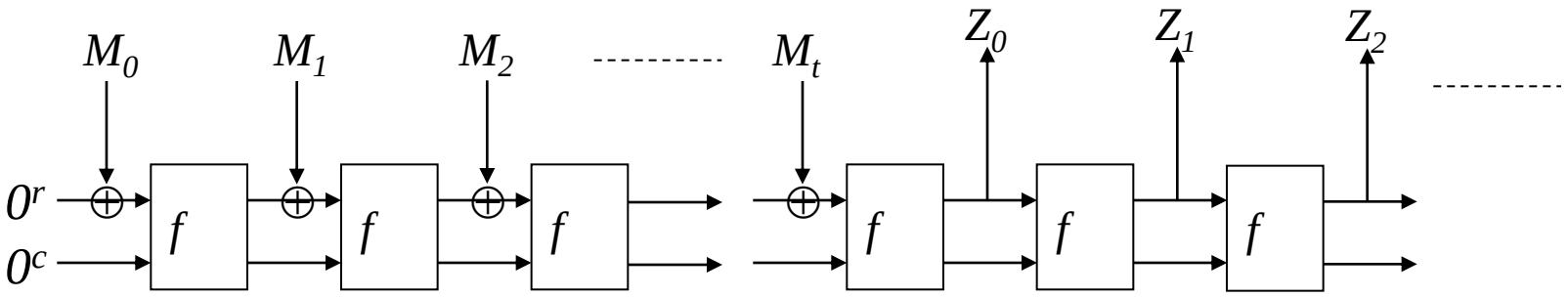
Sufficient Conditions on Padding Schemes of **Sponge Construction** and **Sponge-based Authenticated-Encryption Scheme**

Donghoon Chang
IIIT-Delhi, India

12 December 2012, Kolkata, Indocrypt 2012

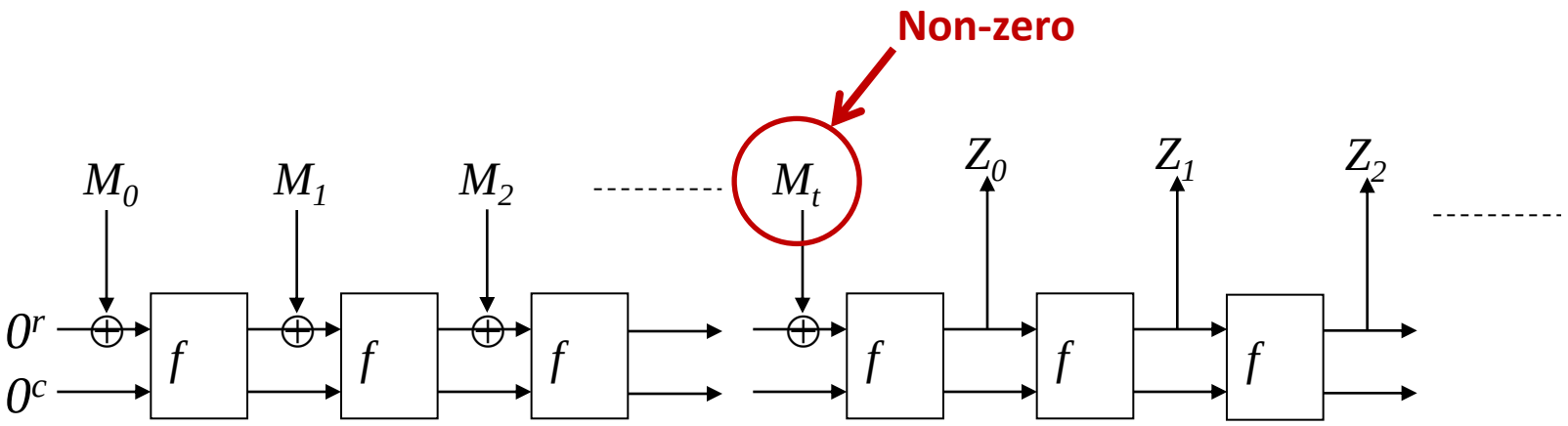
Sponge Construction

- Domain Extension designed by Bertoni, Daemen, Peeters, and Van Assche (Eurocrypt 2008): it is used for **Keccak (SHA-3).**



Sponge Construction

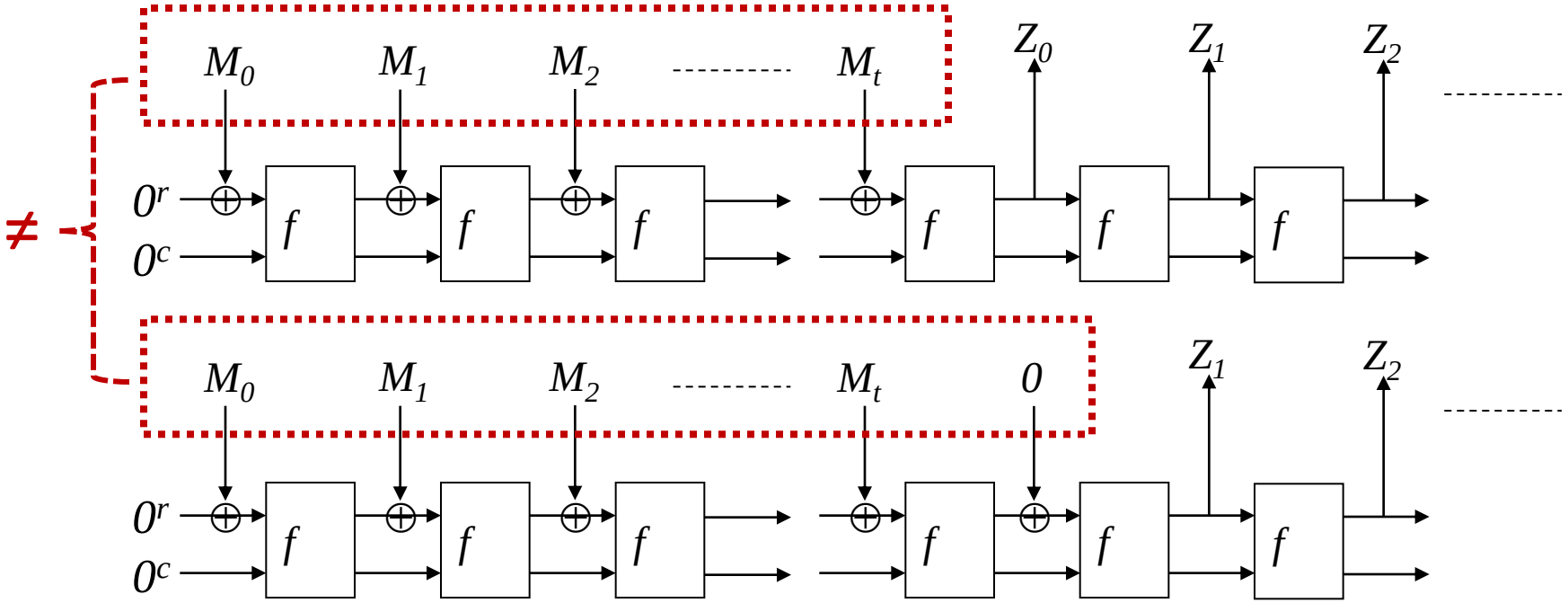
- Domain Extension designed by Bertoni, Daemen, Peeters, and Van Assche (Eurocrypt 2008): it allows hash output of any length.



A Simple Example for Padding Scheme: pad(M)=M||10*

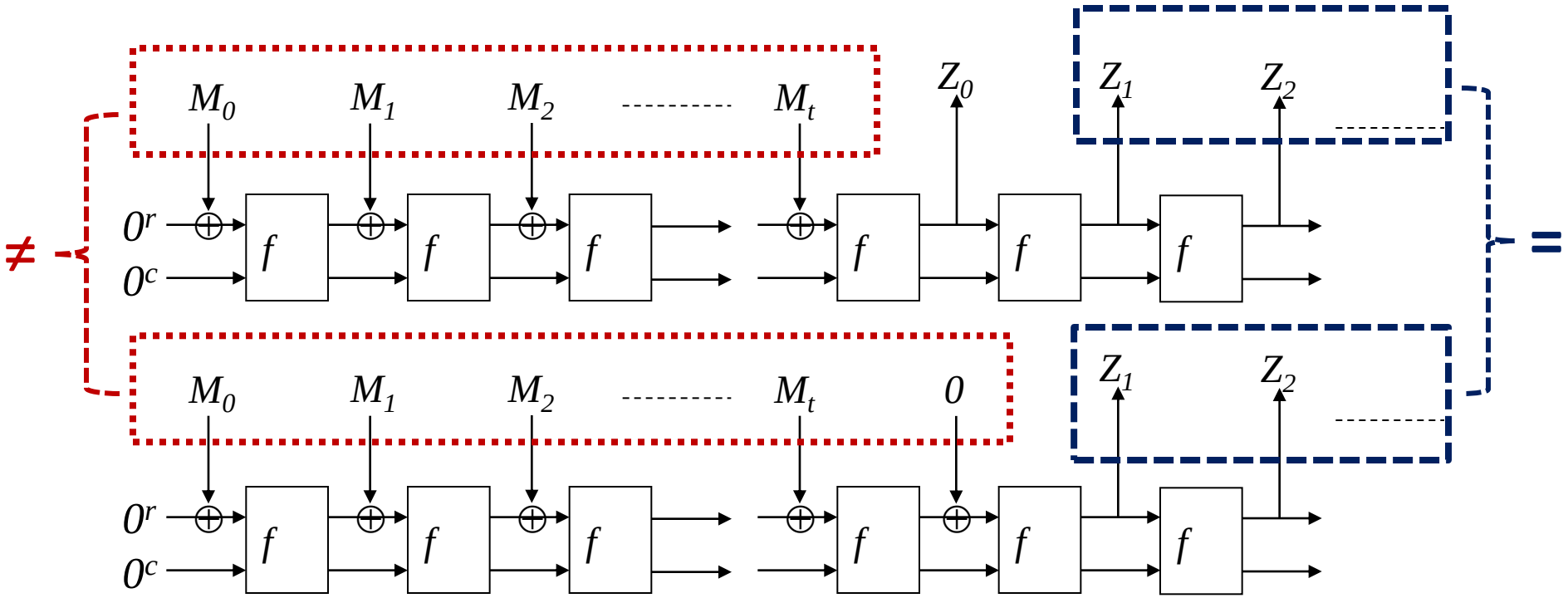
Sponge Construction

- If the last block can be zero,



Sponge Construction

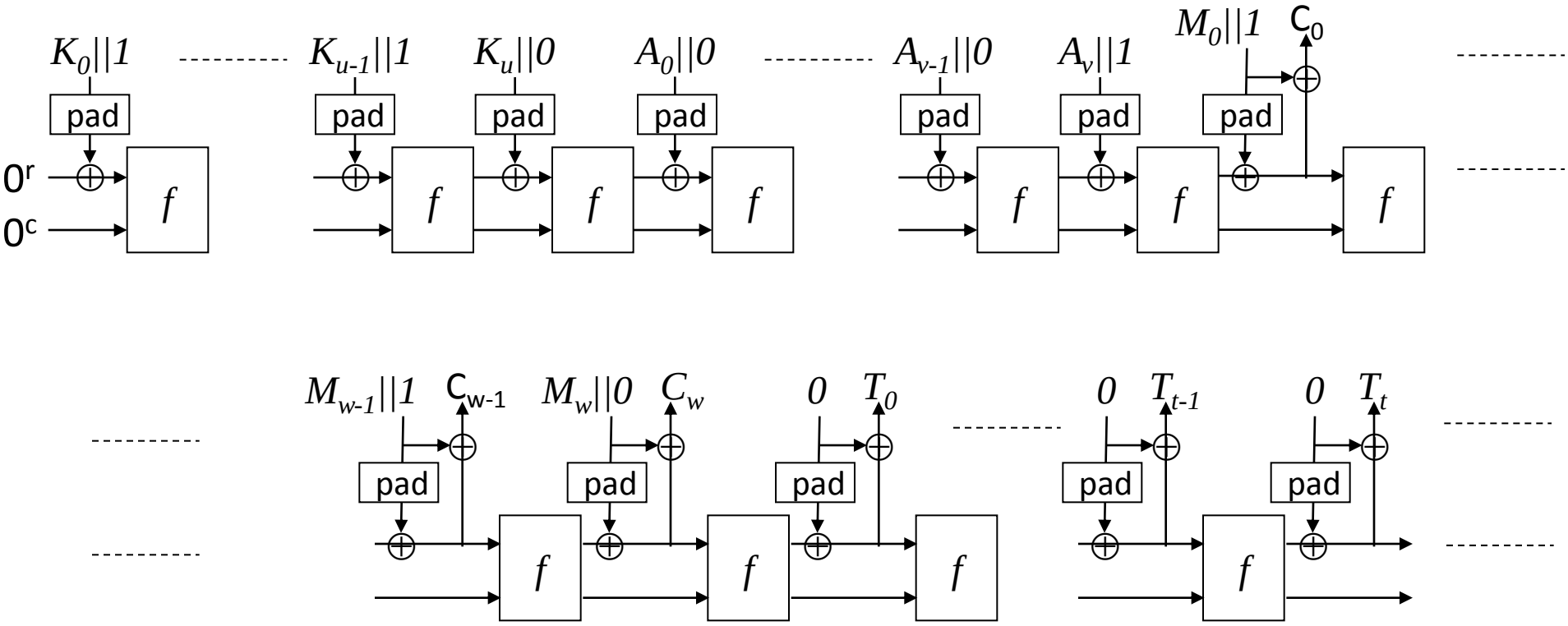
- If the last block can be zero,



Spongent

- Sponge-based Authenticated Encryption (AE) Scheme
- Designed by Bertoni, Daemen, Peeters, and Van Assche (NIST Second Hash workshop 2010)
- Its security is based on the security of Sponge construction.

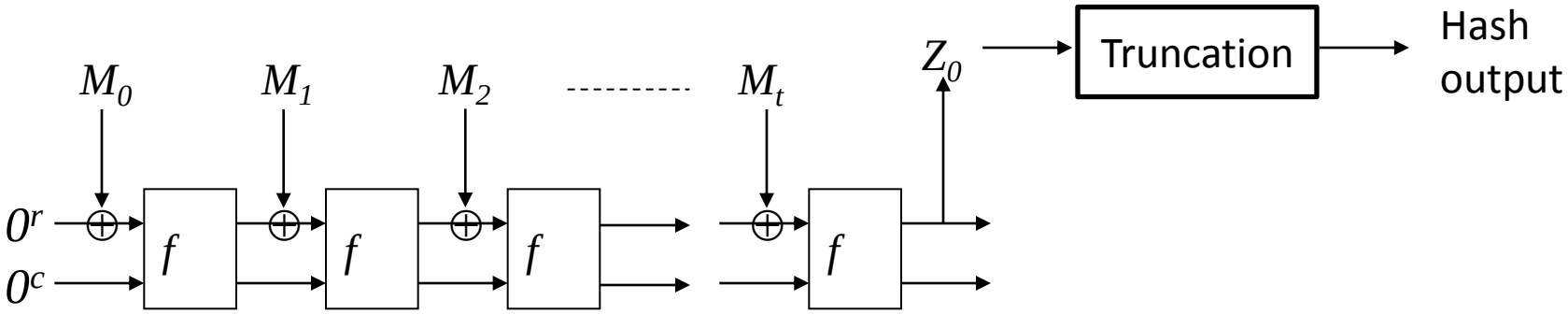
Spongent


$K_0||1$
$K_{u-1}||1$
$K_u||0$
$A_0||0$
$A_{v-1}||0$
$A_v||1$
$M_0||1$
C_0
pad
0^r
0^c
f
$M_{w-1}||1$
C_{w-1}
$M_w||0$
C_w
0
T_0
T_{t-1}
T_t

Our results

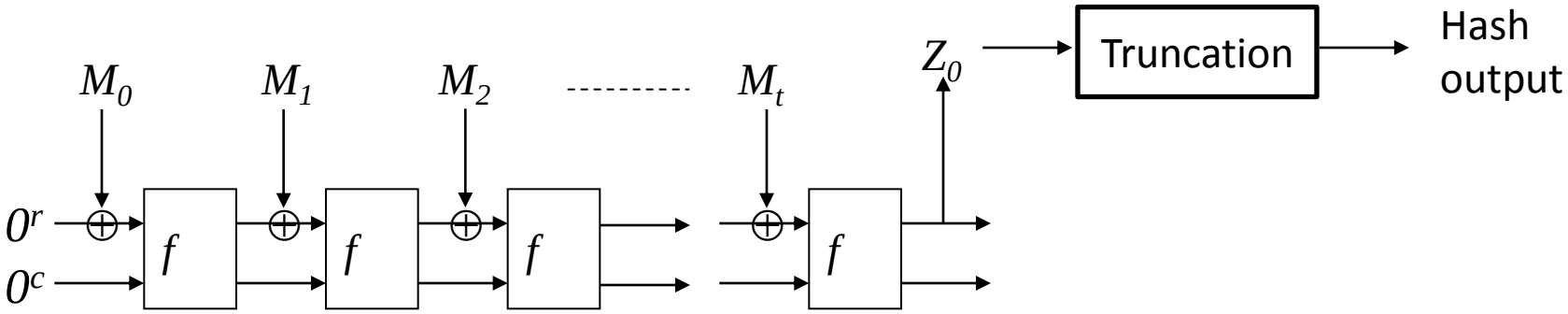
Sponge construction with the truncation of one-block hash output

- Non-zero condition for padding is not required. (Any reversible padding is fine.)



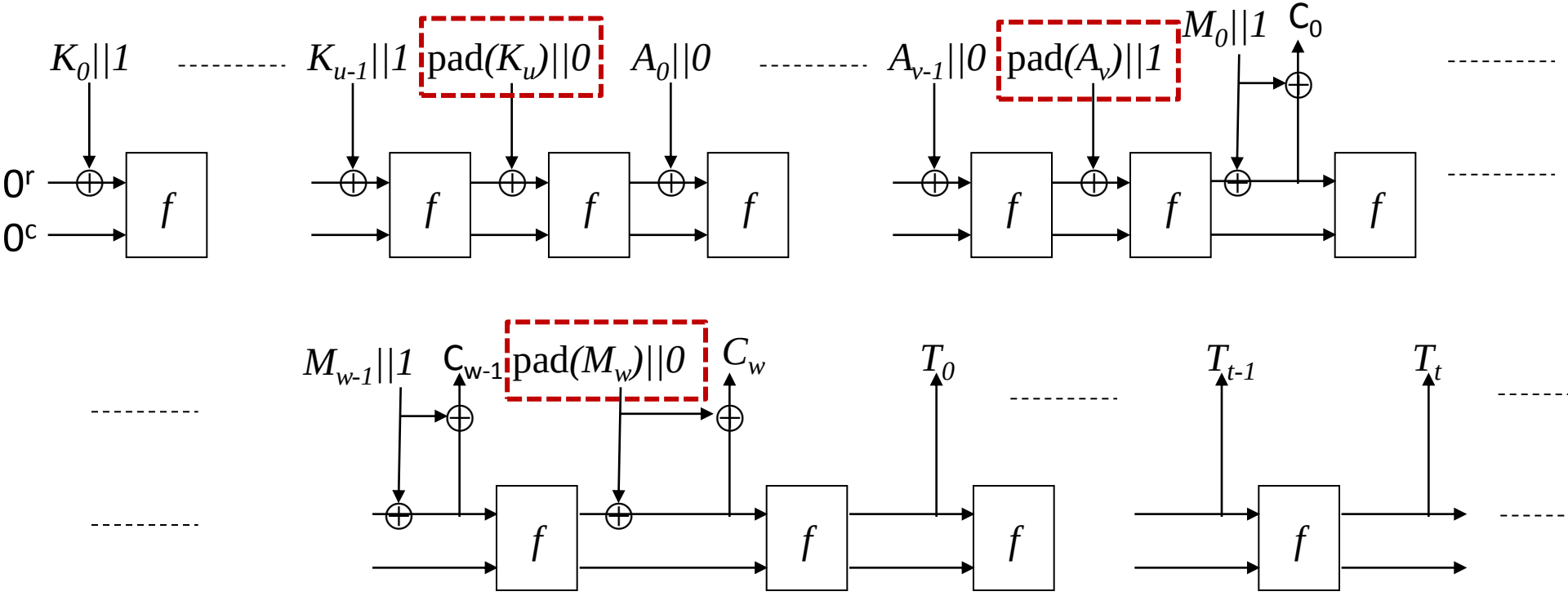
Sponge construction with the truncation of one-block hash output

- If a message is only allowed to be a multiple of a block, no padding is required.



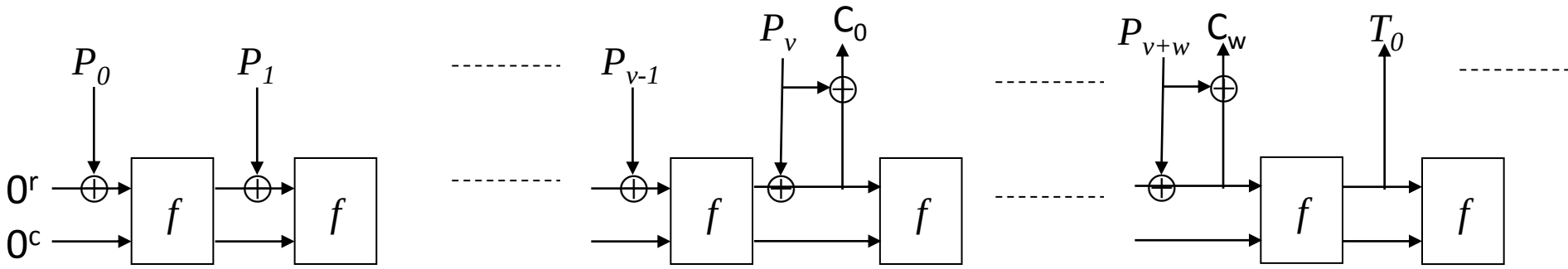
Efficient Sponge-based AE Scheme

- We need to apply the underlying padding scheme **pad** three times **unlike Spongent**.



Sponge-based AE with any Prefix-free Padding Scheme

- We say Pad is prefix-free if for any x, x' (x≠x') Pad(x) is not a prefix of Pad(x'), where x=(x1,x2,x3).
- Pad(K,A,M)=$P_0||\ldots||P_{v+w}$.



Conclusion

- We provided sufficient conditions on padding schemes of Sponge construction and Sponge-based AE in the ideal permutation model.
- It is interesting to know if our result can be further improved **with** a weaker condition than prefix-freeness and **without** any ideal assumption.