Post-quantum security of the sponge construction

Andreas Hülsing

Based on joined work with Jan Czajkowski, Christian Schaffner, Leon Groot Bruinderink, Dominique Unruh

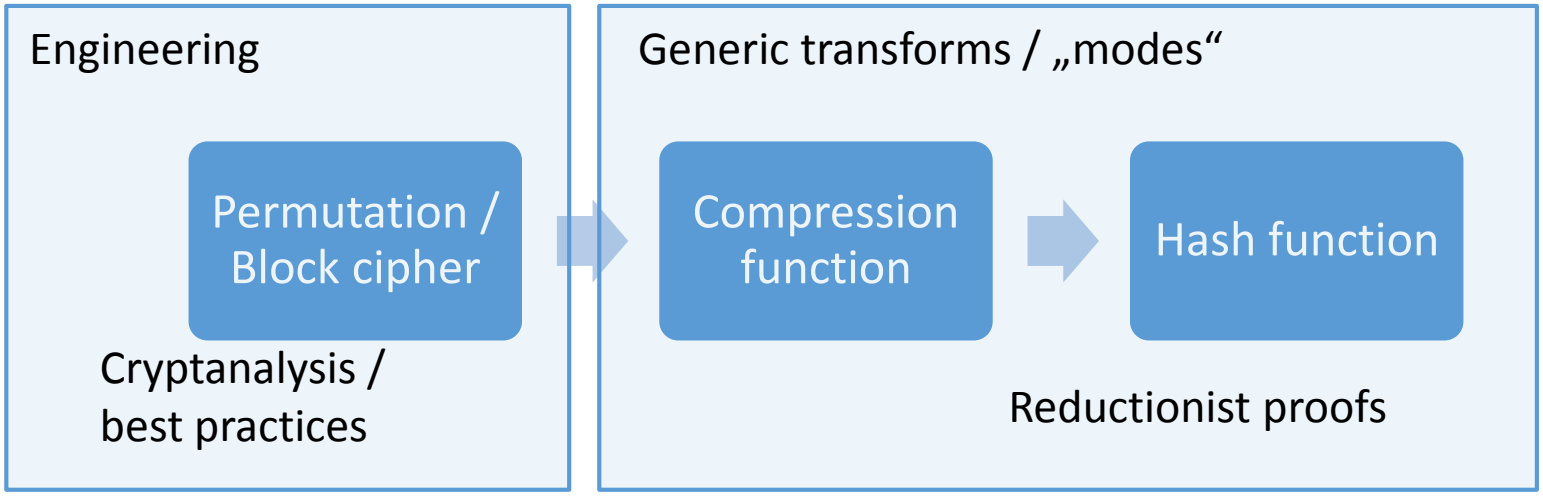
Post-quantum security of hash functions

- Hashes ubiquitous in public key crypto
- Public function -> Adversary can run on quantum computer
- Believe: Grover is best adversary can do
  - True if hash behaves like random function (Zhandry‘15, Hülsing, Rijneveld, Song ‘16)
- What if hash has structure?
- What if classical properties do not suffice?

What if hash has structure?

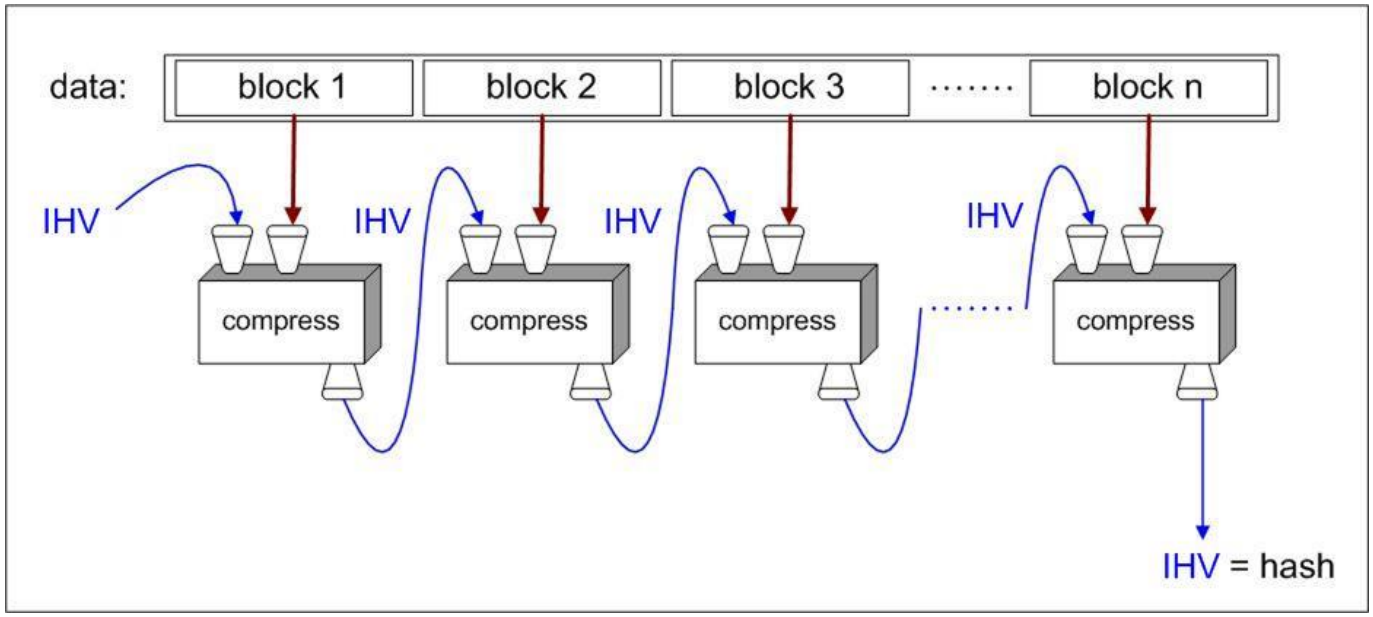
Hash function design

- Create fixed input size building block
- Use building block to build compression function
- Use „mode“ for length extension

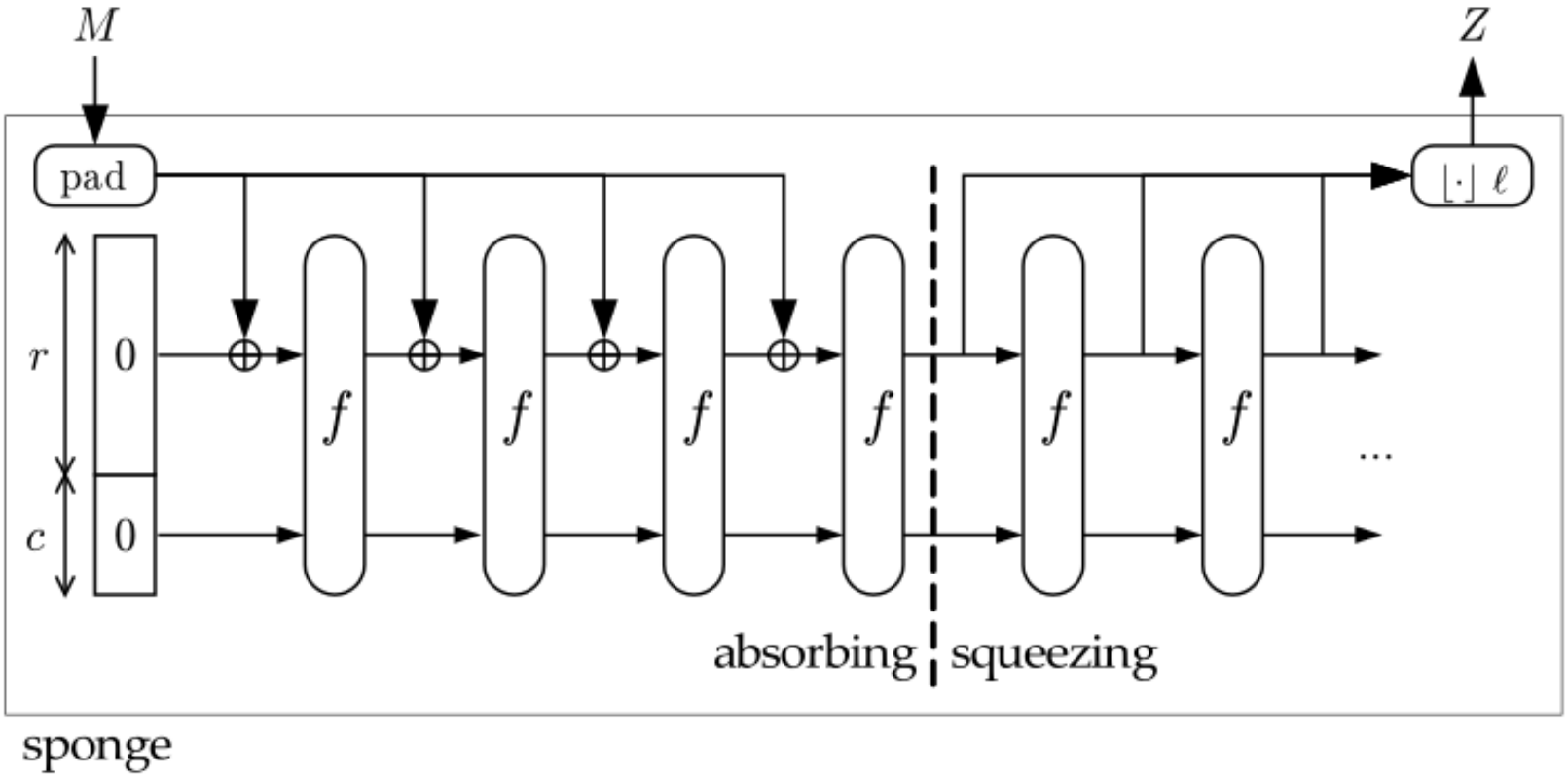


SHA2: Most classical results carry over

(CR / OW) compression function ⇒ (CR / OW) Hash



SHA3: Classical result fails in quantum setting



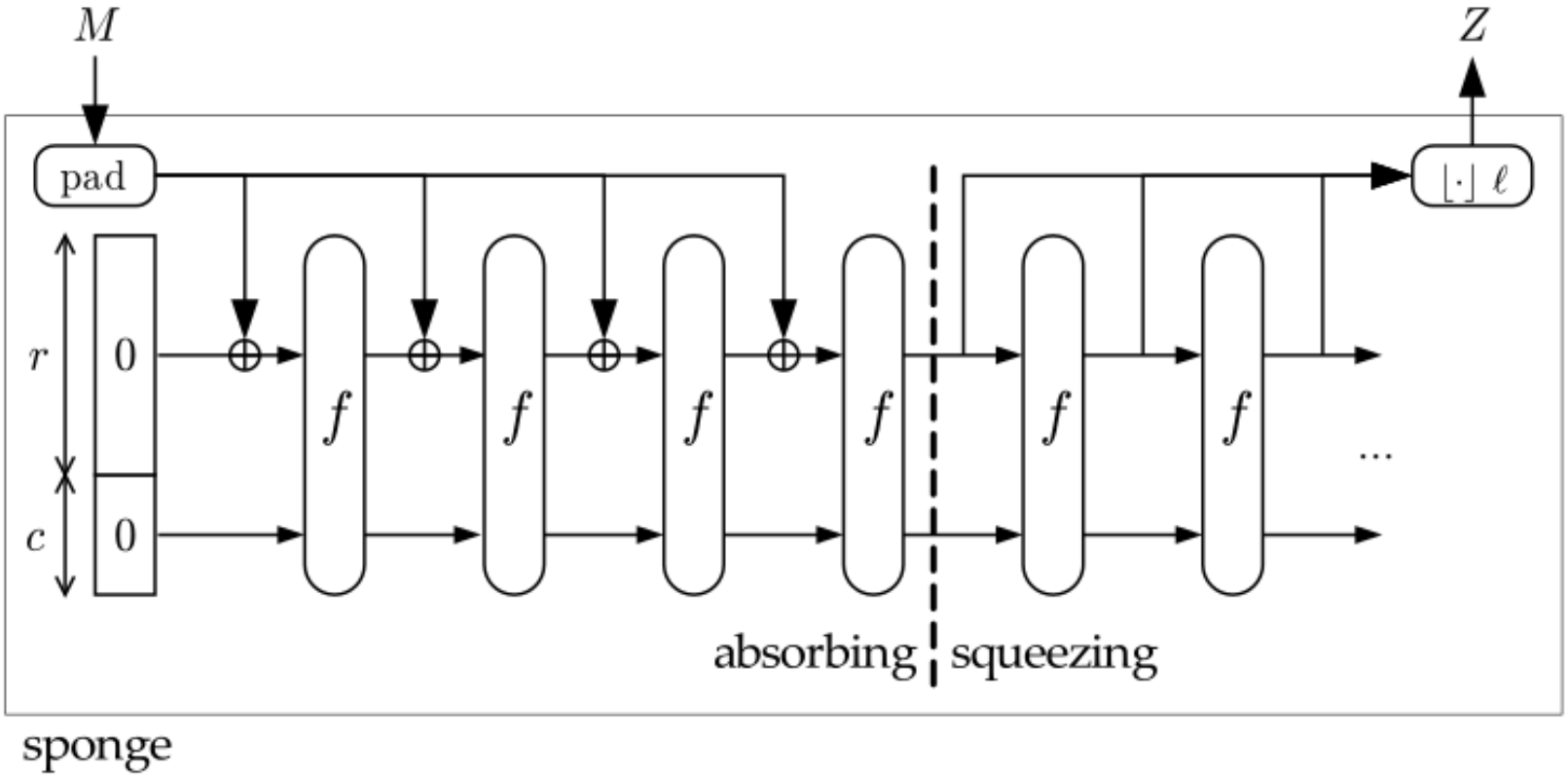
Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche. Cryptographic Sponge Functions. 2007

SHA3: Classical result fails in quantum setting

Theorem ([BDPV07] Informally):
If f is a random permutation or transformation, the expected complexity for differentiating a sponge S_f from a random oracle is $\boldsymbol{\mathcal{O}(2^{c/2})}$.

- Proof inherently query based.
- Proof requires knowledge of queries to S_f.

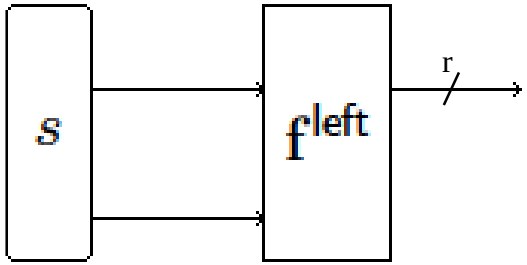
SHA3: Classical result fails in quantum setting

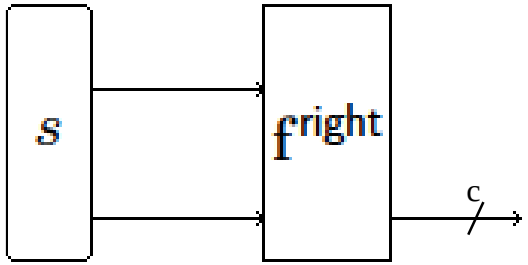


Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche. Cryptographic Sponge Functions. 2007

SHA3: Classical result fails in quantum setting

Note: If f is random permutation, f is not one-way, $f(s \oplus (x||0^c))$ is not collision resistant, and f^{left} and f^{right} are neither one-way nor collision-resistant. (If adversary gets access to f^{-1})

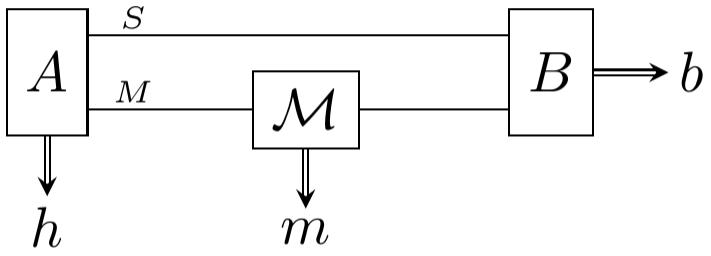




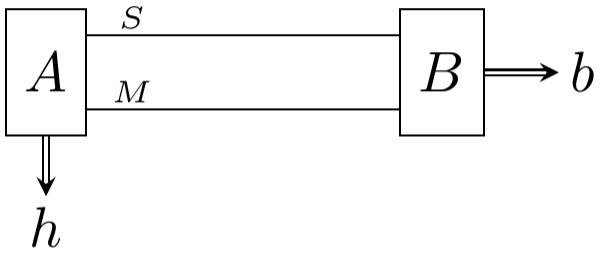
What if classical properties do not suffice?

Collapsing (Unruh, 2016)

- Quantum version of collision resistance
- Example: collapse-binding commitments



(a) – Game_1



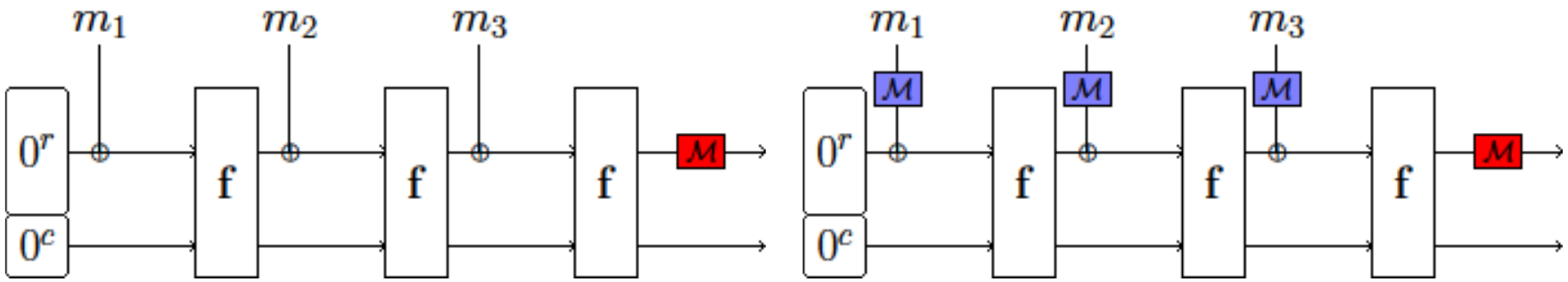
(b) – Game_2

$$\forall (A, B) - \textit{quantum PPT adversary}:$$
$$|Pr[b = 1 : Game1] - Pr[b = 1 : Game2]| \approx 0$$

Results (http://ia.cr/2017/771)

- Proofs for sponges if block function f is **random function or random <u>one-way</u> permutation** (does not cover SHA3!).
- **Collision-resistance** from collision-resistance and zero-preimage resistance of f^{left} and f^{right}
- **Collapsing** from collapsing and zero-preimage resistance of f^{left} and f^{right}.
- Quantum attack that meets lower bounds.

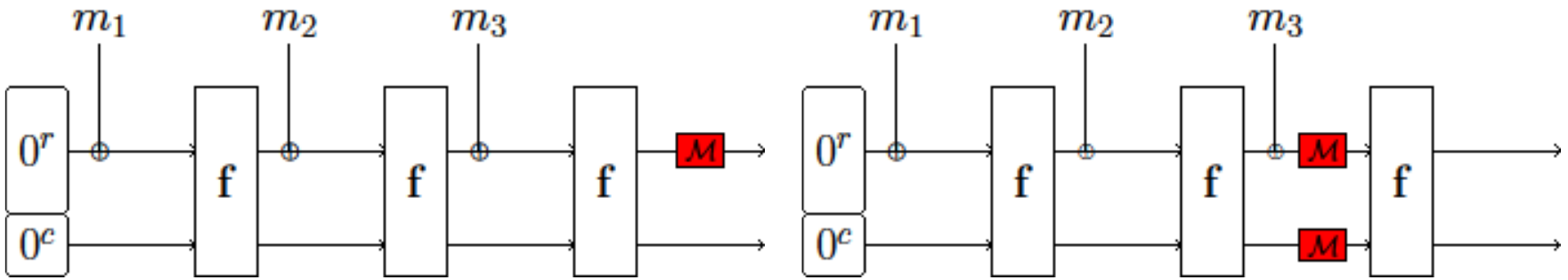
Collapsing Proof (Intuition)



Game$_2$ Game$_1$

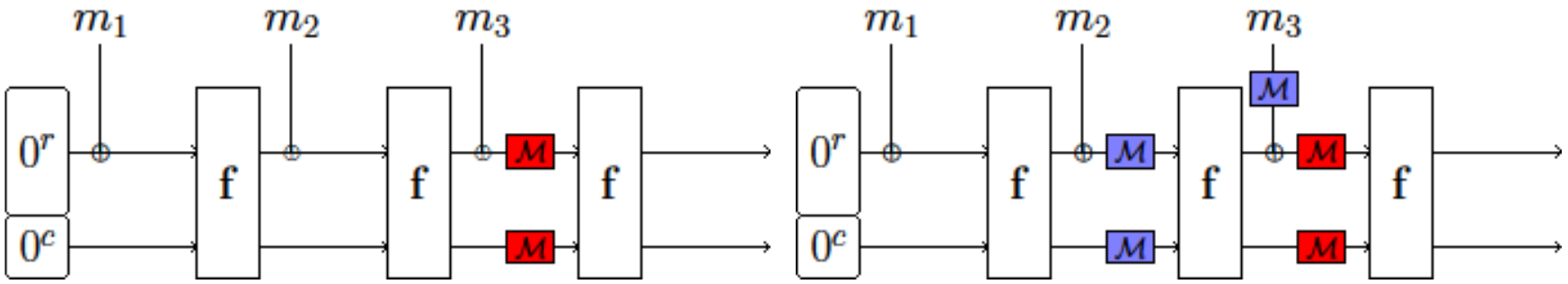
- Hybrid argument
- Omitted here: Have to deal with preimages of 0^c

Collapsing Proof (Intuition)



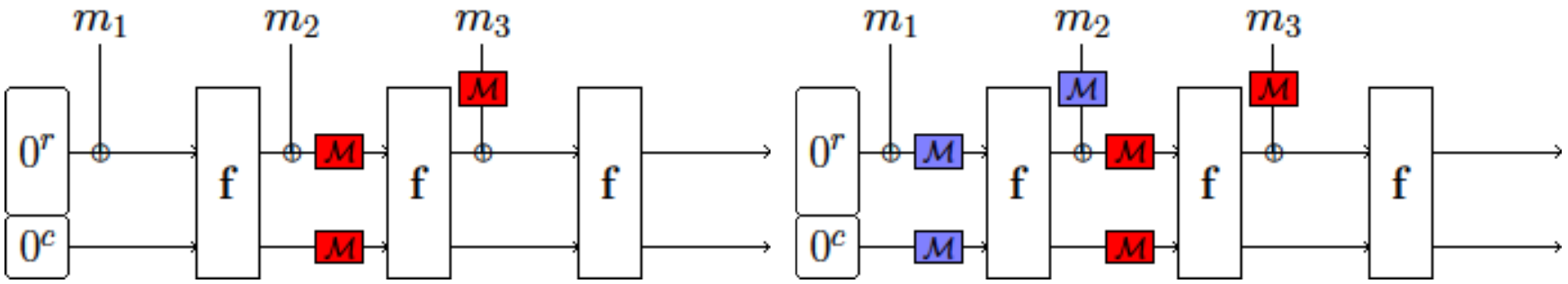
Game$_2$ $\approx$ Collapsing of f^{left} Hyb$_1$

Collapsing Proof (Intuition)



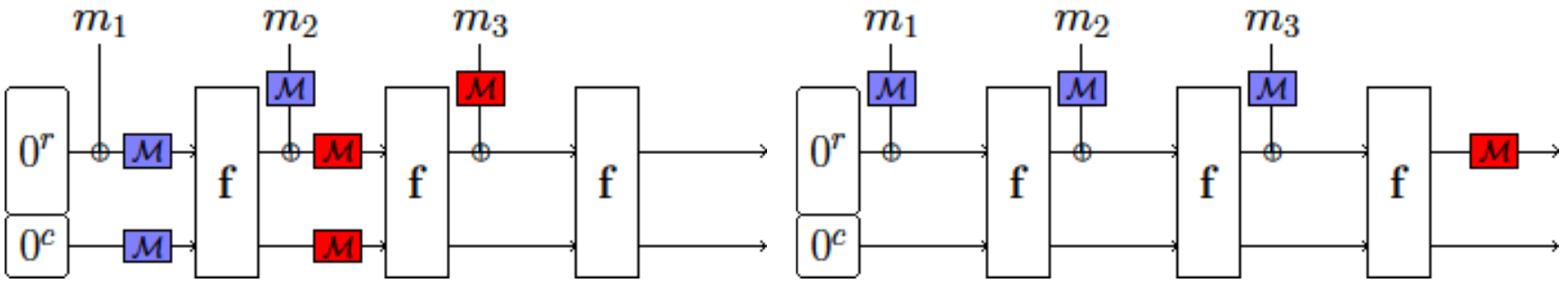
Hyb$_1$ $\approx$ Collapsing of f^{right} Hyb$_2$

Collapsing Proof (Intuition)



Hyb_2 Hyb_3

Collapsing Proof (Intuition)



Hyb$_3$

$\approx$

Collapsing of f^{right}
& Zero-preimage
resistance of f^{right}

Game$_1$

Careful: This gives the misleading impression that all messages in superposition are of equal length!

Thank you!
Questions?