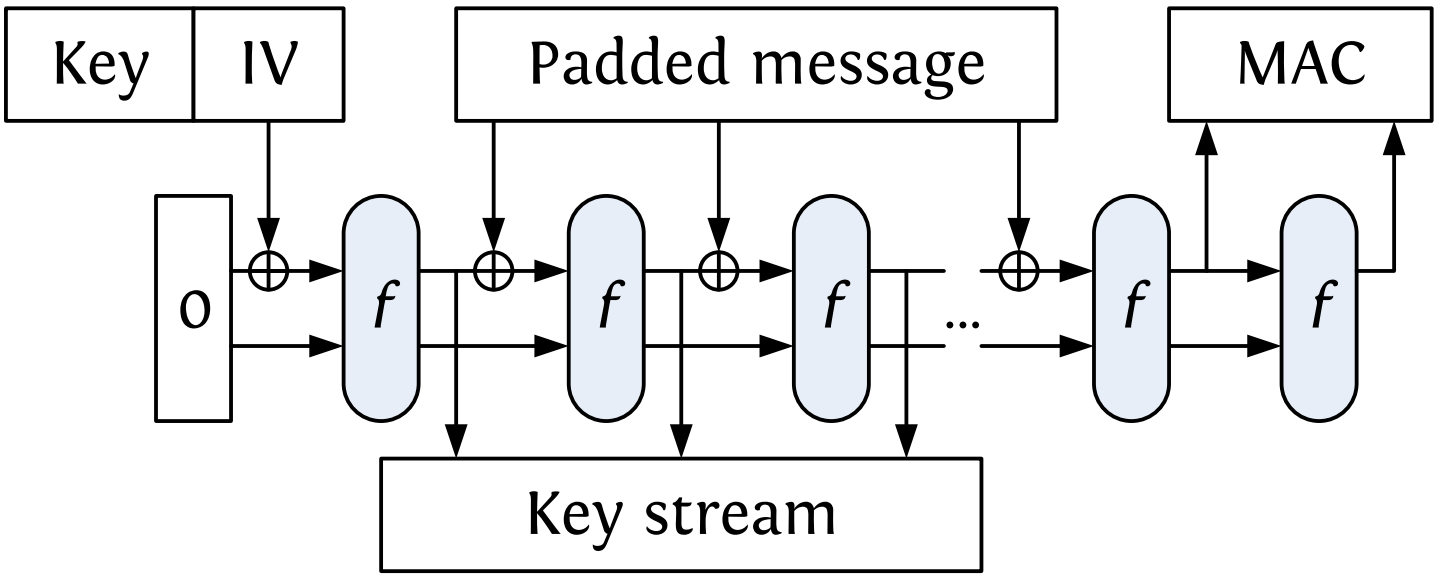
- Similar to block cipher modes:
  - Long keystream per IV: like OFB
  - Short keystream per IV: like counter mode
- Independent permutation-based stream ciphers: Salsa and ChaCha [Bernstein 2005]

Single pass authenticated encryption



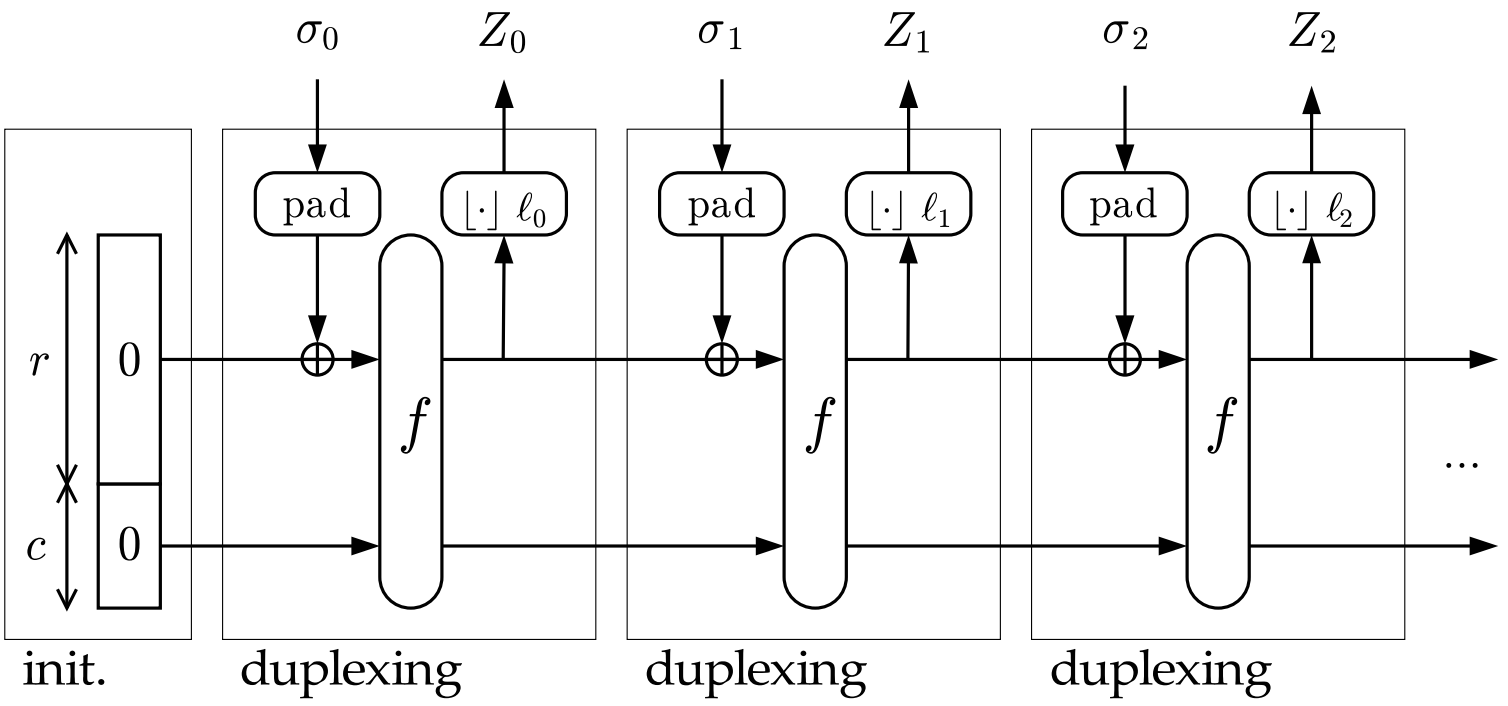
- Authentication and encryption in a single pass!
- Secure messaging (*SSL/TLS, SSH, IPSEC* ...)

Single pass authenticated encryption



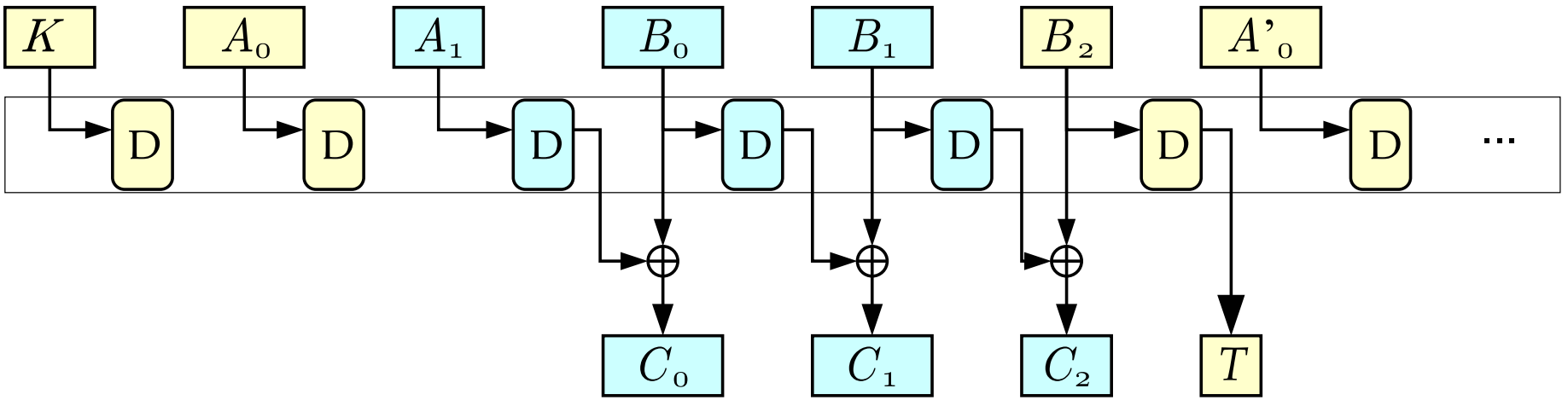
- But this is no longer the sponge ...

The duplex construction



- Generic security equivalent to Sponge [Keccak Team, SAC 2011]
- Applications include:
  - Authenticated encryption: spongeWrap
  - Reseedable pseudorandom sequence generator

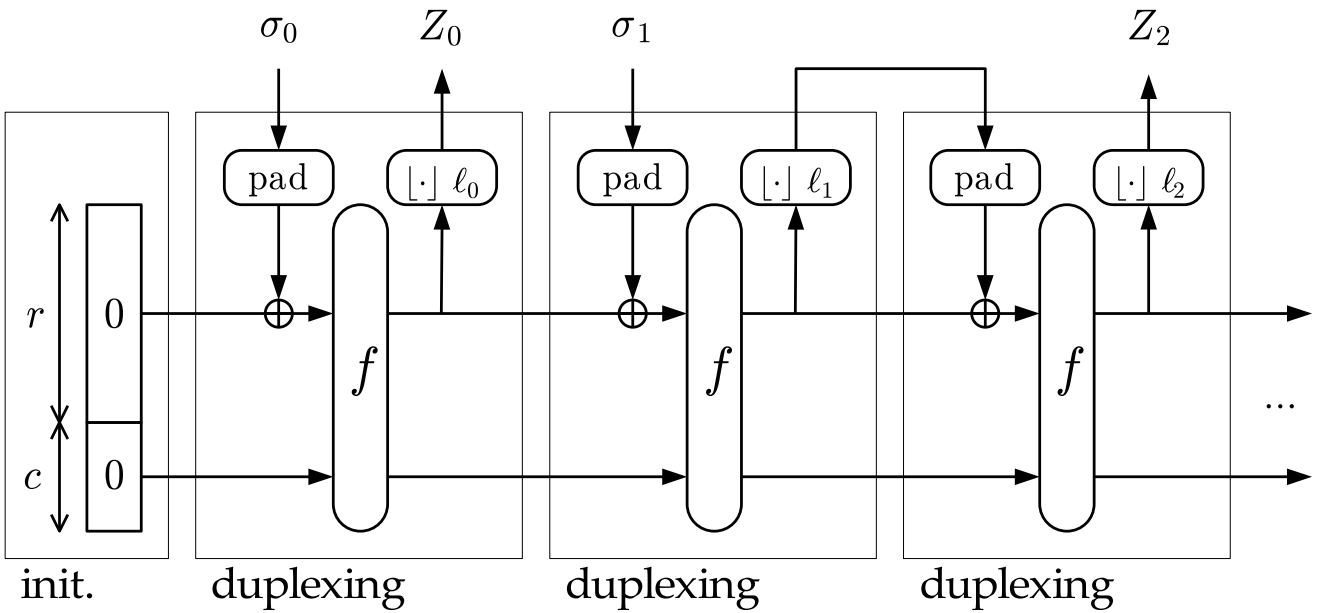
SpongeWrap authenticated encryption



- Single-pass authenticated encryption
- Processes up to r bits per call to f
- Functionally similar to (P)helix [Lucks, Muller, Schneier, Whiting, 2004]

Reseedable pseudorandom sequence generator

- Defined in [Keccak Team, CHES 2010] and [Keccak Team, SAC 2011]
- Support for forward secrecy by *forgetting* in duplex:



Reseedable pseudorandom sequence generator

- Defined in [Keccak Team, CHES 2010] and [Keccak Team, SAC 2011]
- Support for forward secrecy by *forgetting* in duplex: