# Variants of Sponge-like Construction

Yuji Suga

IIJ

Internet Initiative Japan

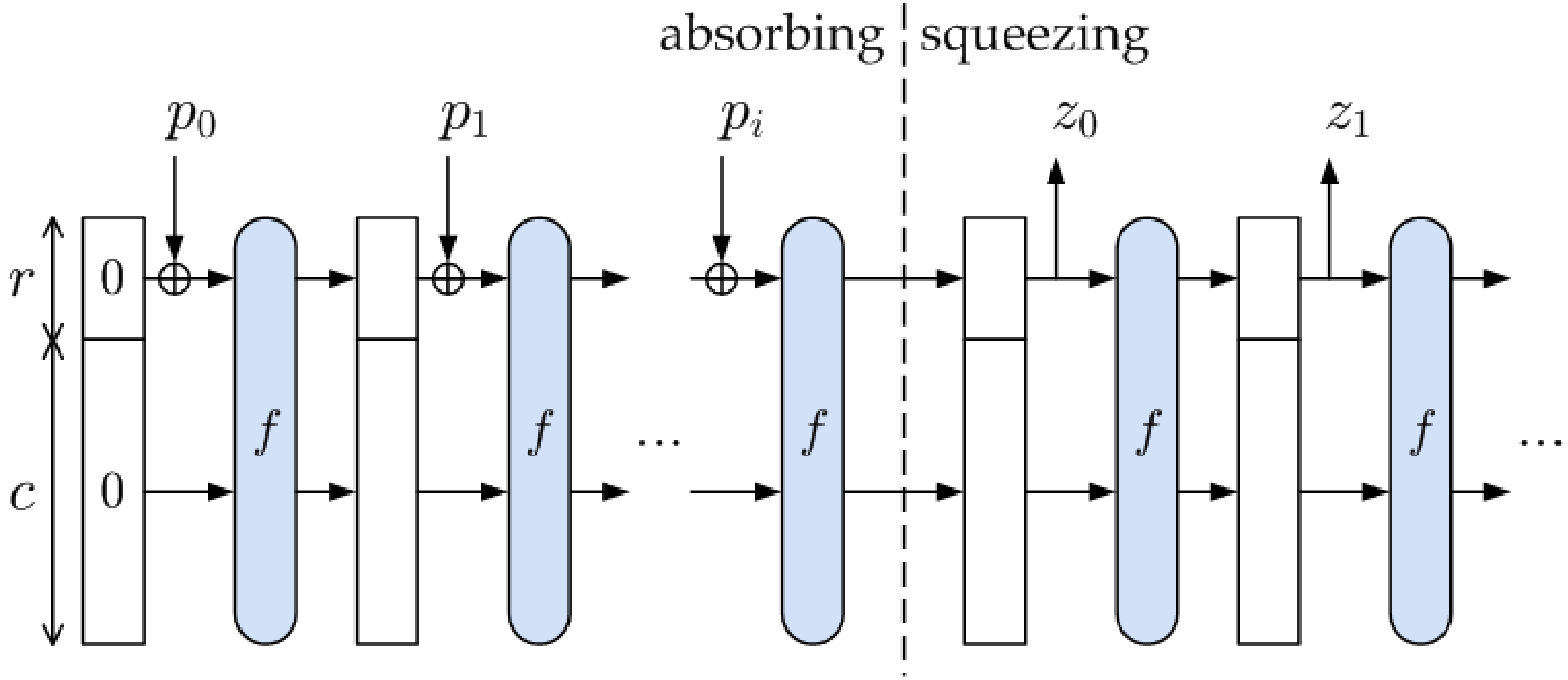
# Sponge construction

- Proposed by Bertoni et al. [1]
  - Simple iterated construction

- Keccak by Bertoni et al.[SHA-3(2008)]
  - Quark by Aumasson et al.[CHES2010]
  - Photon by Guo et al.[CRYPTO2011]
  - Spongent by Bogdanov et al.[CHES2011]

[1] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, *Sponge Functions*, Ecrypt Hash Workshop 2007.

# Sponge construction



© Keccak Team

http://sponge.noekeon.org/

# Sponge

Absorbing -then- Squeezing

# Motivation

Why only Sponge?

# Motivation

- To apply alternatives of “Sponge”, we can design new constructions.
- There are many house-cleaning goods.

# Mop

Absorbing -then- Squeezing

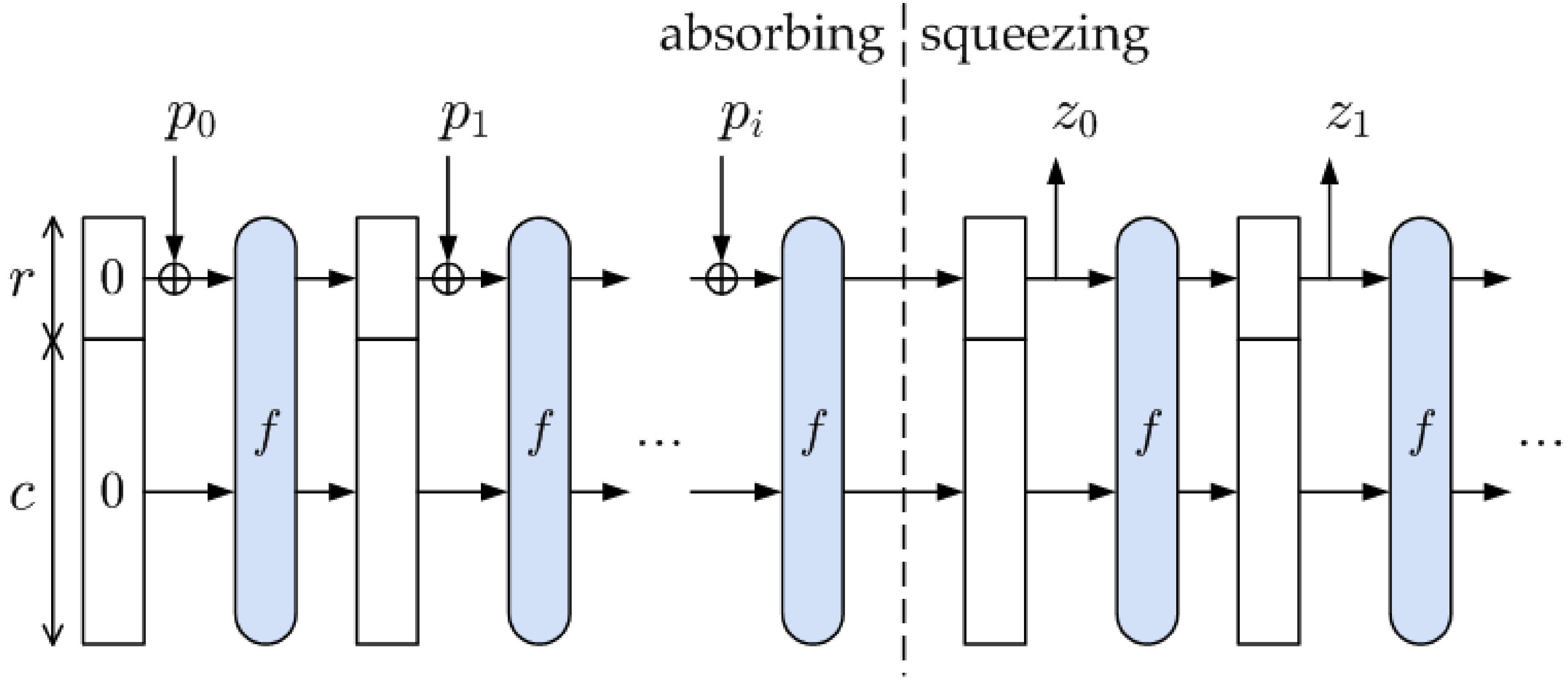
# Mop with Squeezer

Absorbing -then- Squeezing

# Mop with Squeezer

Absorbing -then- Squeezing w/ Rotation

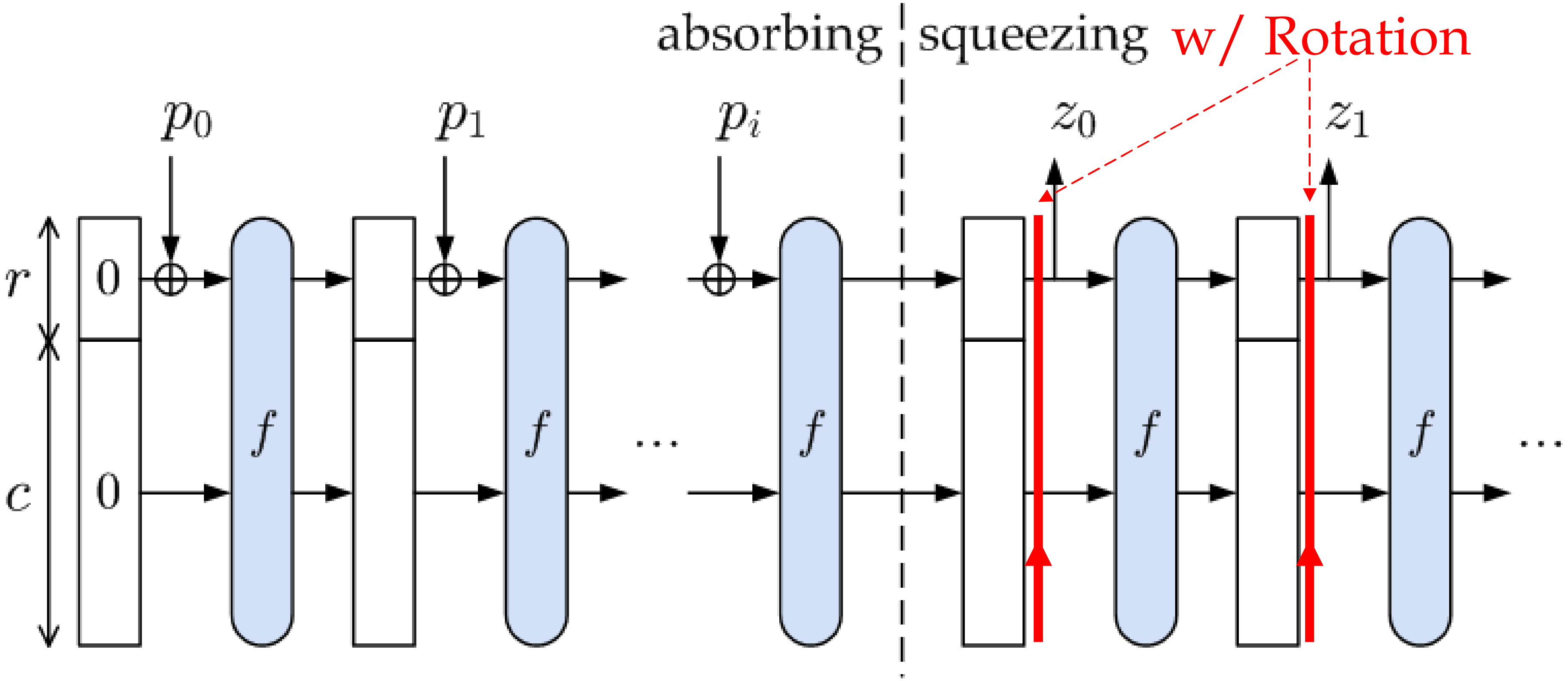
# Sponge construction



© Keccak Team

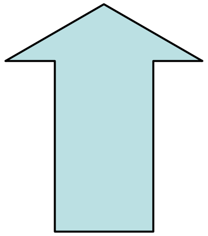
http://sponge.noekeon.org/

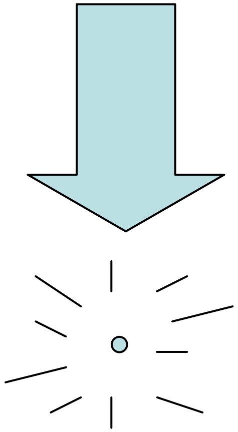
# Mop construction



© Ketchup Team

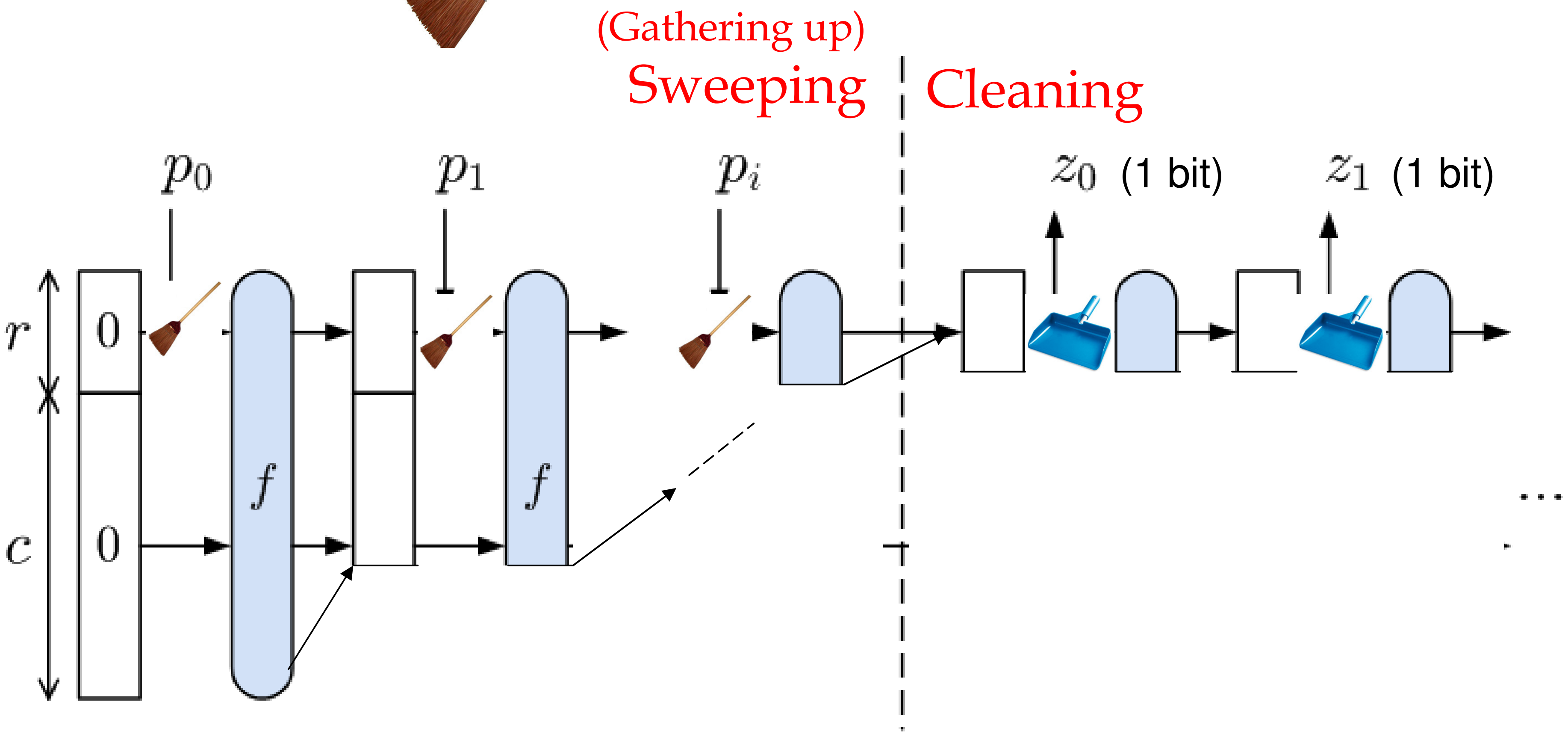
# Broom and Dustpan





Sweeping -then-

# Broom construction



© Ketchup Team

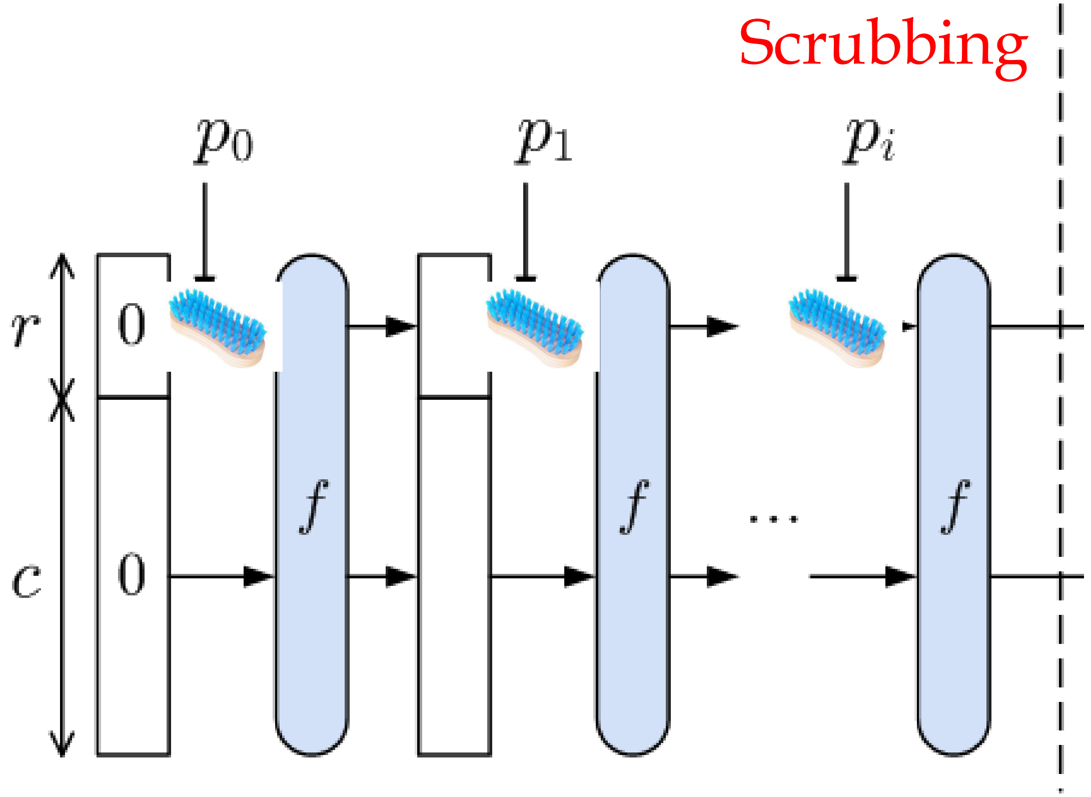
# Scrubbing Brush

Scrubbing -then- ?

# Scrubbing Brush

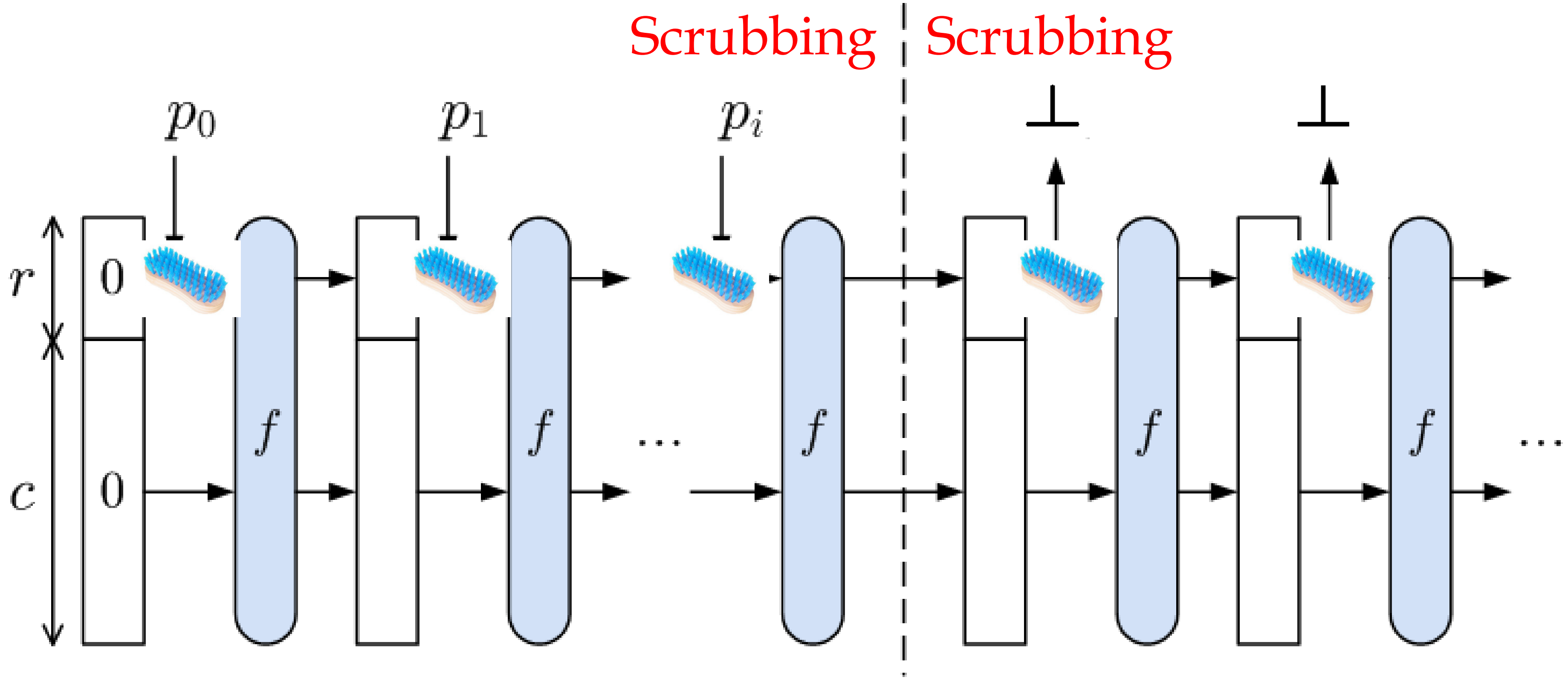
Scrubbing -then- Scrubbing

# Brush construction



© Ketchup Team

# Brush construction

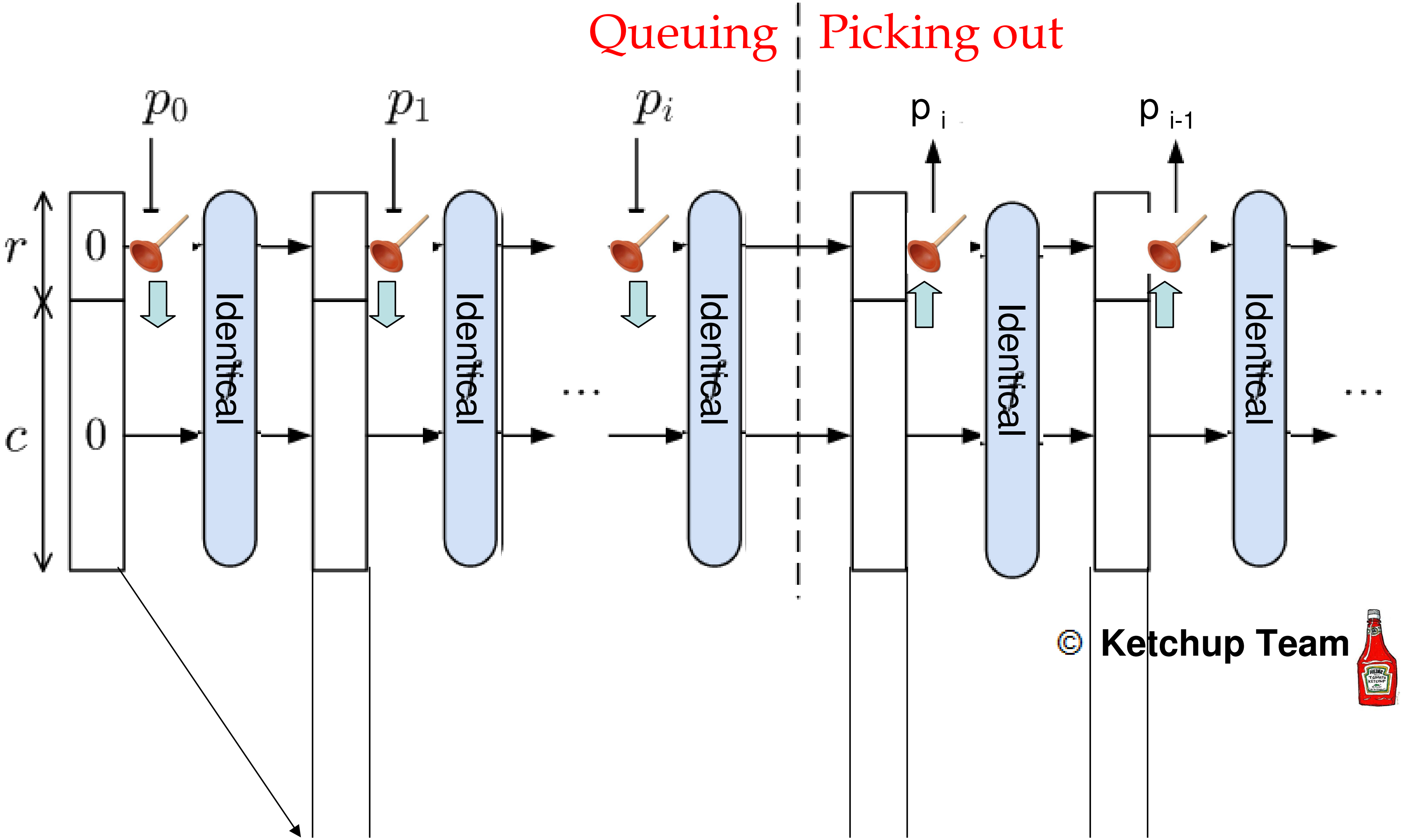


© Ketchup Team

# Sink Plunger

Queuing -then- Picking out

# Plunger construction



# Conclusion

- I know a sponge is the best.

- Future works
  - Window squeezer  and …
  - Kitchen items

# Conclusion

- I know a sponge is the best.

- Future works
  - Window squeezer and …
  - Kitchen items

Join us!

© Ketchup Team