Quantum One-Wayness of the Single Round Sponge with Invertible Permutations

Joseph Carolan[1], Alexander Poremba[2]

1. University of Maryland, 2. MIT

Motivation: SHA3

- International hash standard: SHA3
- SHA3 uses the **sponge** to achieve variable input length

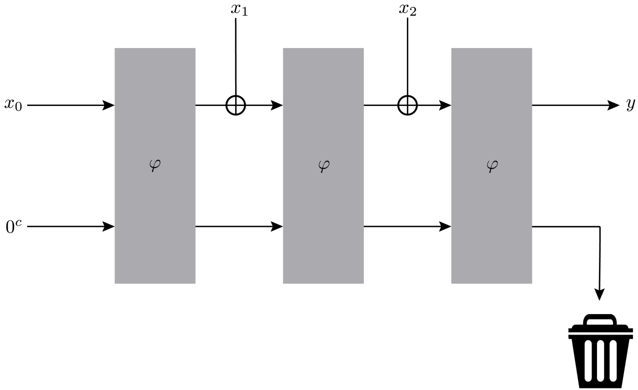


Image credit: https://www.vecteezy.com/free-vector/garbage-can, Garbage Can Vectors by Vecteezy

Sponge Construction

- Based on permutation φ on $\text{RATE} + \text{CAPACITY}$ bits
- Both φ and φ^{-1} have a public description
- Oracles can be implemented given this description:

$$O_\varphi |x\rangle |y\rangle = |x\rangle |y \oplus \varphi(x)\rangle$$
$$O_{\varphi^{-1}} |x\rangle |y\rangle = |x\rangle \left|y \oplus \varphi^{-1}(x)\right\rangle$$

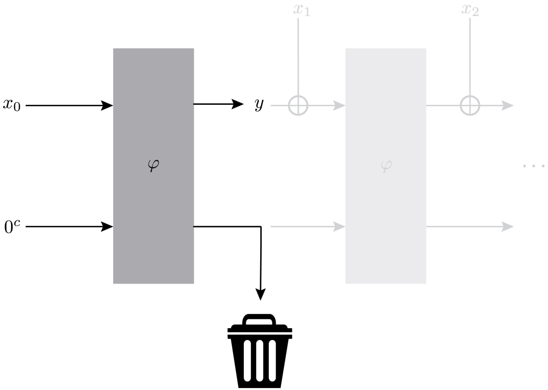
- We model adversaries as having black-box access $O_\varphi, O_{\varphi^{-1}}$
- It is standard to model φ as *random permutations*

Sponge Security

- We then show security in the *Random Permutation Model*
- Strong classical results in this model ("Indifferentiability")
  - ($\rightarrow$) This is the classical theory basis of the Sponge/SHA3
  - ($\rightarrow$) We want a similar basis for quantum security
- Post-quantum security of the sponge is a major open problem
- Very **few quantum results** allowing inverse queries
- Problem: quantum adversaries can query φ and φ^{-1}
  - ($\rightarrow$) No compressed oracle! How to analyze?
  - ($\rightarrow$) In fact, few techniques whatsoever.

Quantum Security of the Sponge

- For simplicity, restrict to one round:



Quantum Security of the Sponge

- Single-round sponge is reset indifferentiable from a random oracle when $\textsc{rate} \leq \textsc{capacity}$ [Zhandry 21]
- "As good as a random oracle" when $\textsc{rate} \leq \textsc{capacity}$
- Problem:

Hash	Rate	Capacity
SHA3-224	1152	448
SHA3-256	1088	512
SHA3-384	832	768
SHA3-512	576	1024

- Reset indifferentiability is *impossible* when $\textsc{rate} > \textsc{capacity}$
- Even when $\textsc{rate} \leq \textsc{capacity}$, known bounds are only super-polynomial (not tight)
- We need **more techniques!**

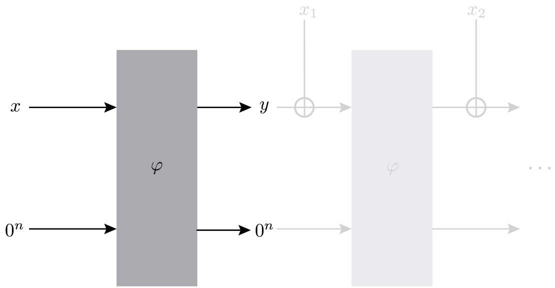
Double Sided Zero Search [Unruh 21, 23]

Problem (DSZS)

In: *Queries to permutation* φ *and* φ^{-1} *on* $2n$ *bits*
Out: *A "zero pair"* (x, y) *s.t.*

$$\varphi(x||0^n) = y||0^n$$

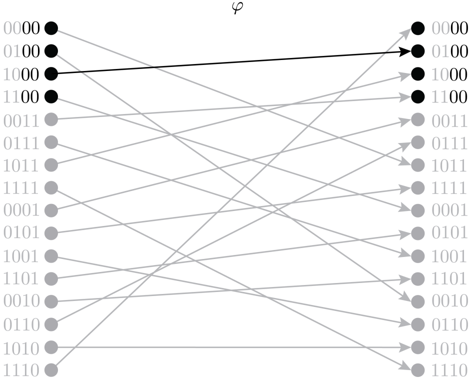
- DSZS $\approx$ zero pre-image in one-round sponge
- DSZS $\geq$ collision in (full) sponge



Zero Pairs Intuition

Some facts [CP'24]:

- Exactly one zero pair on average
- At least one with probability $1 - 1/e + o(1)$
- More than k with probability $\exp(-\Omega(k))$
- $\Omega(2^n)$ classical queries required to find one (if it exists)



Double Sided Zero Search Hardness

Conjecture [Unruh 21, 23]

Finding a zero pair requires $\Omega\left(\sqrt{2^n}\right)$ *quantum queries*

- Would provide evidence of post-quantum security of sponge
- Motivates new techniques
- **"Even simple questions relating to (superposition access to) random permutations are to the best of our knowledge not in the scope of existing techniques"** [Unruh 23]

Double Sided Zero Search Hardness

Theorem [CP'24]

Finding a zero pair requires $\Omega\left(\sqrt{2^n}\right)$ *quantum queries*

- We prove Unruh's conjecture
- Tight up to constant, even for small success probabilities
- Technique: worst-to-average case reduction, inspired by *Young subgroups*
- Leads to quantum one-wayness of the single round sponge

Proof outline

Theorem [CP'24]

Finding a zero pair requires $\Omega\left(\sqrt{2^n}\right)$ *quantum queries*

Proof.

A worst-to-average case reduction:

(1) Construct a worst-case instance from unstructured search

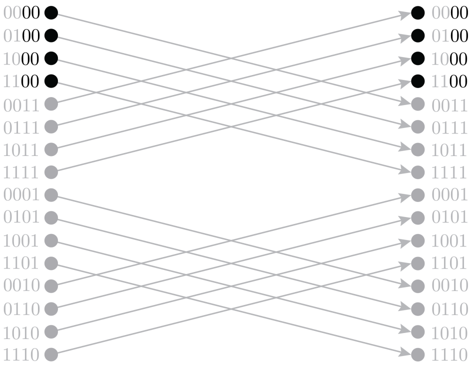
(2) Rerandomize to an average-case instance, by symmetrizing

$\square$

Worst-Case Hardness

- In the worst case, solution may not exist!

$$\varphi_w(x\|y) := x\|(y \oplus 1^n)$$

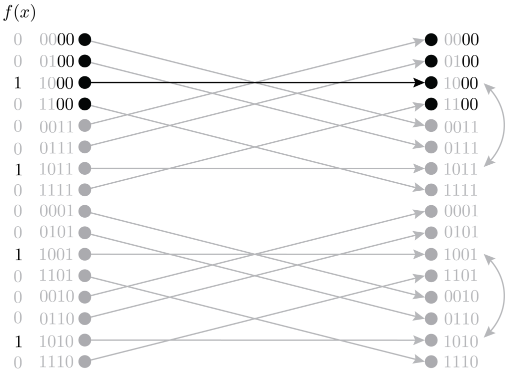


Worst-Case Hardness with K solutions

- Let f be a function on n bits that marks K many inputs,

$$\varphi_w(x\|y) = \begin{cases} x\|y & \text{if } f(x) = 1 \\ x\|(y \oplus 1^n) & \text{if } f(x) = 0 \end{cases}$$

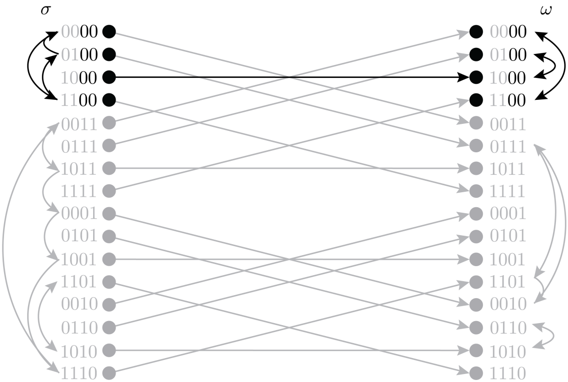
- x is in a zero pair of φ_w if and only if $f(x) = 1$
- Inverse queries don't help, because $\varphi_w = \varphi_w^{-1}$



Symmetrization

- Let ω, σ be random permutations that preserve suffix 0^n
- Sandwich a worst-case instance to get an average-case instance (with K zero pairs)

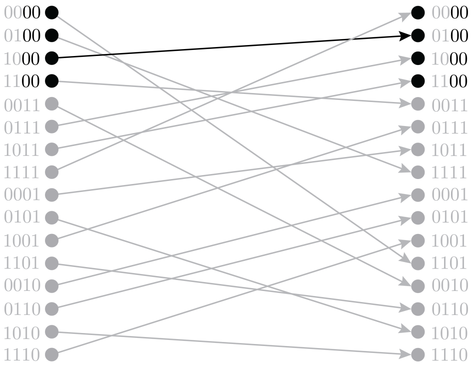
$$\varphi := \omega \circ \varphi_W \circ \sigma$$



Symmetrization

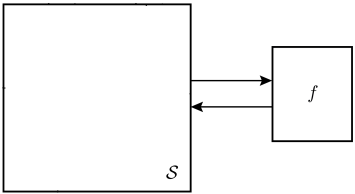
- Let ω, σ be random permutations that preserve suffix 0^n
- Sandwich a worst-case instance to get an average-case instance (with K zero pairs)

$$\varphi := \omega \circ \varphi_w \circ \sigma$$



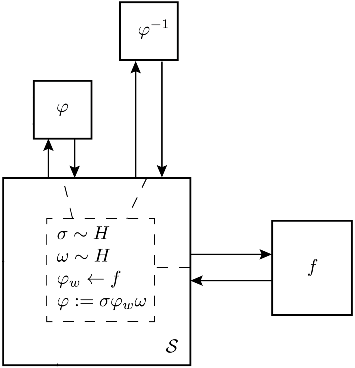
Symmetrization Soundness

- Let H be the symmetric subgroup which preserves the suffix 0^n
- Given zero pair (x, y) in $\varphi = \omega \circ \varphi_w \circ \sigma$, have a zero pair $(\sigma(x), \omega^{-1}(y))$ in φ_w, hence $\sigma(x)$ is marked by f



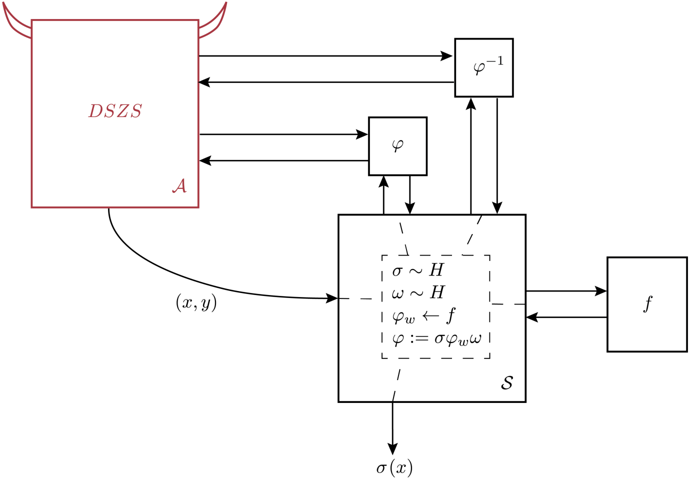
Symmetrization Soundness

- Let H be the symmetric subgroup which preserves the suffix 0^n
- Given zero pair (x, y) in $\varphi = \omega \circ \varphi_w \circ \sigma$, have a zero pair $(\sigma(x), \omega^{-1}(y))$ in φ_w, hence $\sigma(x)$ is marked by f



Symmetrization Soundness

- Let H be the symmetric subgroup which preserves the suffix 0^n
- Given zero pair (x, y) in $\varphi = \omega \circ \varphi_w \circ \sigma$, have a zero pair $(\sigma(x), \omega^{-1}(y))$ in φ_w, hence $\sigma(x)$ is marked by f



Symmetrization Soundness

- Let G be the symmetric group on 2^{2n} elements
- Let H be the symmetric subgroup which preserves the suffix 0^n
- Consider double cosets $\{C_0, C_1, ..., C_{2^n}\} = H \diagdown G \diagup H$
- From the theory of Young subgroups:

Characterization Lemma [CP'24]

The double coset C_K is the set of permutations with K Zero Pairs

Symmetrization Lemma [CP'24]

If $\omega, \sigma \sim H$ are uniformly random, and any fixed $\varphi_w \in C_K$, then $\omega \circ \varphi_w \circ \sigma$ is uniform random over C_K

Summary of results

- Prior argument plus tail bounds on Zero Pairs gives:

Theorem [CP'24]

A quantum algorithm making q queries to random φ, φ^{-1} on $2n$ bits finds a Zero Pair with probability at most $50 \cdot \frac{q^2}{2^n}$.

- A similar proof gives:

Theorem [CP'24]

A quantum algorithm making q queries to random φ, φ^{-1} on $r + c$ bits breaks one-wayness of the single-round sponge with probability at most $80 \cdot \frac{q^2}{2^{\min(r,c)}}$.

- These are tight up to a constant factor, for all success probabilities

Future Directions

- Other applications of symmetrizing over double cosets?
- One-wayness beyond a single round?
- Query lower bounds for collision resistance, second preimage resistance, etc?
- **Indifferentiability?**
- See also concurrent work by Majenz, Malavolta, and Walter

($\rightarrow$) Similar results, different techniques, [eprint:2024/1140]

Thank you!

[CP24] Quantum One-Wayness of the Single Round Sponge with Invertible Permutations, eprint:2024/414
[Unruh 21 (23)] (Towards) Compressed Permutation Oracles, eprint:2021/062(2023/770)
[Zhandry 21] Redeeming Reset Indifferentiability and Post-Quantum Groups eprint:2021/288