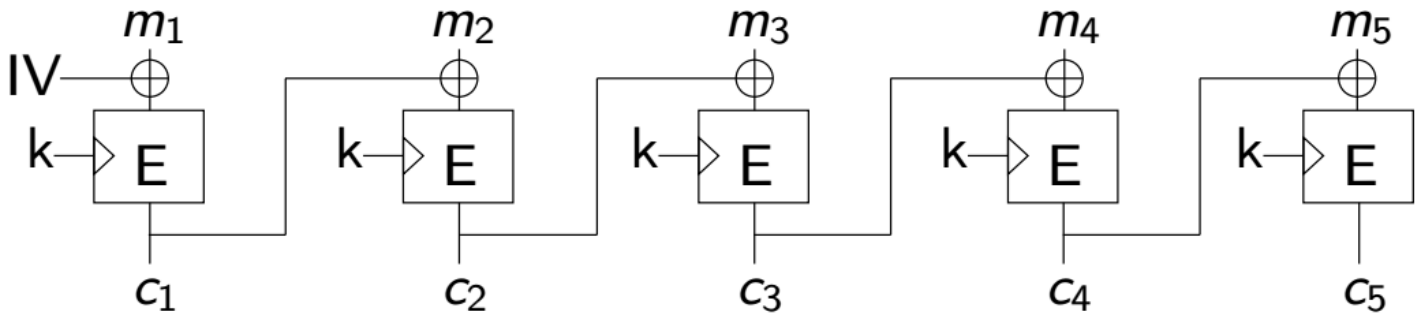
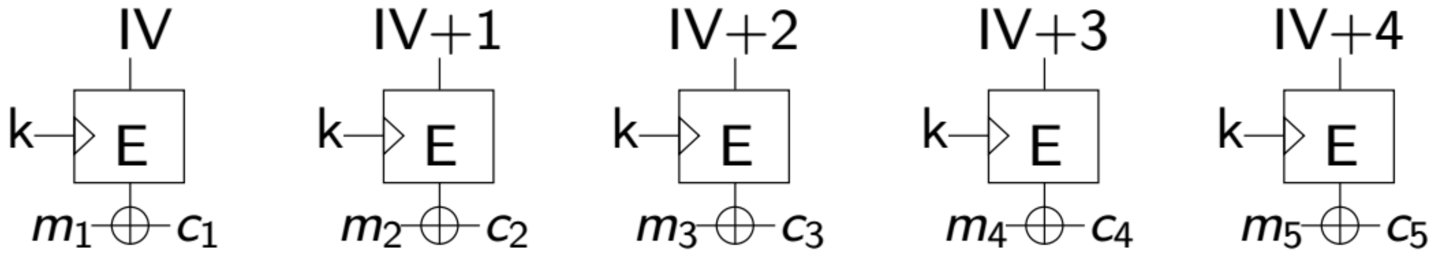
TETSponge: a Duplex-based Leakage-Resilient AEAD Mode

Chun Guo. Joint work with

Olivier Pereira, Thomas Peters, and François-Xavier Standaert

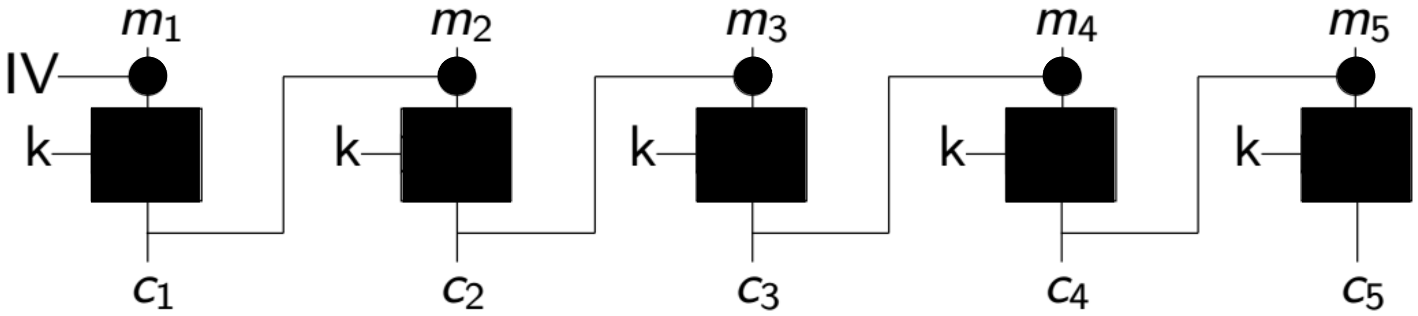
Classical Modes: CBC, CTR

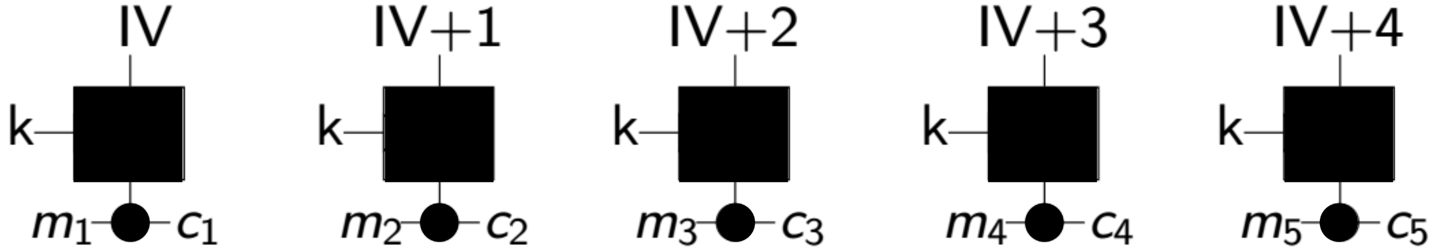




- Differential power analysis (DPA) to recover the key k.

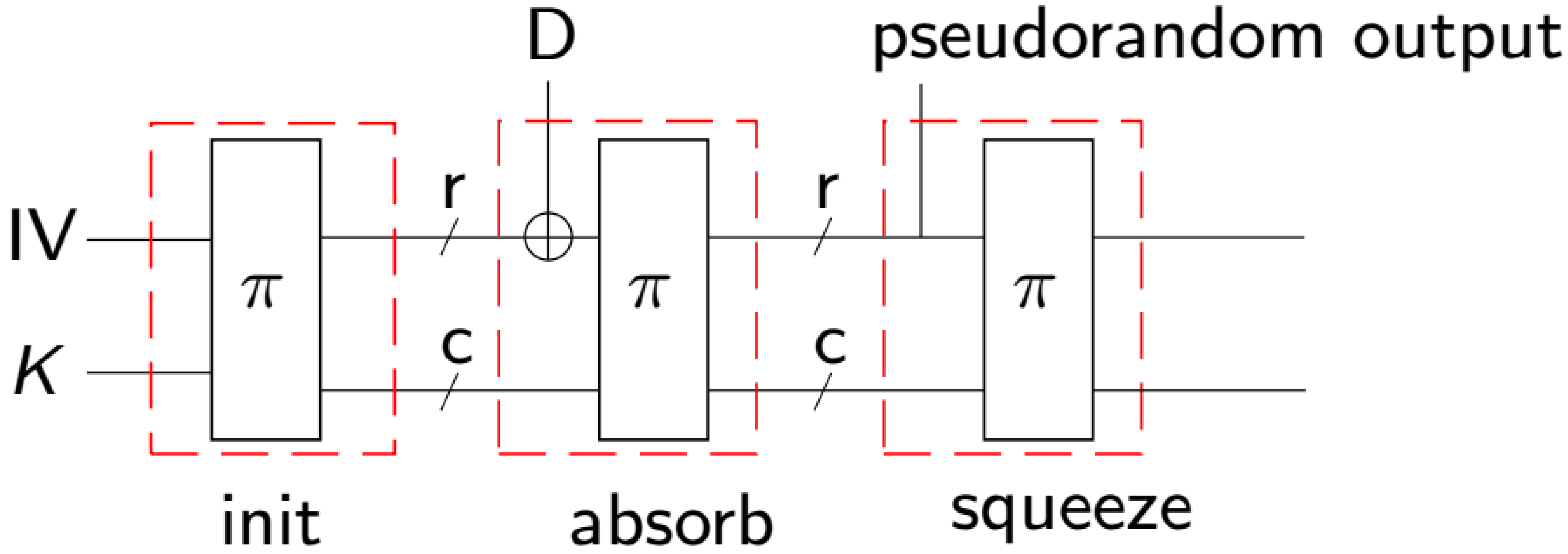
DPA Resistance: Full Protection





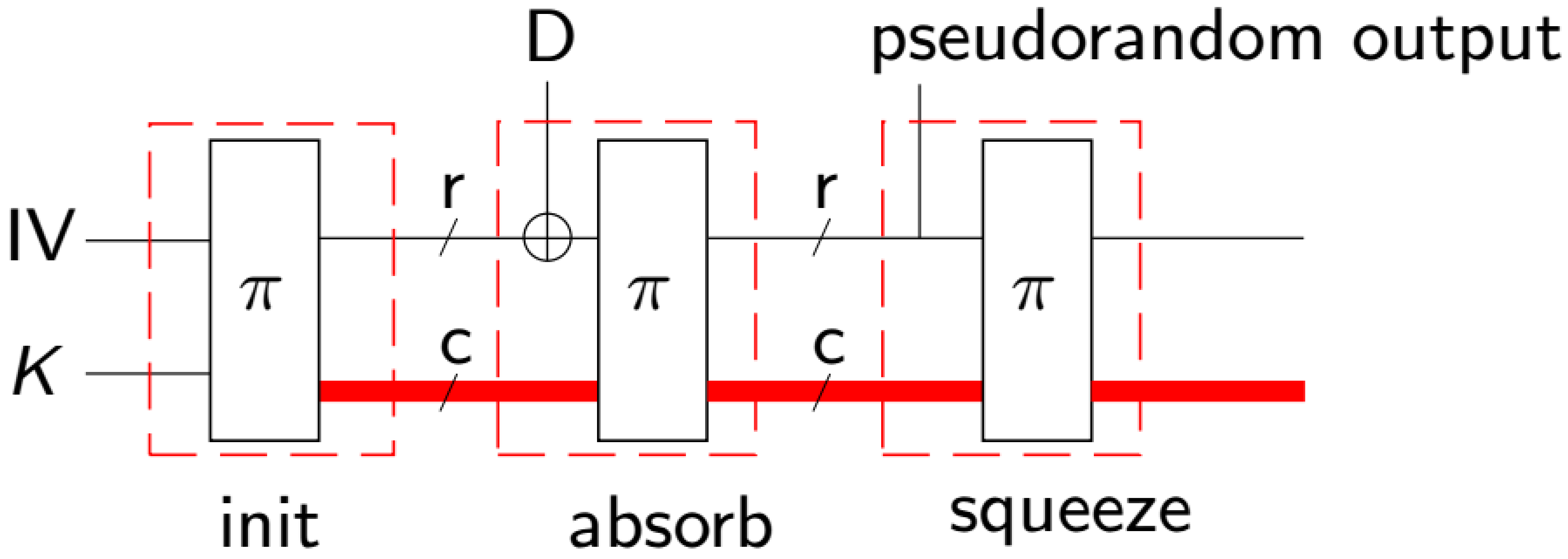
- **A dark world**.

DPA Resistance: the Duplex construction



- Consistently refreshing the internal secret state.

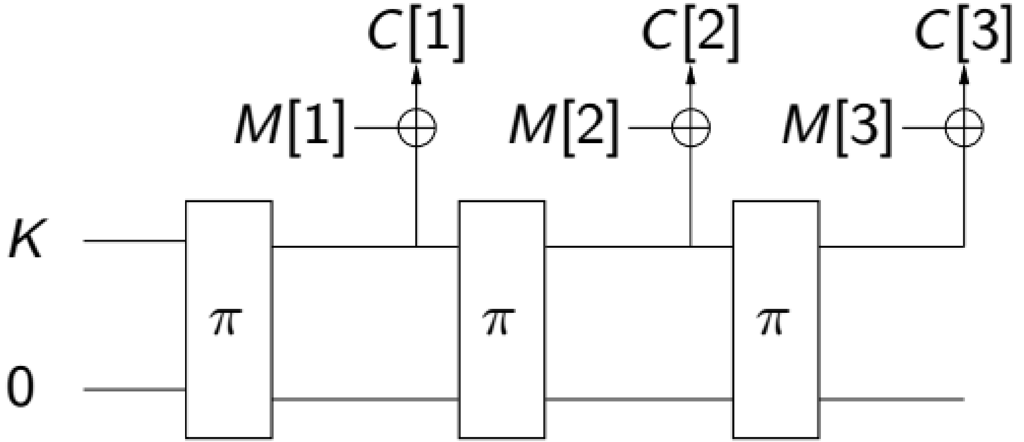
DPA Resistance: the Duplex construction

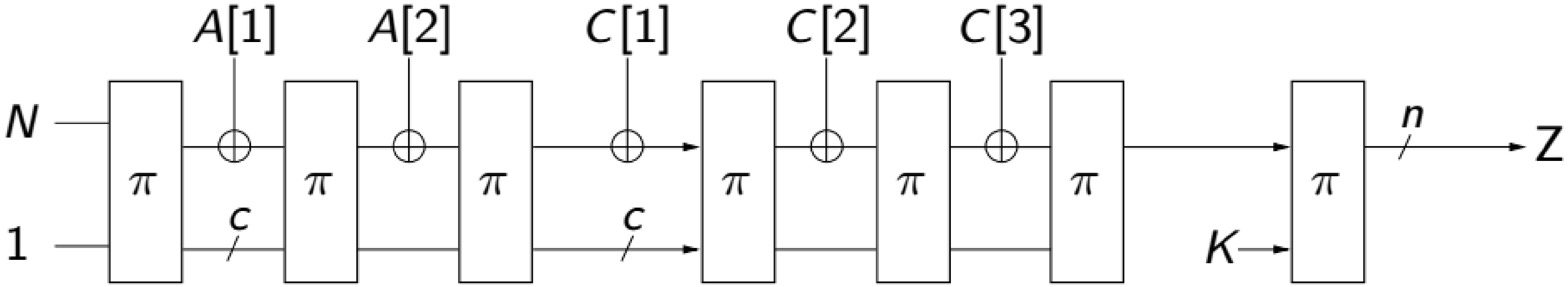


- Consistently refreshing the internal secret state.

To an AE: Encrypt-then-MAC (Why?)

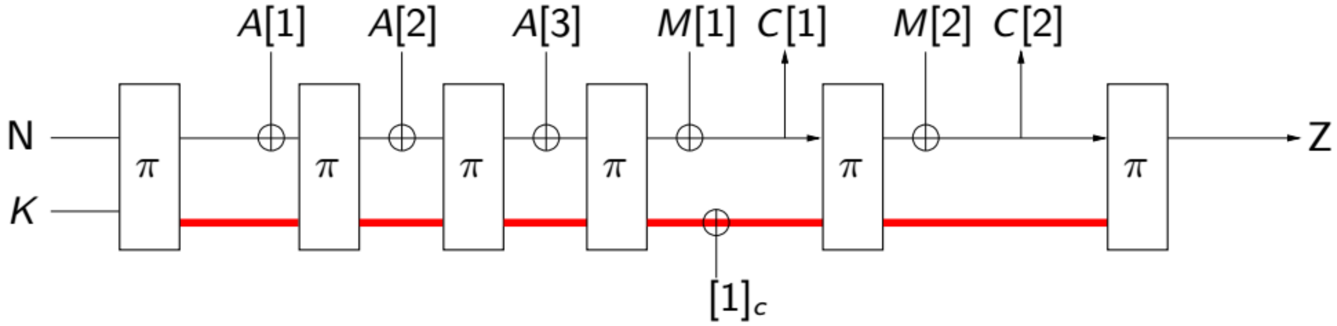
- Duplex-based Stream cipher + Sponge-based MAC





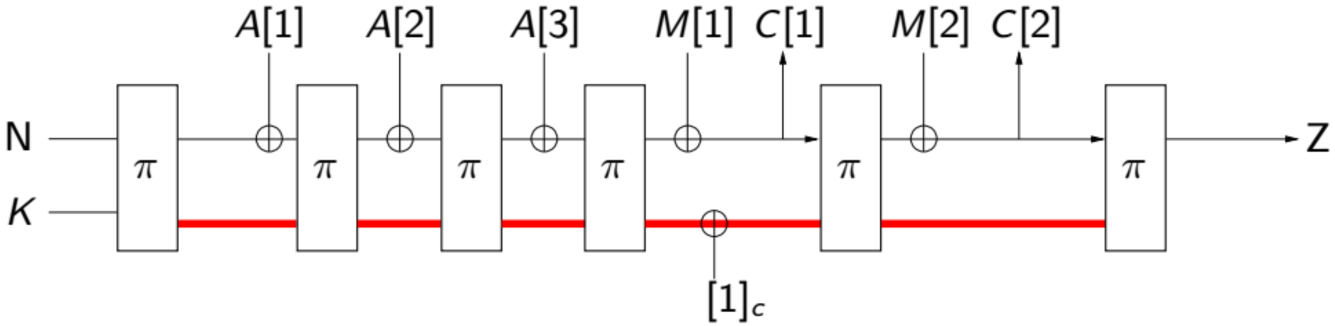
Question

- What if we want better efficiency?
- What can we achieve in 1 pass? Just completely surrender to decryption leakages?

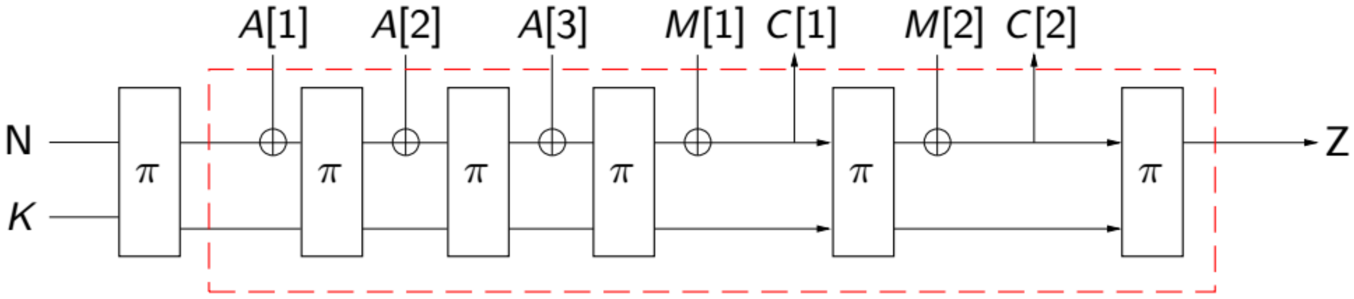


Towards Efficiency: 1-pass

- Duplex for two roles. With secrets: a standard 1-pass duplex-based AE

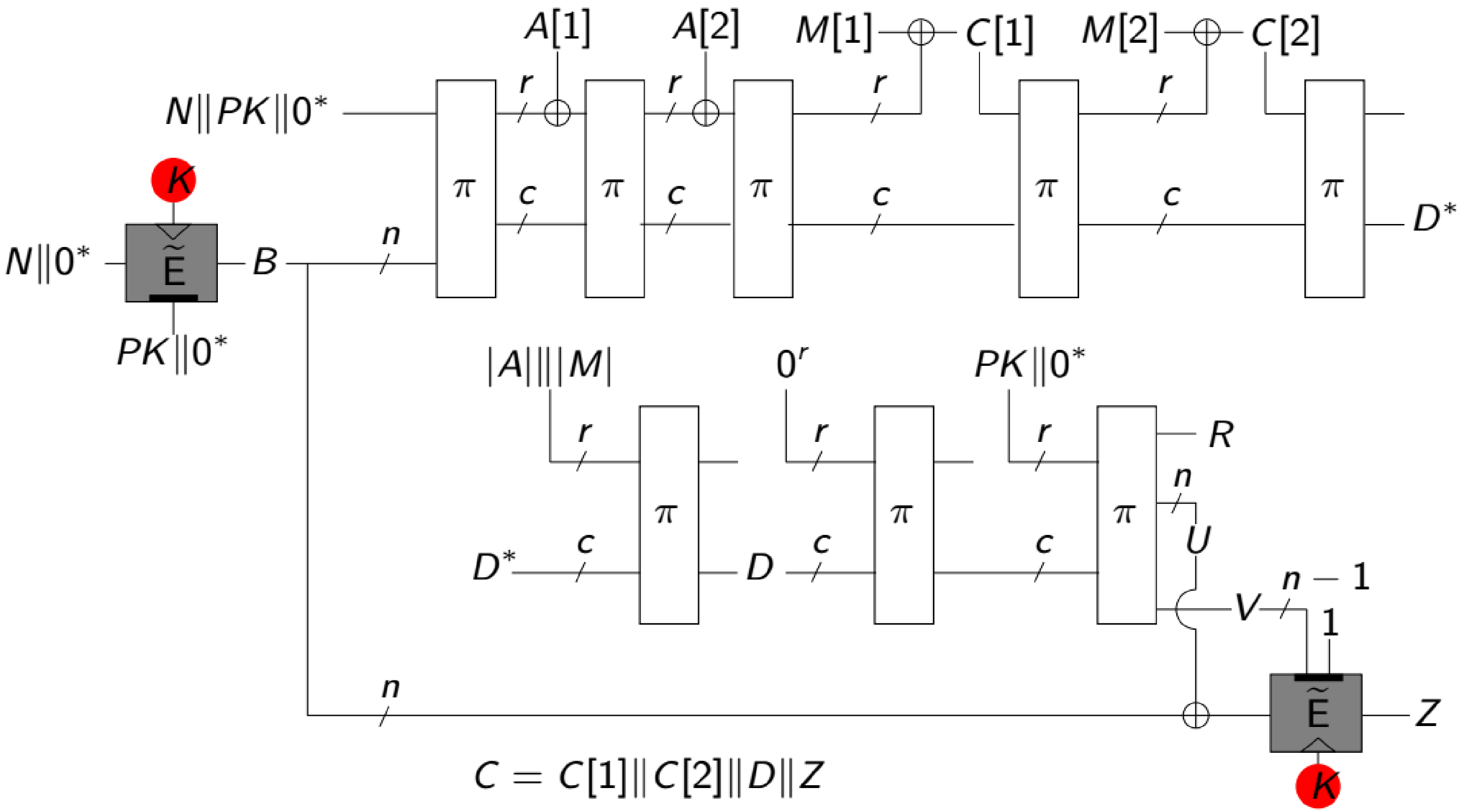


- With no secret: a hash (now we can play with the hash digest Z)



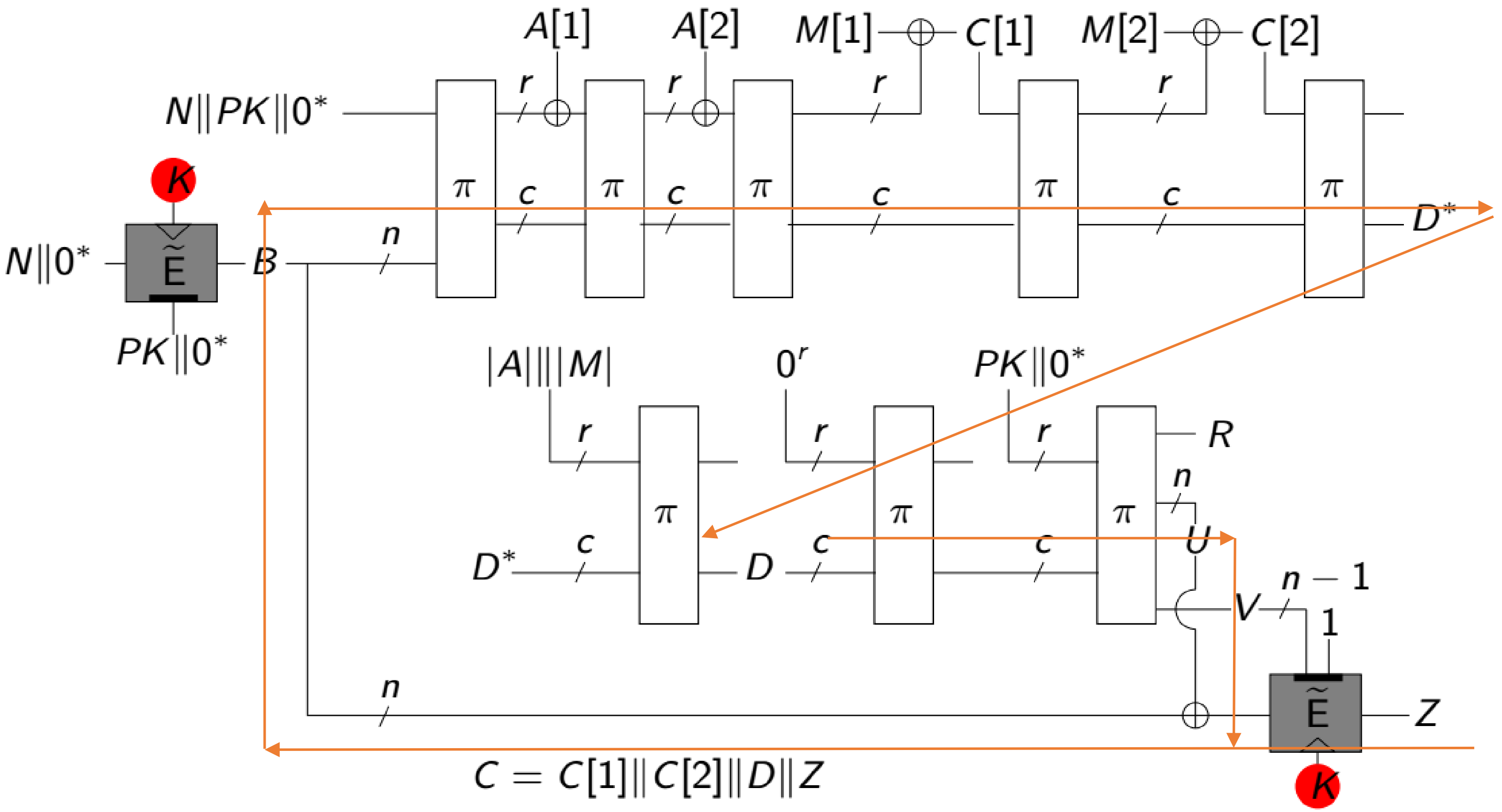
$Hash(A[1], A[2], A[3], C[1], C[2])$

TETSponge version 1

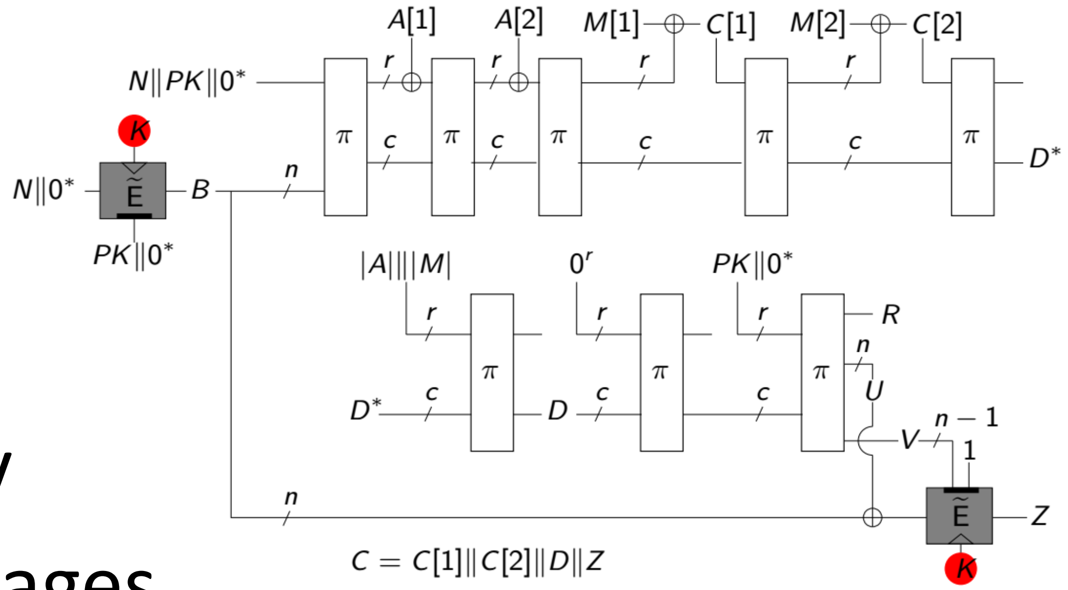


$C = C[1]||C[2]||D||Z$

TETSponge version 1 (using TBC inverse)



TETSponge version 1



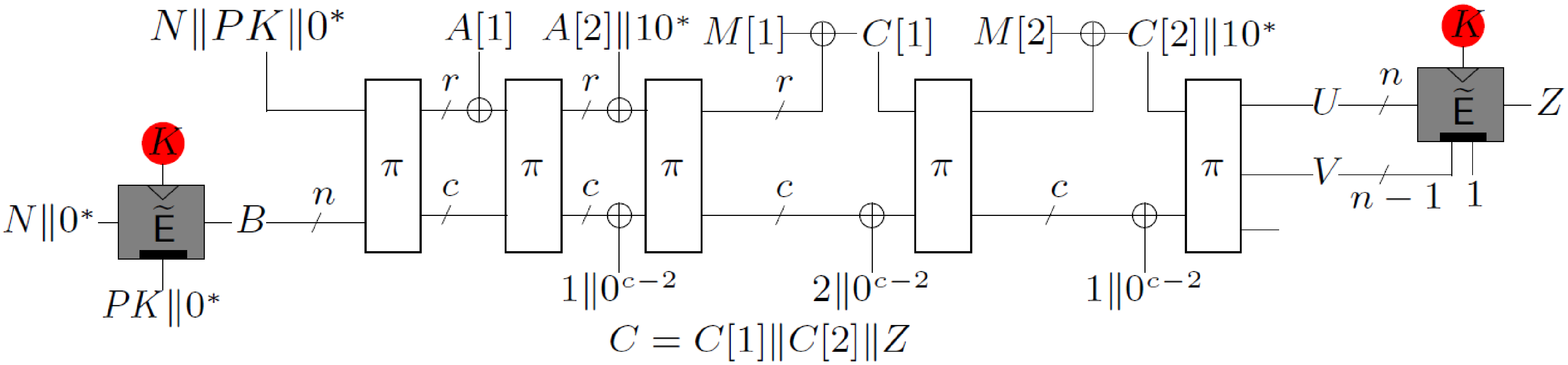
- 1 pass, online encryption
- Beyond n/2 *multi-user* security
- Inverse of the TBC for less leakages
- Weakly secure online decryption
  - Decrypting with fresh (D,Z) gives pseudorandom message that can be securely released.
- Shortage: too large stretch
  - $(N, A, M) \rightarrow (A, C, D, Z)$. Ciphertext expansion: $|D| + |Z| = c + n$ bits

TETSponge Current Version: Better Efficiency

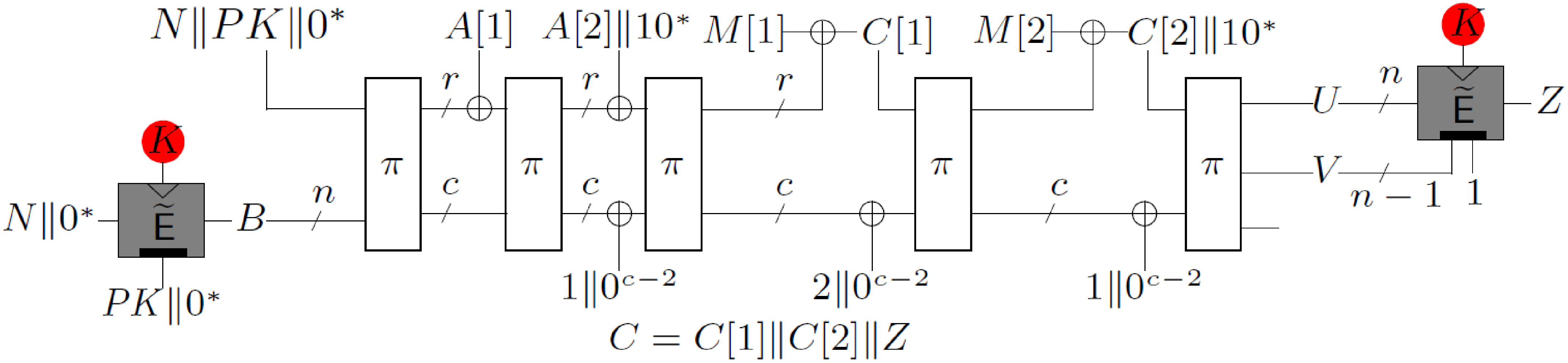
- Why not just use the duplex hash digest as the input to the TBC?

TETSponge Current Version: Better Efficiency

- Why not just use the duplex hash digest as the input to the TBC?



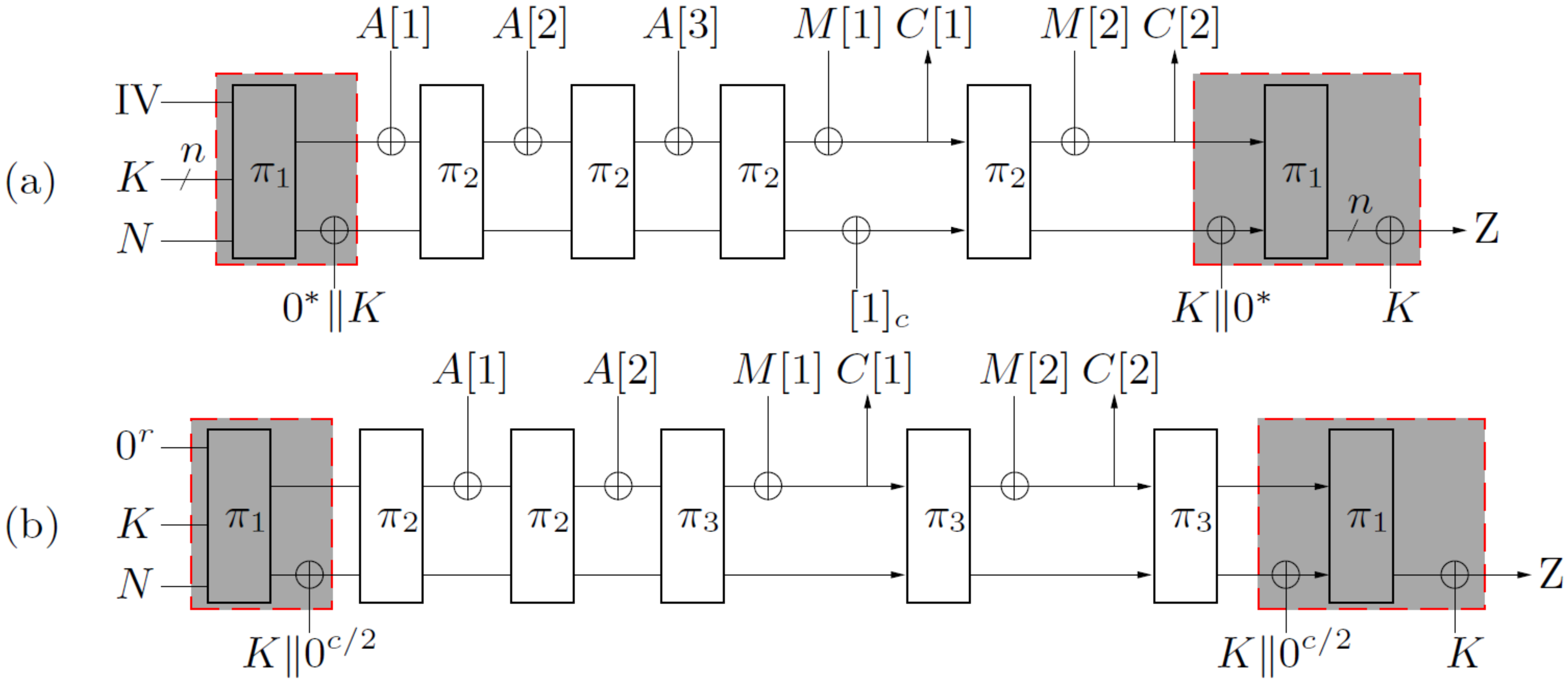
TETSponge Current Version: Better Efficiency



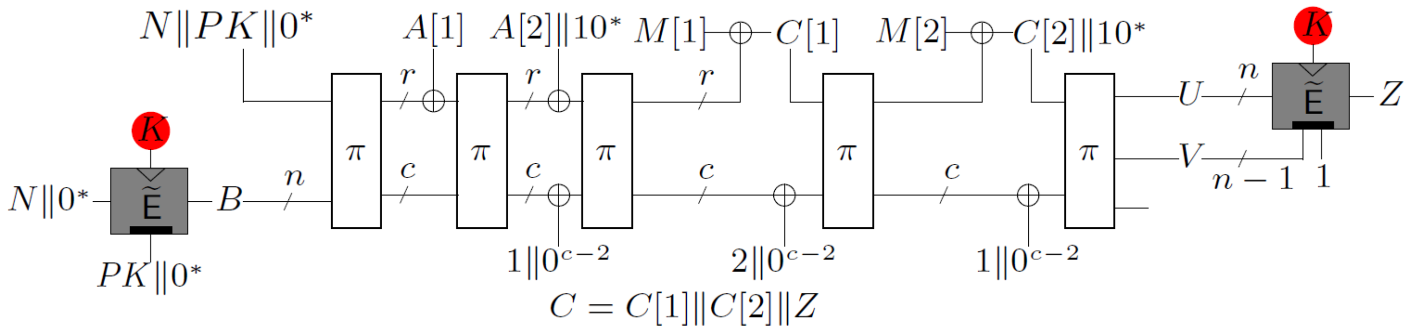
$C = C[1]\|C[2]\|Z$

- Domain separation bits
- The other details are inherited from v1.

Hitting Ascon & GIBBON



TETSponge: Security



- $Min\{\frac{2^n}{n^2}, 2^{c/2}\}$ bit black-box CCA security at fresh nonce up to $2^{|PK|}$ users
- $Min\{\frac{2^n}{n^2}, 2^{c/2}\}$ bit ciphertext integrity with nonce-misuse and decryption leakages up to $2^{|PK|}$ users
- $2^{n/2}$ bit leakage CCA security with encryption leakages at fresh nonce, up to $2^{|PK|}$ users. https://eprint.iacr.org/2019/193

Thanks!
Comments & Questions?

The author would like to thank Francesco Berti for identifying some typos.