Post-quantum Security of the Sponge Construction

Jan Czajkowski, **Leon Groot Bruinderink**, Andreas Hülsing, Christian Schaffner, and Dominique Unruh

April 10th, 2018

Post-Quantum Cryptography

- Search for cryptography secure against quantum adversaries
  - Public-key (based on new problems)
  - Symmetric-key (double security parameter)

Post-Quantum Cryptography

- Search for cryptography secure against quantum adversaries
  - Public-key (based on new problems)
  - Symmetric-key (double security parameter)
- **Are models, constructions and proofs still sound in the post-quantum setting?**

Motivation

- Imagine a commitment scheme using hash function H

Canonical Commitment Scheme

1. $r \xleftarrow{\$} R$
2. Commit to $h = H(x||r)$
3. Open by giving $x||r$

Motivation

- Imagine a commitment scheme using hash function H

Canonical Commitment Scheme

1. $r \xleftarrow{\$} R$
2. Commit to $h = H(x||r)$
3. Open by giving $x||r$

- Binding: cannot come up with two different openings to the same commitment

Motivation

- Imagine a commitment scheme using hash function H

Canonical Commitment Scheme

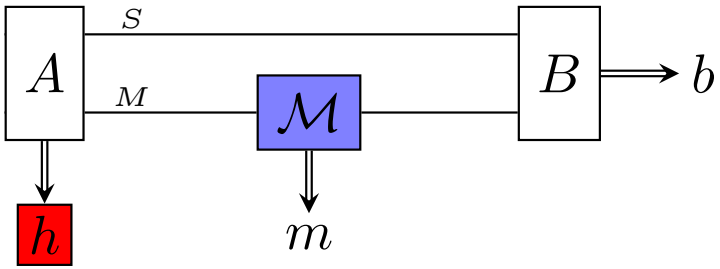
1. $r \xleftarrow{\$} R$
2. Commit to $h = H(x||r)$
3. Open by giving $x||r$

- Binding: cannot come up with two different openings to the same commitment
- Post-quantum we need something stronger[1]: **collapse binding**

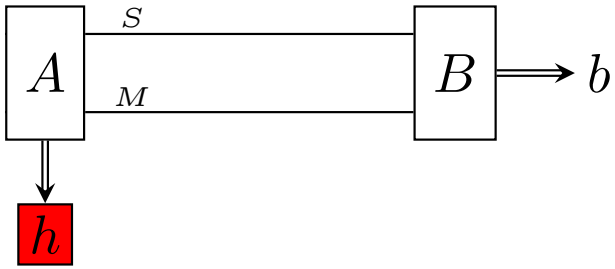
[1] D. Unruh - Computationally binding quantum commitments [Eurocrypt 2016]

Collapsing functions

- Adversary (A, B) has quantum oracle access to H



(a) – Game_1

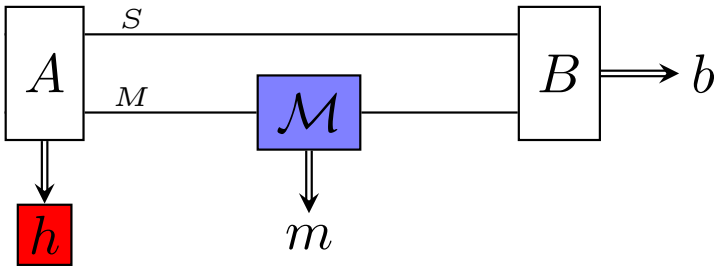


(b) – Game_2

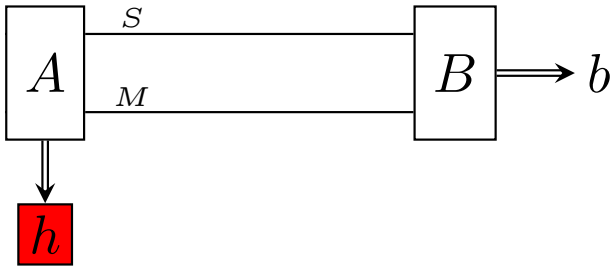
- In Game_2, B receives $M = |\phi\rangle = \sum_{\substack{m \\ H(m)=h}} \alpha_m |m\rangle$
- In Game_1, B receives $M = |m\rangle$ with probability $|\alpha_m|^2$
- Purely a quantum definition!

Collapsing functions

- Adversary (A, B) has quantum oracle access to H



(a) – Game_1

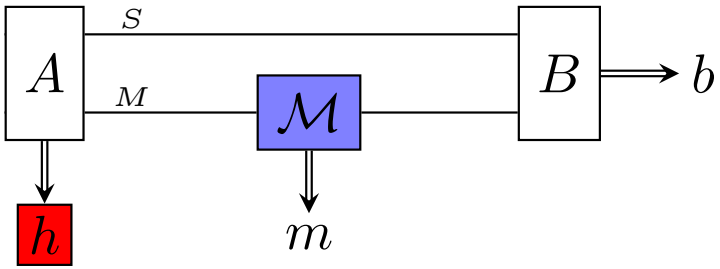


(b) – Game_2

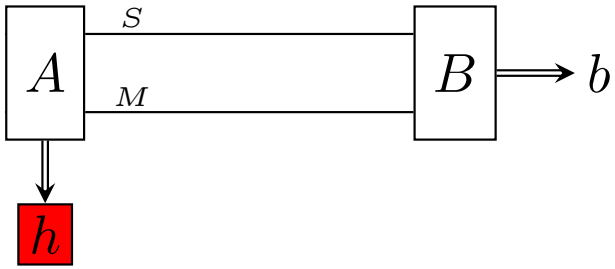
- H collapsing iff $\mathbb{P}[b = 1 : \mathrm{Game}_1] \approx \mathbb{P}[b = 1 : \mathrm{Game}_2]$
- Intuitively: register M can be measured without (A, B) noticing

Collapsing functions

- Adversary (A, B) has quantum oracle access to H



(a) – Game_1

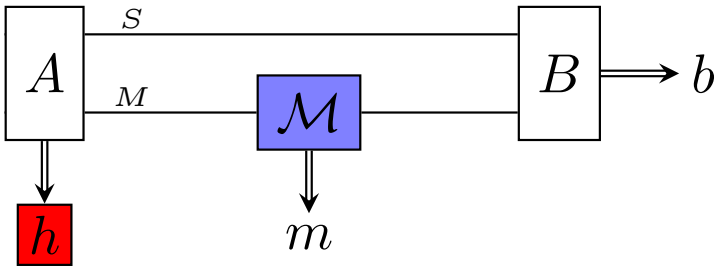


(b) – Game_2

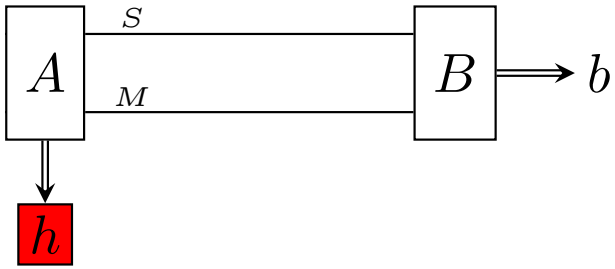
- Easy example: injective functions are collapsing, as:
  - In Game_1: B receives $M = |m\rangle$ as it is measured

Collapsing functions

- Adversary (A, B) has quantum oracle access to H



(a) – Game_1

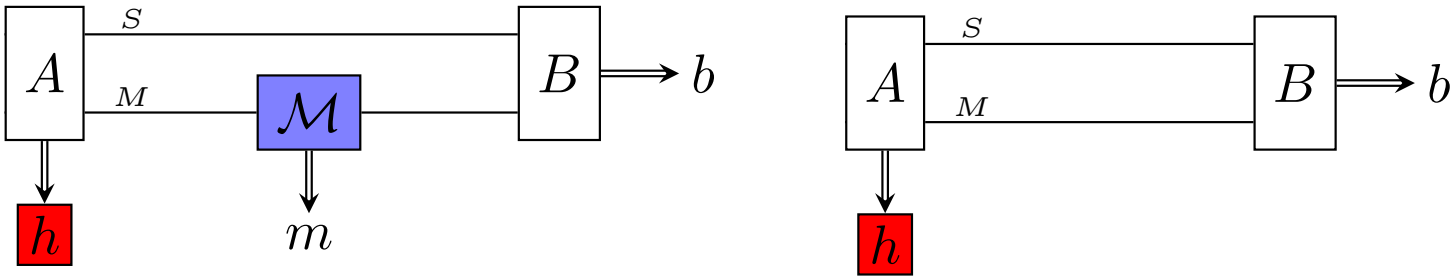


(b) – Game_2

- Easy example: injective functions are collapsing, as:
  - In Game_1: B receives $M = |m\rangle$ as it is measured
  - Similar, Game_2: $M = |m\rangle$ as there is only one $m : H(m) = h$

Collapsing functions

- Adversary (A, B) has quantum oracle access to H



(a) – Game_1 (b) – Game_2

- Easy example: injective functions are collapsing, as:
  - In Game_1: B receives $M = |m\rangle$ as it is measured
  - Similar, Game_2: $M = |m\rangle$ as there is only one $m : H(m) = h$
- More interesting example: random oracles

Collapsing implies Collision Resistance

- Proof by contradiction: suppose algorithm P can find collisions in H

Collapsing implies Collision Resistance

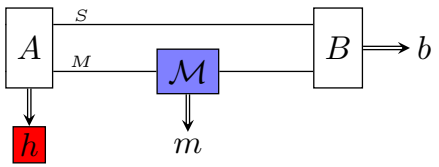
- Proof by contradiction: suppose algorithm P can find collisions in H
- Algorithm A does the following:
  - Let P find m_1, m_2 with $H(m_1) = H(m_2) = h$
  - A outputs h and sends $M = |\phi\rangle = \frac{1}{\sqrt{2}}(|m_1\rangle + |m_2\rangle)$ and $S = (m_1, m_2)$ to B

Collapsing implies Collision Resistance

- Proof by contradiction: suppose algorithm P can find collisions in H
- Algorithm A does the following:
  - Let P find m_1, m_2 with $H(m_1) = H(m_2) = h$
  - A outputs h and sends $M = |\phi\rangle = \frac{1}{\sqrt{2}}(|m_1\rangle + |m_2\rangle)$ and $S = (m_1, m_2)$ to B
- Algorithm B does the following:
  - B receives S, M and measures wether M contains $|\phi\rangle$
  - If the measurement succeeds, he outputs 1 and 0 otherwise

Collapsing implies Collision Resistance

- Proof by contradiction: suppose algorithm P can find collisions in H
- Algorithm A does the following:
  - Let P find m_1, m_2 with $H(m_1) = H(m_2) = h$
  - A outputs h and sends $M = |\phi\rangle = \frac{1}{\sqrt{2}}(|m_1\rangle + |m_2\rangle)$ and $S = (m_1, m_2)$ to B
- Algorithm B does the following:
  - B receives S, M and measures wether M contains $|\phi\rangle$
  - If the measurement succeeds, he outputs 1 and 0 otherwise

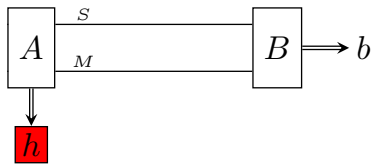


(a) – Game_1

- In Game_1, M collapses to one of the states so $\mathbb{P}[b = 1 : \text{Game}_1] = \frac{1}{2}$

Collapsing implies Collision Resistance

- Proof by contradiction: suppose algorithm P can find collisions in H
- Algorithm A does the following:
  - Let P find m_1, m_2 with $H(m_1) = H(m_2) = h$
  - A outputs h and sends $M = |\phi\rangle = \frac{1}{\sqrt{2}}(|m_1\rangle + |m_2\rangle)$ and $S = (m_1, m_2)$ to B
- Algorithm B does the following:
  - B receives S, M and measures wether M contains $|\phi\rangle$
  - If the measurement succeeds, he outputs 1 and 0 otherwise



(b) – Game_2

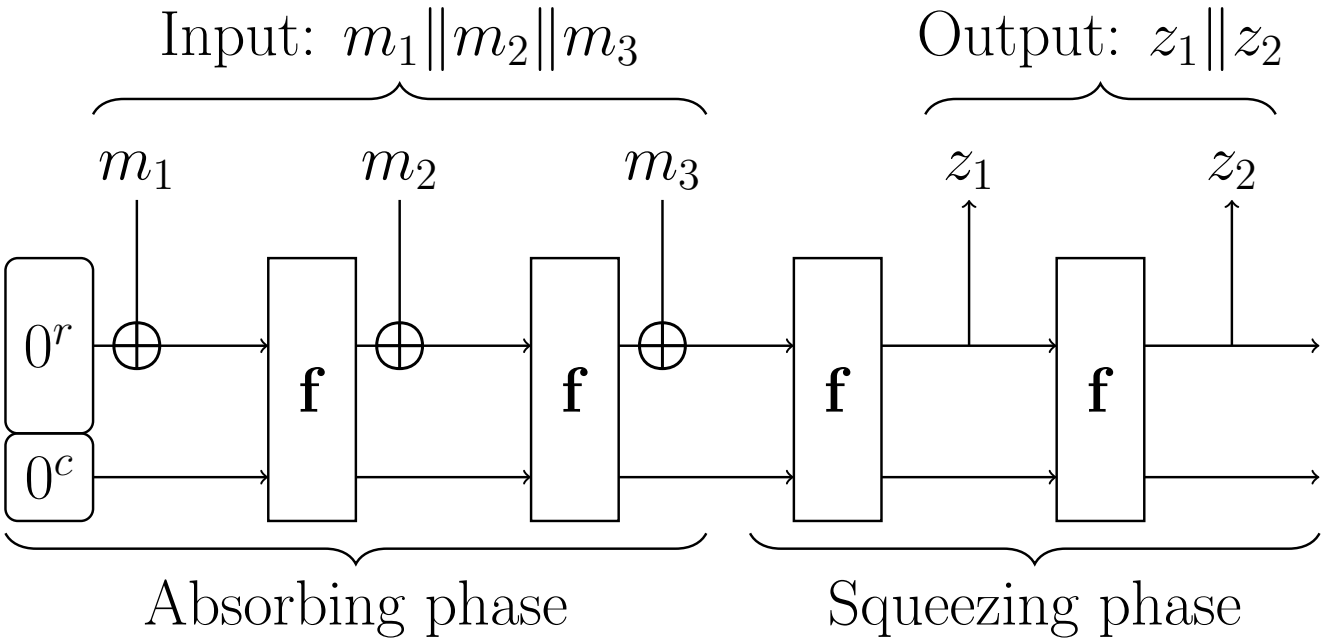
- In Game_1, M collapses to one of the states so $\mathbb{P}[b = 1 : \text{Game}_1] = \frac{1}{2}$
- In Game_2, M stays $|\phi\rangle$ so $\mathbb{P}[b = 1 : \text{Game}_2] = 1$

Hash functions

- Hash-functions: virtually used everywhere
- Post-quantum we want hash-functions to be collapsing
- Unruh[2] showed Merkle-Damgard is collapsing (SHA2)
- What about other constructions for hash-functions?

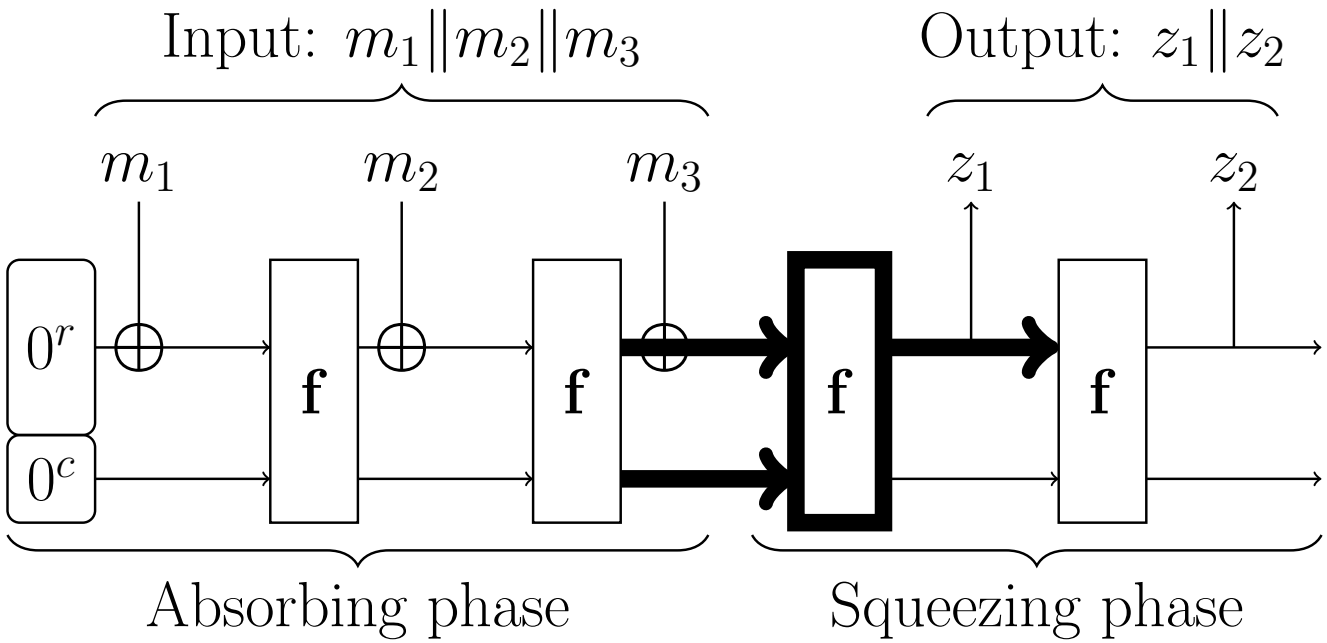
[2] D. Unruh - Collapse-binding quantum commitments without random oracles [Asiacrypt 2016]

Sponge construction



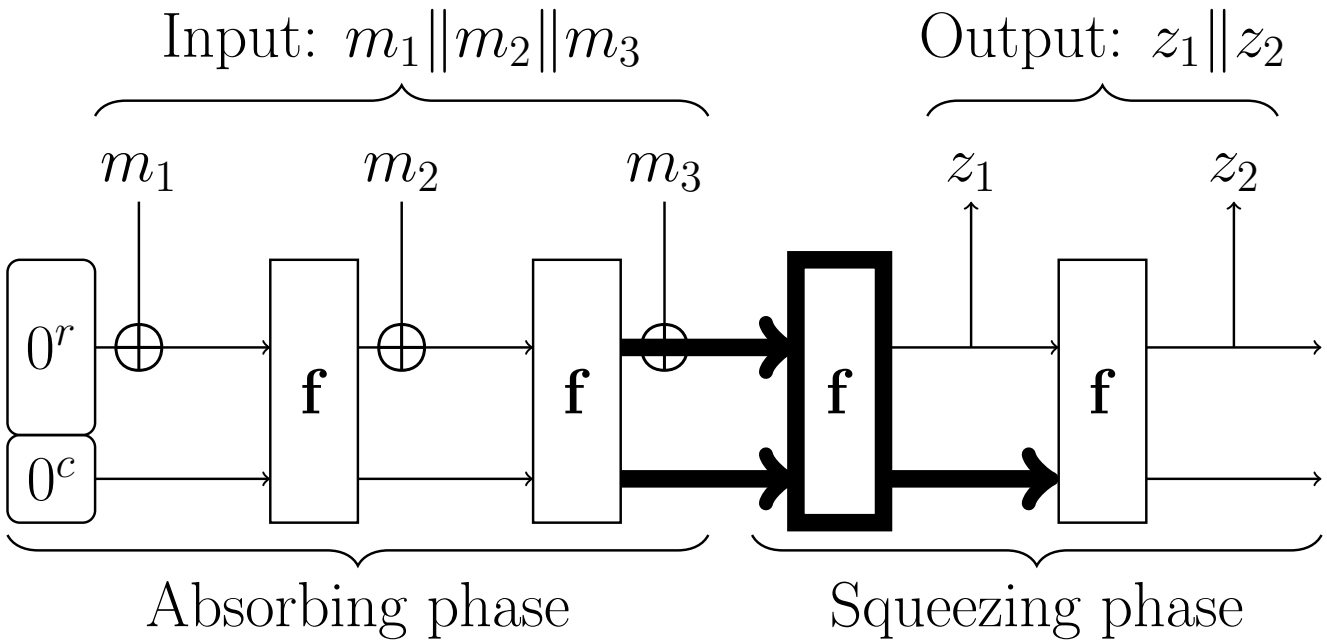
- For example Keccak(SHA3)

Sponge construction



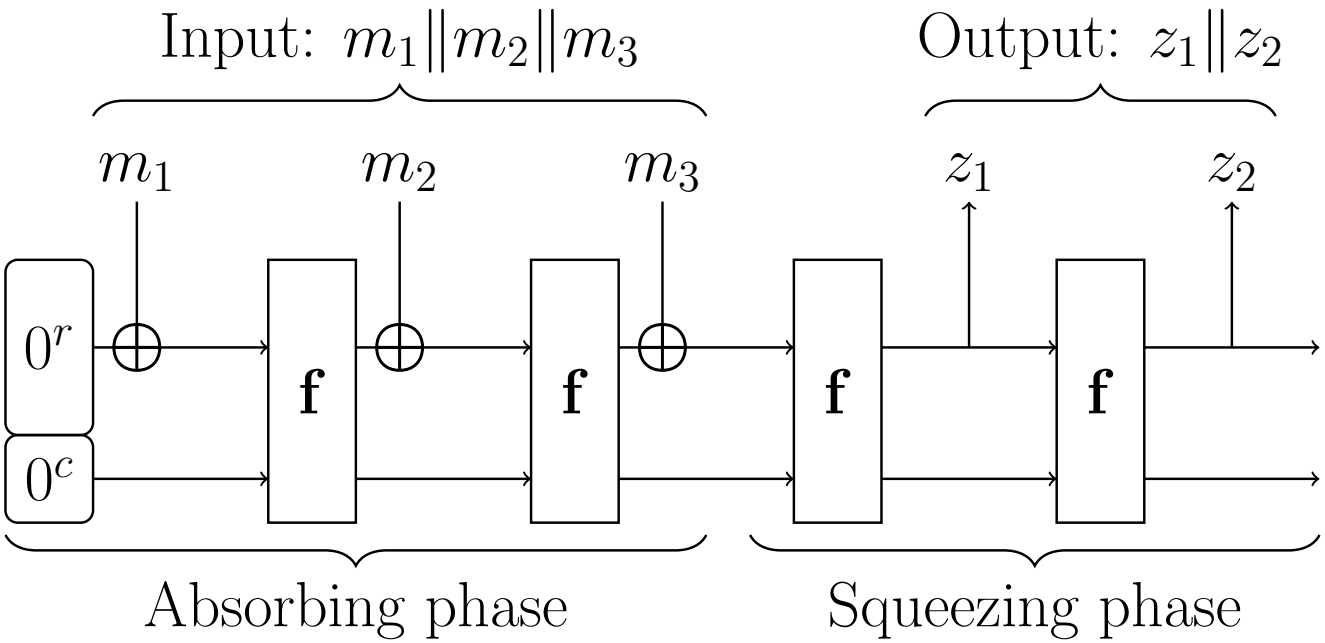
- Internal block-function $\mathbf{f} := \mathbf{f}^{\text{left}} ||$

Sponge construction



- Internal block-function $\mathbf{f} := \mathbf{f}^{\text{left}} || \mathbf{f}^{\text{right}}$

Sponge construction



- Internal block-function $\mathbf{f} := \mathbf{f}^{\text{left}} || \mathbf{f}^{\text{right}}$ with $\mathbf{f}^{\text{left}} : \{0,1\}^{r+c} \to \{0,1\}^r$, $\mathbf{f}^{\text{right}} : \{0,1\}^{r+c} \to \{0,1\}^c$

This work

- We show that the sponge construction is collapsing (but not SHA3)

This work

- We show that the sponge construction is collapsing (but not SHA3)
- We show that the sponge construction is collision resistant in the quantum adversary model
- We give a quantum algorithm for finding collisions in any function, in particular the sponge construction

This work

- We show that the sponge construction is collapsing $\leftarrow$ **This talk**
- We show that the sponge construction is collision resistant in the quantum adversary model
- We give a quantum algorithm for finding collisions in any function, in particular the sponge construction

Requirements on internal block-function

- We only want to make assumptions on $\mathbf{f}$
- Can write sponge as $\mathbf{S} = (\mathbf{S}^{out} \circ \mathbf{S}^{in}) \circ pad$

Requirements on internal block-function

- We only want to make assumptions on $\mathbf{f}$
- Can write sponge as $\mathbf{S} = (\mathbf{S}^{out} \circ \mathbf{S}^{in}) \circ pad$
- pad is injective, thus it is collapsing

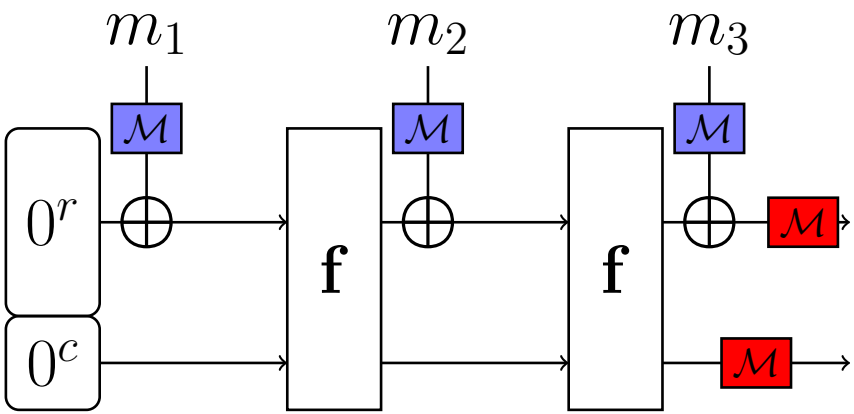
Requirements on internal block-function

- We only want to make assumptions on $\mathbf{f}$
- Can write sponge as $\mathbf{S} = (\mathbf{S}^{out} \circ \mathbf{S}^{in}) \circ pad$
- pad is injective, thus it is collapsing
- If g, h are collapsing, so is $g \circ h$

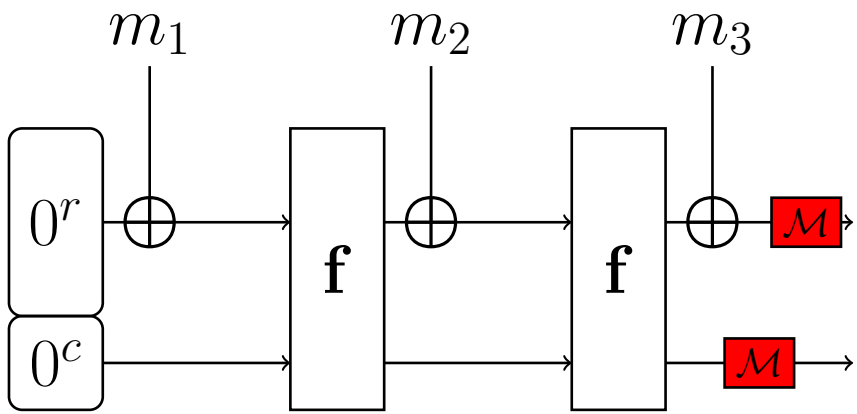
Requirements on internal block-function

- We only want to make assumptions on $\mathbf{f}$
- Can write sponge as $\mathbf{S} = (\mathbf{S}^{out} \circ \mathbf{S}^{in}) \circ pad$
- pad is injective, thus it is collapsing
- If g, h are collapsing, so is $g \circ h$
- To show: $\mathbf{S}^{out}$ and $\mathbf{S}^{in}$ collapsing
- Next: proof sketch for collapsing of $\mathbf{S}^{in}$

Proof sketch $\mathbf{S}^{in}$ collapsing



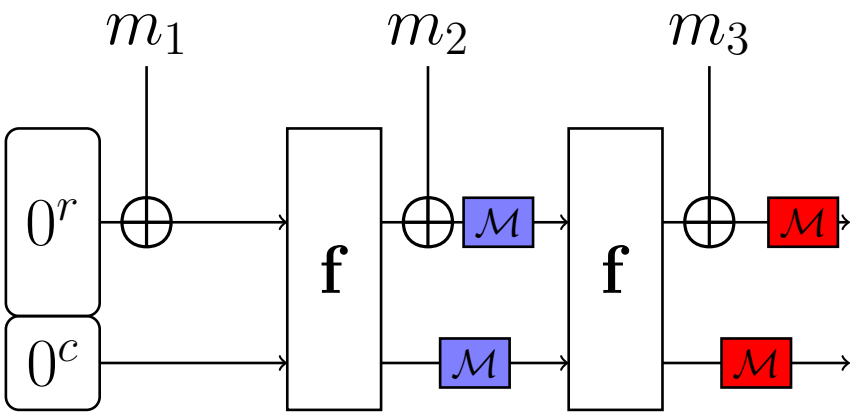
(a) $\mathrm{Game}_1 = \mathrm{Hyb}_1$



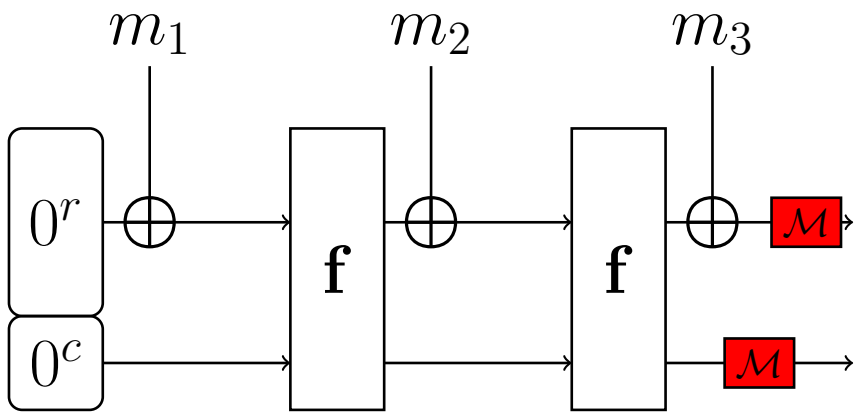
(b) $\mathrm{Game}_2 = \mathrm{Hyb}_4$

- Hybrid argument: subsequently measure more using properties of $\mathbf{f}$

Proof sketch $\mathbf{S}^{in}$ collapsing

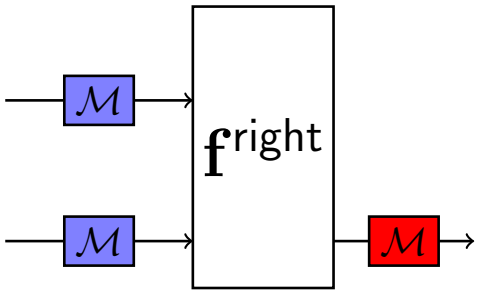


(a) Hyb_3

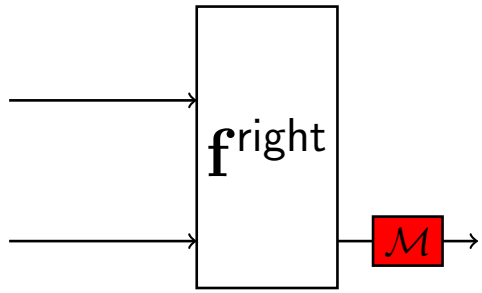


(b) Hyb_4

- Hybrid argument: subsequently measure more using properties of $\mathbf{f}$
- Collapsing games for $\mathbf{f}^{\mathrm{right}}$

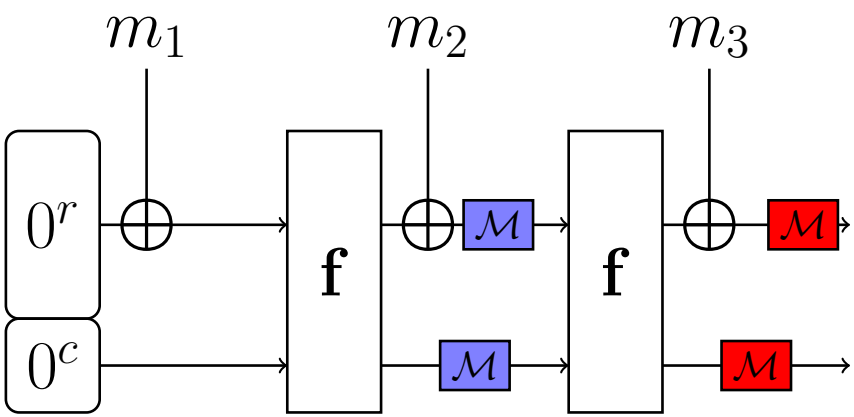


(c) Game_1

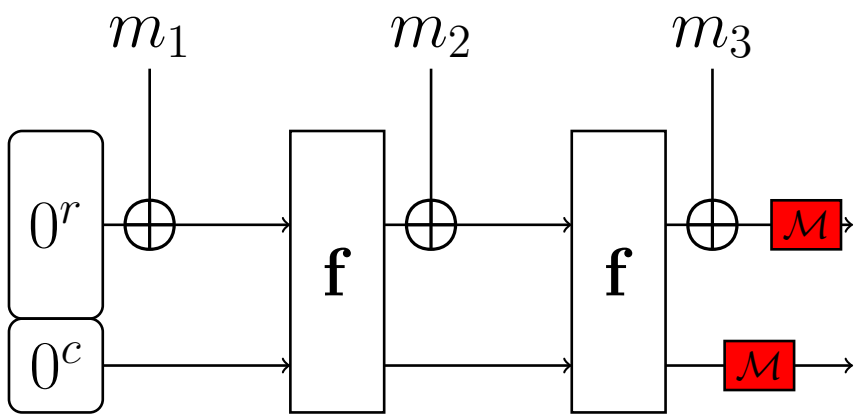


(d) Game_2

Proof sketch $\mathbf{S}^{in}$ collapsing

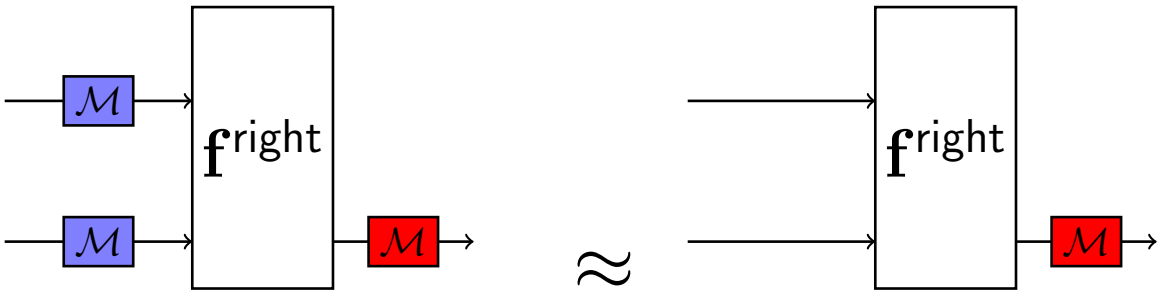


(a) Hyb_3



(b) Hyb_4

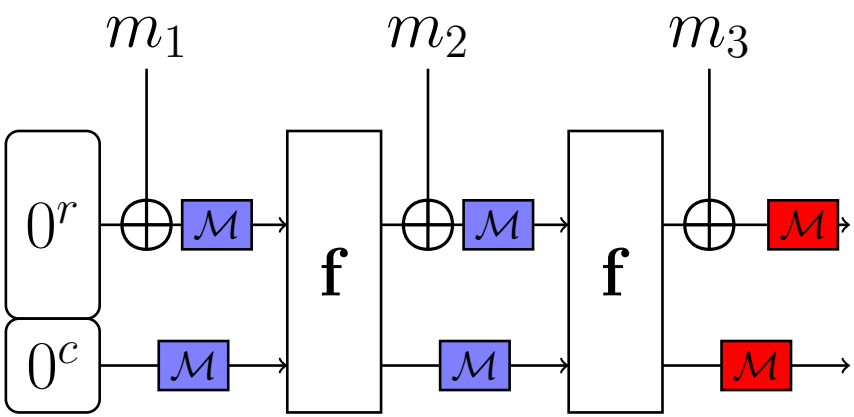
- Required property: $\mathbf{f}^{\mathrm{right}}$ collapsing



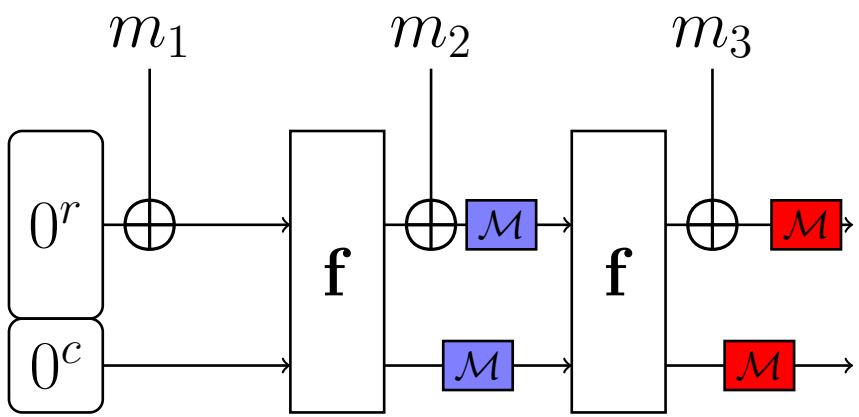
(c) Game_1 (d) Game_2

- $\mathbb{P}[b = 1 : \mathrm{Hyb}_3] \approx \mathbb{P}[b = 1 : \mathrm{Hyb}_4]$

Proof sketch $\mathbf{S}^{in}$ collapsing

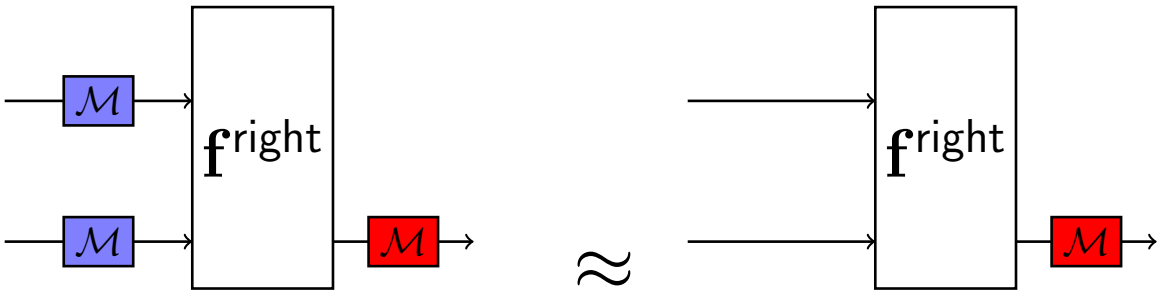


(a) Hyb_2



(b) Hyb_3

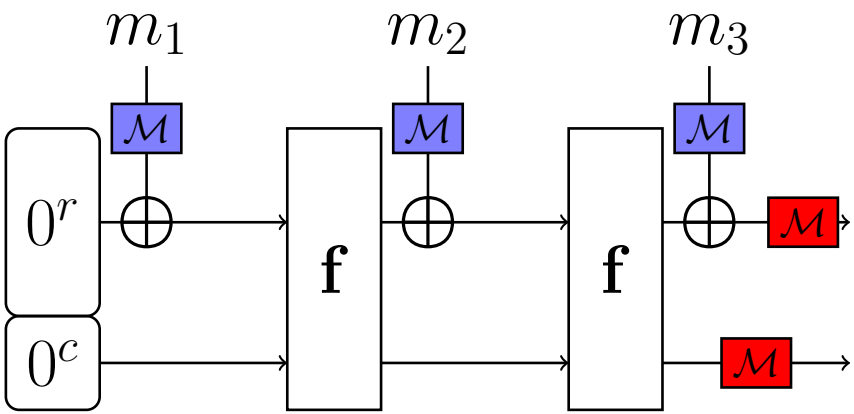
- Required property: $\mathbf{f}^{\mathrm{right}}$ collapsing



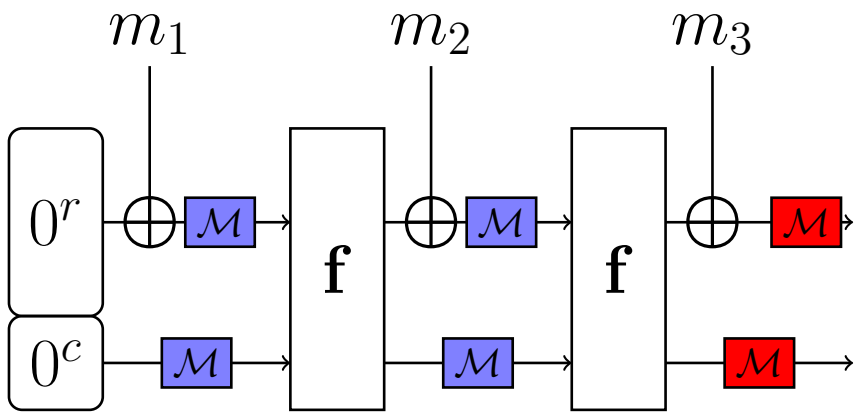
(c) Game_1 (d) Game_2

- $\mathbb{P}[b = 1 : \mathrm{Hyb}_2] \approx \mathbb{P}[b = 1 : \mathrm{Hyb}_3]$

Proof sketch $\mathbf{S}^{in}$ collapsing



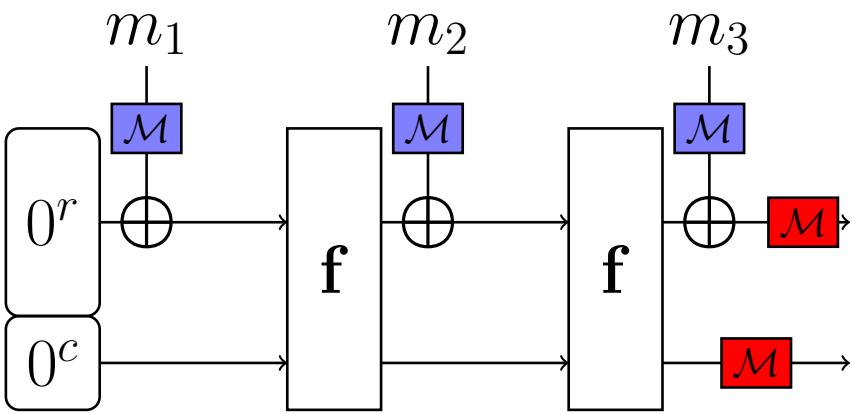
(a) $\mathrm{Game}_1 = \mathrm{Hyb}_1$



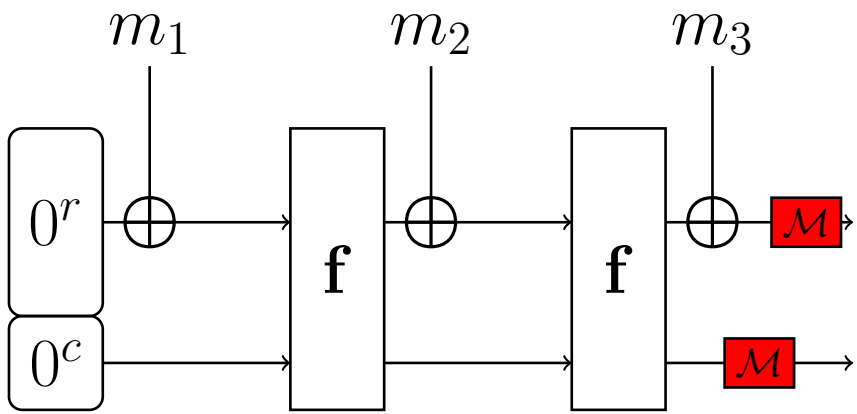
(b) Hyb_2

- $\mathbb{P}[b = 1 : \mathrm{Game}_1] = \mathbb{P}[b = 1 : \mathrm{Hyb}_2]$

Proof sketch $\mathbf{S}^{in}$ collapsing



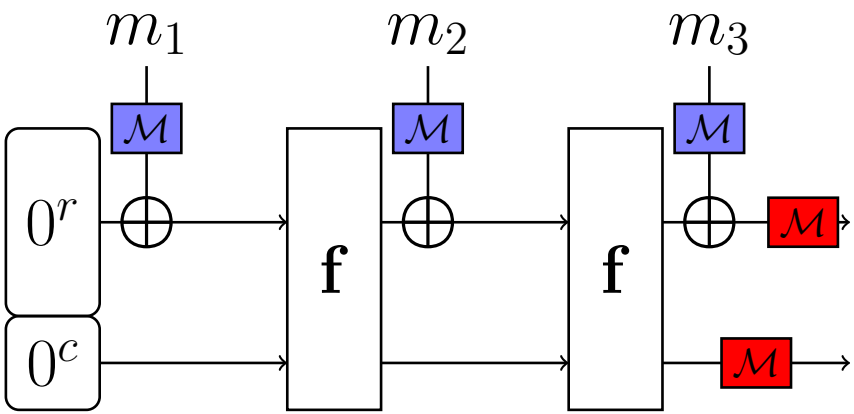
(a) $\mathrm{Game}_1 = \mathrm{Hyb}_1$



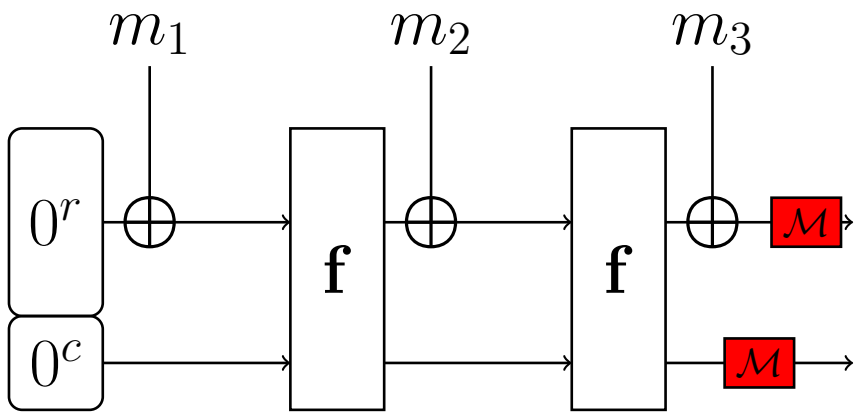
(b) $\mathrm{Game}_2 = \mathrm{Hyb}_4$

- Careful: this gives the misleading impression that all messages in superposition are of equal length
- Additional requirement: $\mathbf{f}^{\mathrm{right}}$ zero-preimage resistant

Proof sketch $\mathbf{S}^{in}$ collapsing



(a) $\mathrm{Game}_1 = \mathrm{Hyb}_1$



(b) $\mathrm{Game}_2 = \mathrm{Hyb}_4$

- Concluding: $\mathbb{P}[b = 1 : \mathrm{Game}_1] \approx \mathbb{P}[b = 1 : \mathrm{Game}_2]$ if $\mathbf{f}^{\mathrm{right}}$ collapsing and zero-preimage-resistant

The sponge construction is collapsing

- We have shown that $\mathbf{S}^{in}$ is collapsing if $\mathbf{f}^{\mathrm{right}}$ collapsing and zero-preimage-resistant

The sponge construction is collapsing

- We have shown that $\mathbf{S}^{in}$ is collapsing if $\mathbf{f}^{\mathrm{right}}$ collapsing and zero-preimage-resistant
- If $\mathbf{f}^{\mathrm{left}}$ is collapsing, then $\mathbf{S}^{out}$ collapsing

The sponge construction is collapsing

- We have shown that $\mathbf{S}^{in}$ is collapsing if $\mathbf{f}^{\mathrm{right}}$ collapsing and zero-preimage-resistant
- If $\mathbf{f}^{\mathrm{left}}$ is collapsing, then $\mathbf{S}^{out}$ collapsing
- So in total, $\mathbf{S} = (\mathbf{S}^{out} \circ \mathbf{S}^{in}) \circ \mathit{pad}$ is collapsing

The sponge construction is collapsing, but....

- We have shown that $\mathbf{S}^{in}$ is collapsing if $\mathbf{f}^{\mathrm{right}}$ collapsing and zero-preimage-resistant
- If $\mathbf{f}^{\mathrm{left}}$ is collapsing, then $\mathbf{S}^{out}$ collapsing
- So in total, $\mathbf{S} = (\mathbf{S}^{out} \circ \mathbf{S}^{in}) \circ \mathit{pad}$ is collapsing
- $\mathbf{f}$ has required properties if it is a random function/ **one-way** permutation
- However, Keccak is an efficiently invertible permutation!

The sponge construction is collapsing, but....

- We have shown that $\mathbf{S}^{in}$ is collapsing if $\mathbf{f}^{\text{right}}$ collapsing and zero-preimage-resistant
- If $\mathbf{f}^{\text{left}}$ is collapsing, then $\mathbf{S}^{out}$ collapsing
- So in total, $\mathbf{S} = (\mathbf{S}^{out} \circ \mathbf{S}^{in}) \circ \mathit{pad}$ is collapsing
- $\mathbf{f}$ has required properties if it is a random function/ **one-way** permutation
- However, Keccak is an efficiently invertible permutation! $\rightarrow$ $\mathbf{f}^{\text{left/right}}$ not collapsing nor zero-preimage-resistant

A lot more in the paper!

- Concrete security bounds for collapsing of sponge construction
- Direct proof of collision resistance of sponge construction
- Quantum search algorithm for finding collisions in a sponge, matching lower bound from the proof

A lot more in the paper!

- Concrete security bounds for collapsing of sponge construction
- Direct proof of collision resistance of sponge construction
- Quantum search algorithm for finding collisions in a sponge, matching lower bound from the proof

Thank you for your attention
Questions?