Mike Hamburg, Rambus Cryptography Research

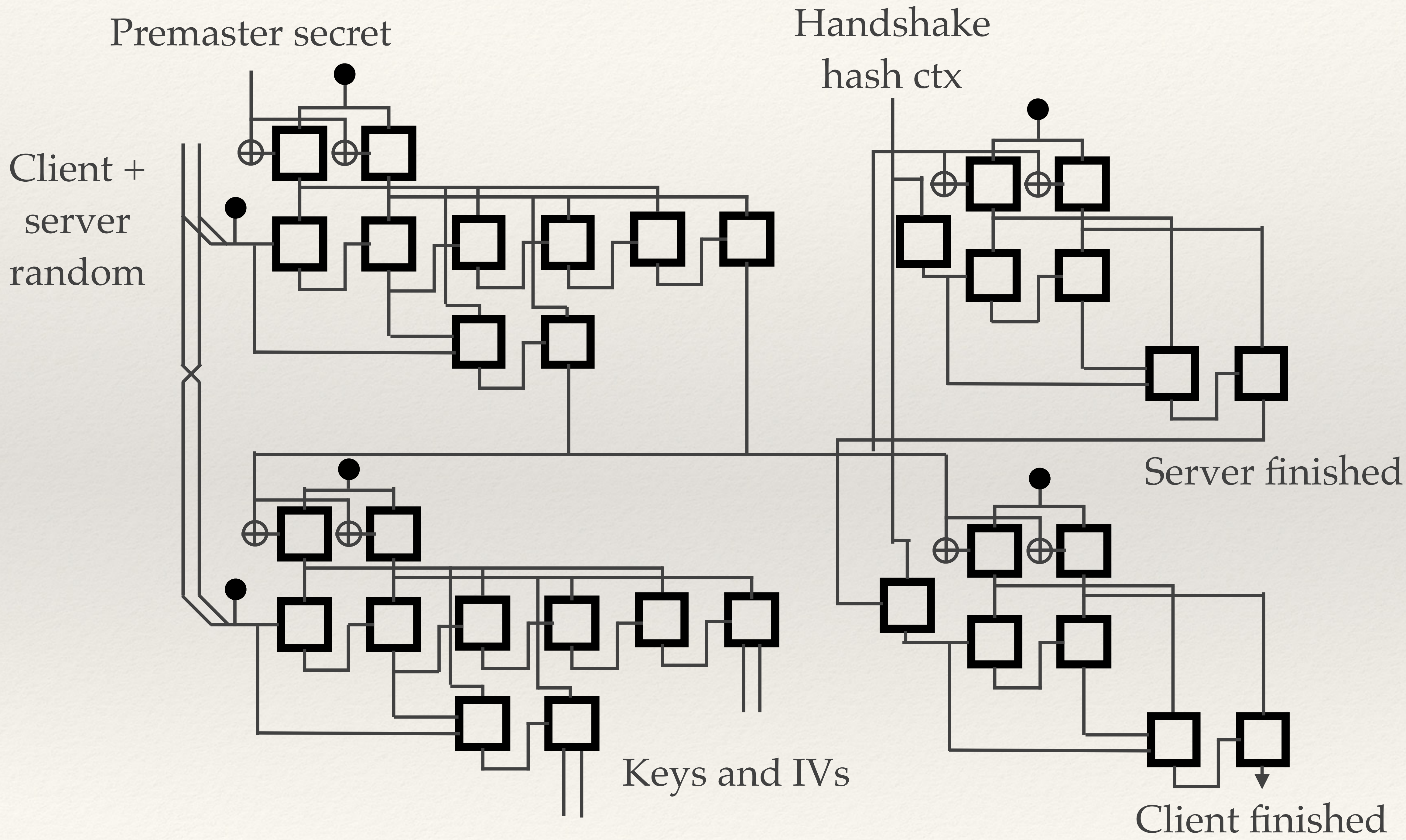
The STROBE lite framework

Protocols for lazy people

Protocol design is hard!

- Can’t always use TLS
- Design <—> analyze, prove
- What to hash, encrypt, etc?
    - Mode?
    - Padding?
    - Framing?
- Easy to get wrong

TLS 1.2 hash calls (calc MS + finished)



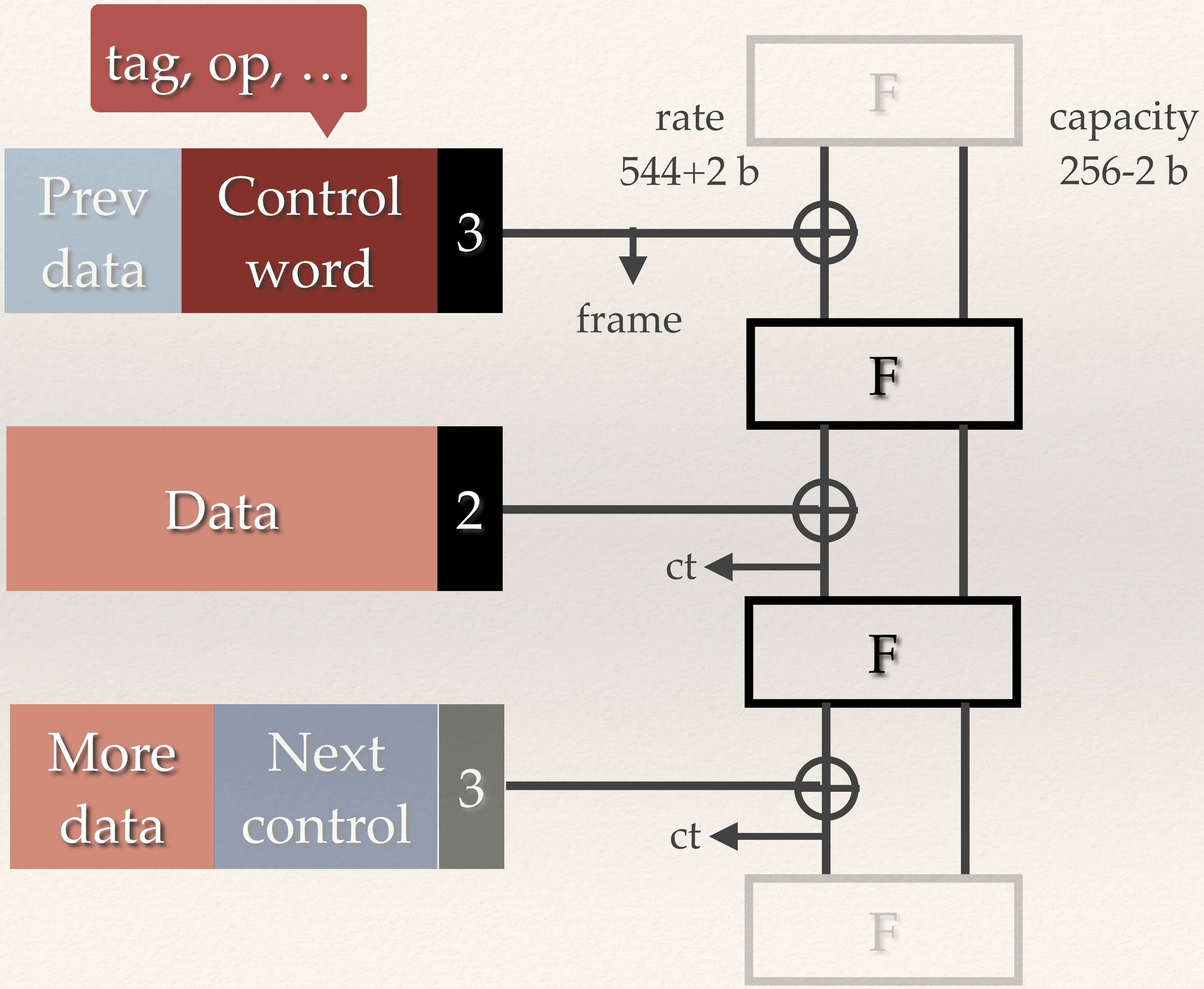
Finished is also encrypted, but I got bored before drawing the cipher calls.

STROBE lite

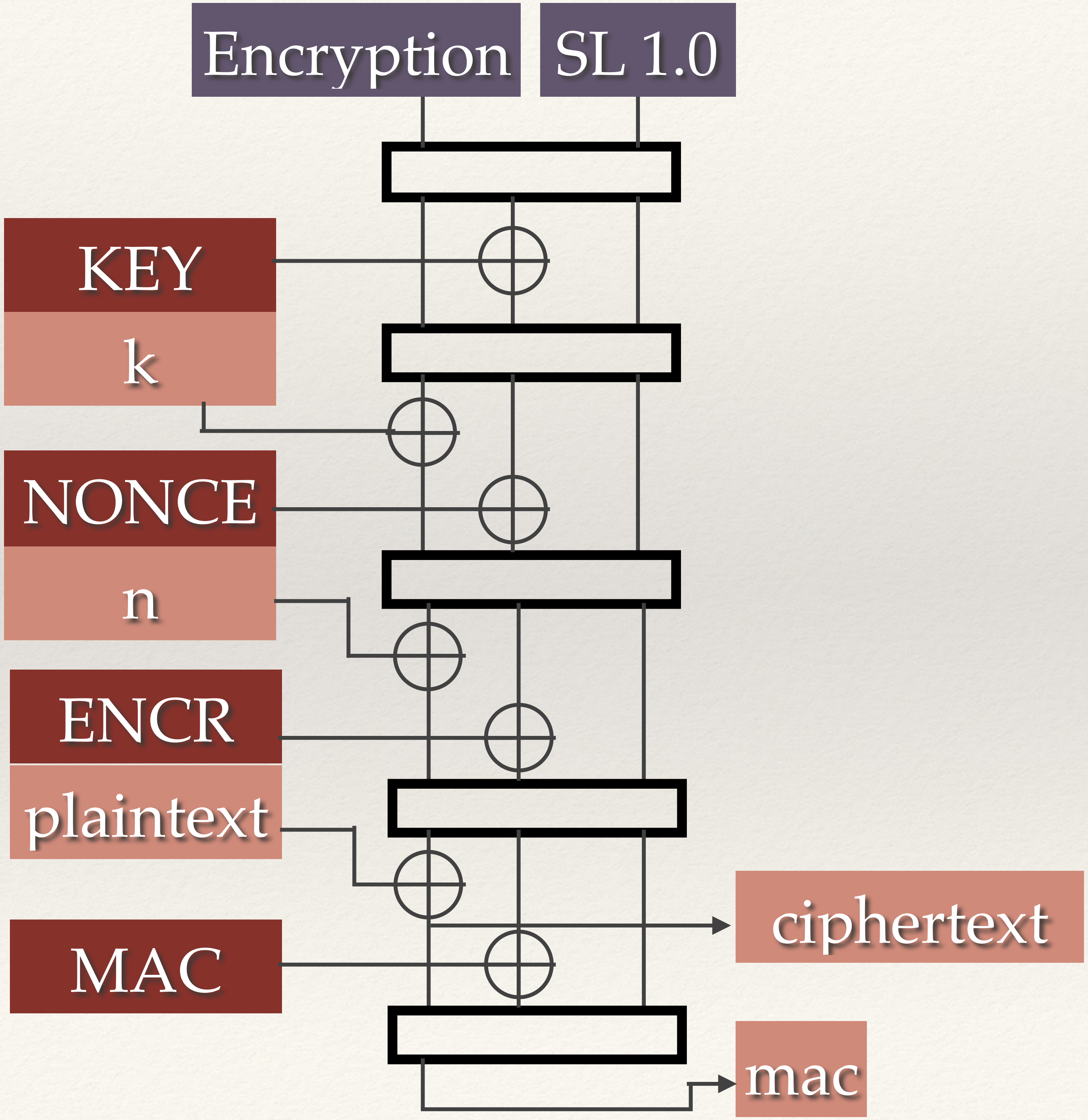
- Sponge to the rescue!

- Variant of Markku-Juhani O. Saarinen’s BLINKER
- KeccakF[800] or other sponge
- < 2kB code (thumb2 C prototype), small mem footprint
- Replace AES and SHA too

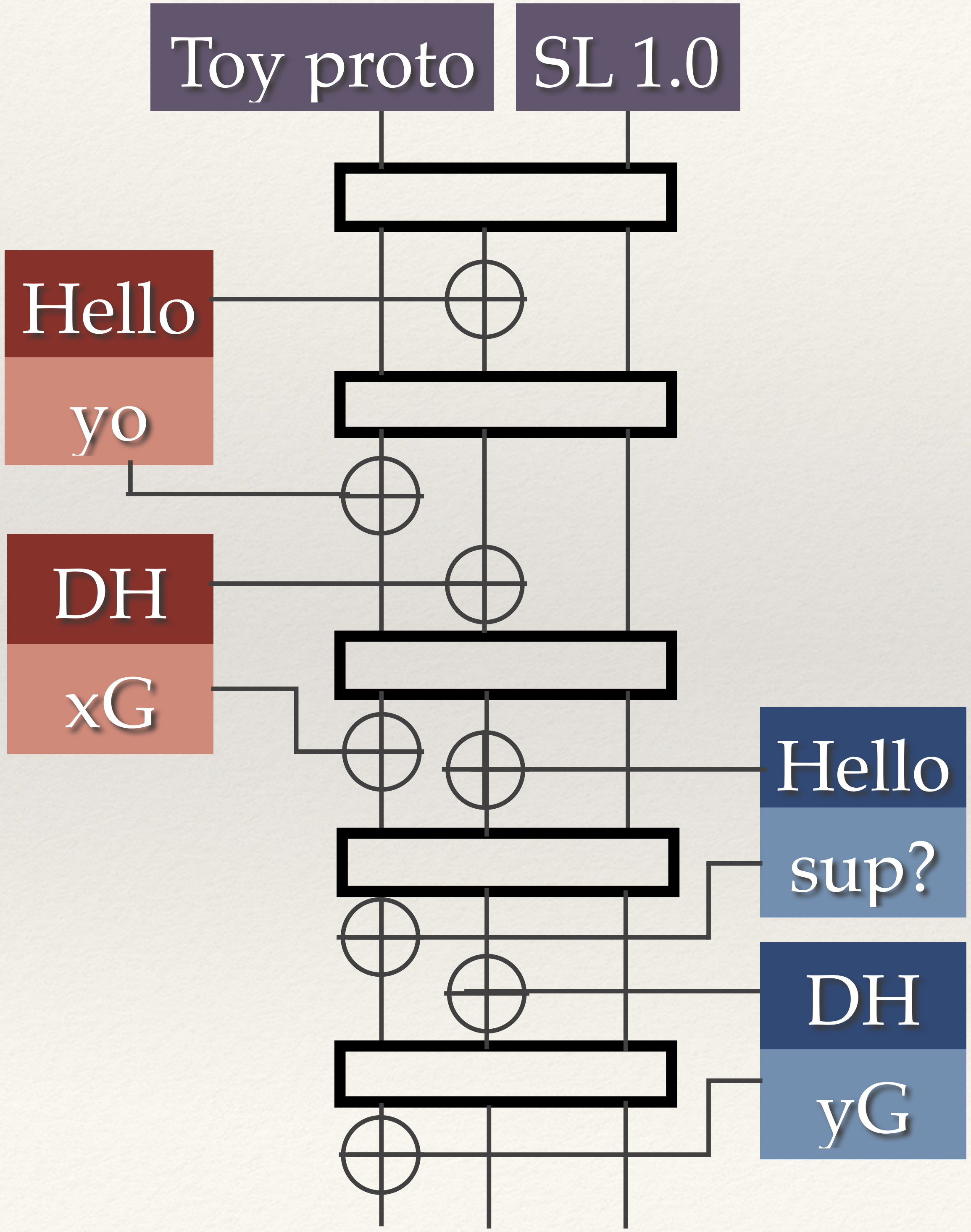
The STROBE lite duplex mode

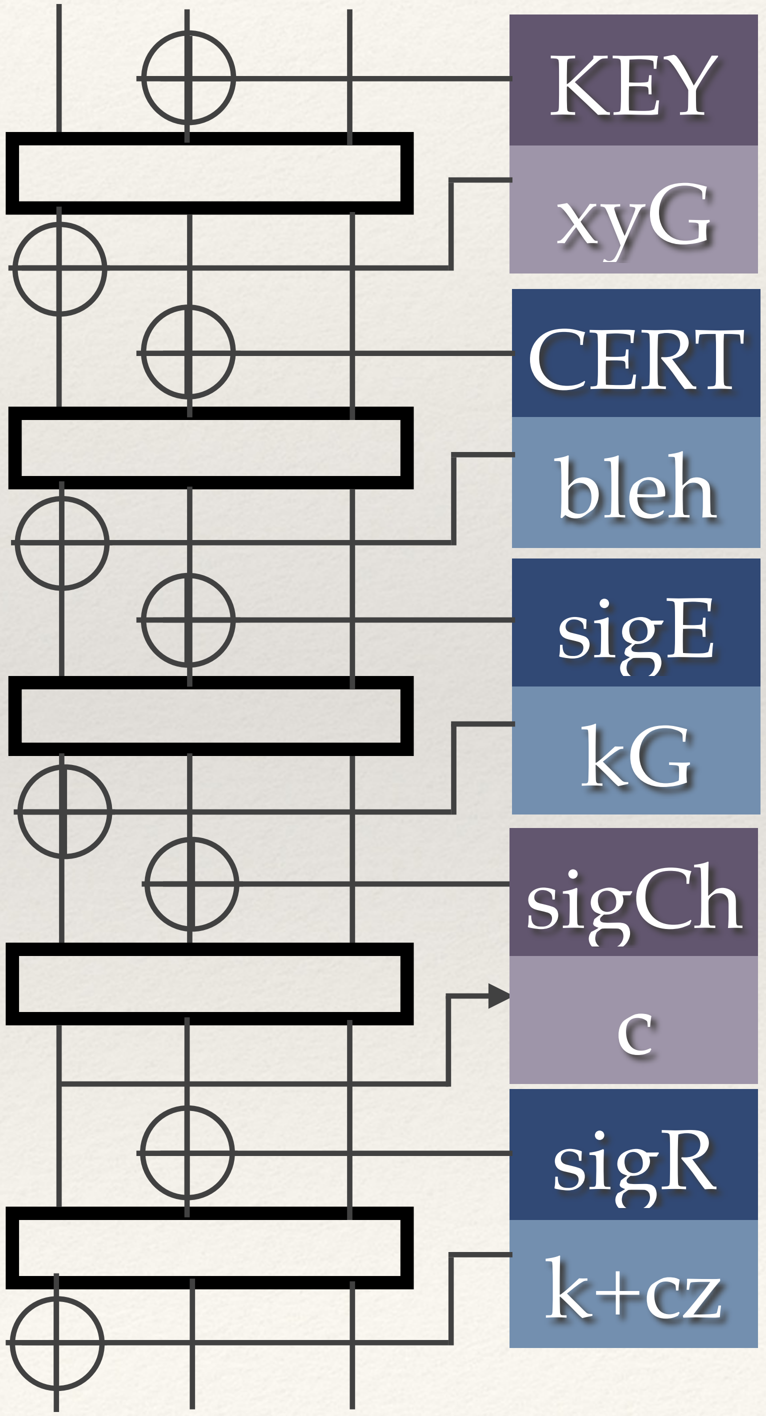


Encryption


Encryption
SL 1.0
KEY
k
NONCE
n
ENCR
plaintext
ciphertext
MAC
mac

Example STROBE lite handshake





That’s all!

`https://github.com/bitwiseshiftleft/strobelite`

I’d love to hear your input!