# Evasive Properties

## A Gap in the Quantum Oracles Zoo

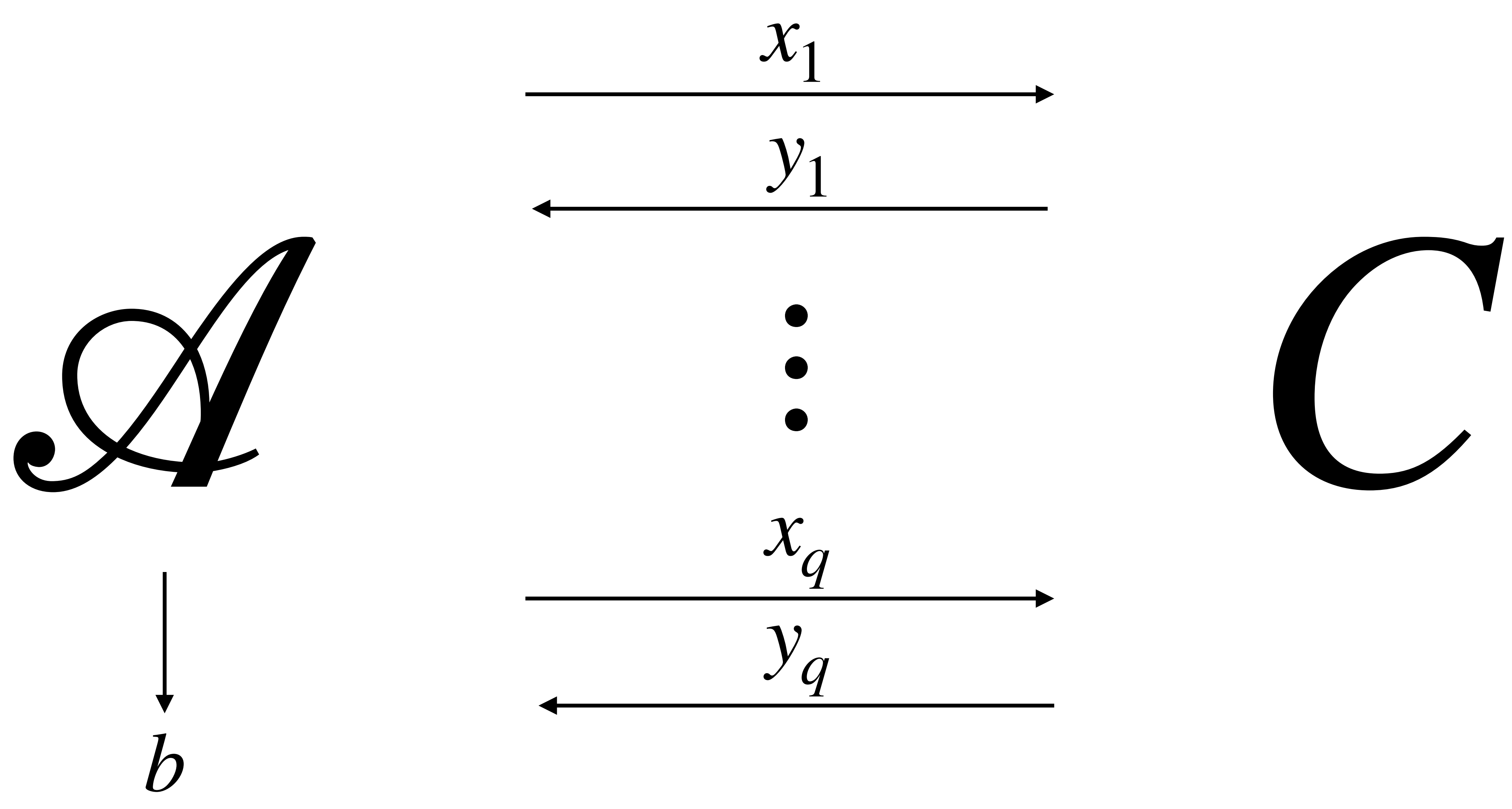
Ashwin Jha
Ruhr University of Bochum

ASK 2024 @ Kolkata, India

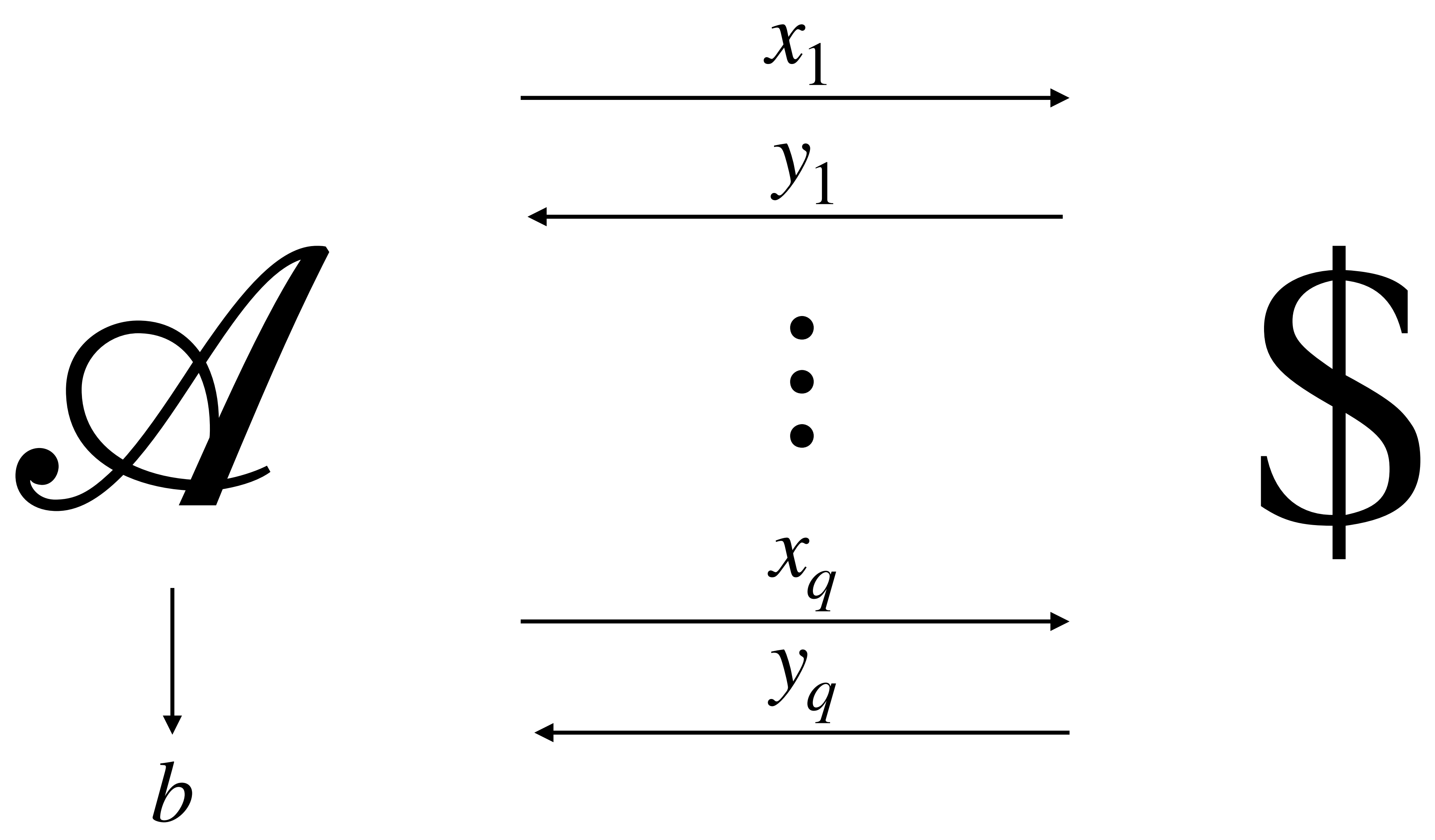
# The Indistinguishability Game

# The Indistinguishability Game

Real world

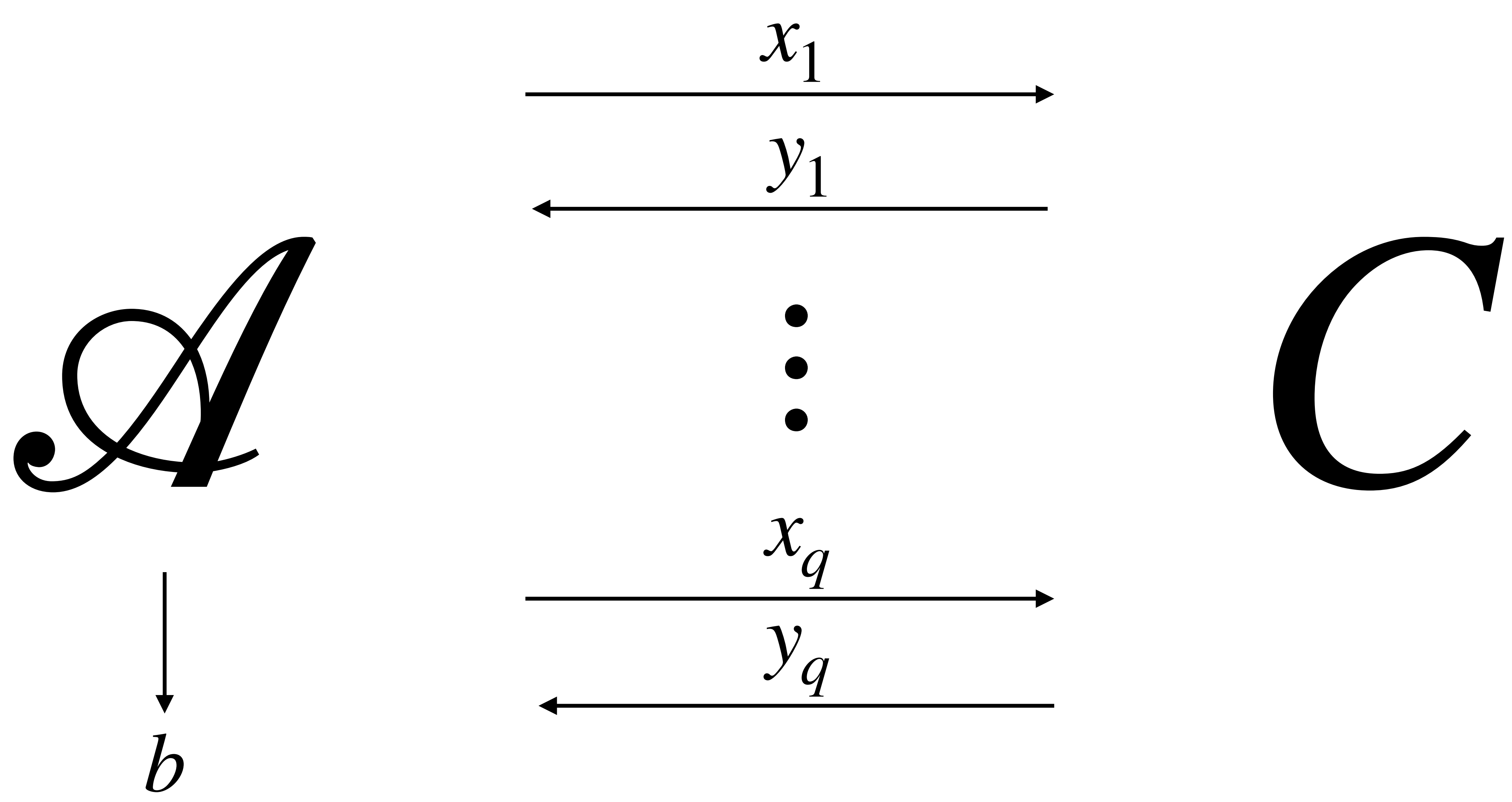



Ideal world

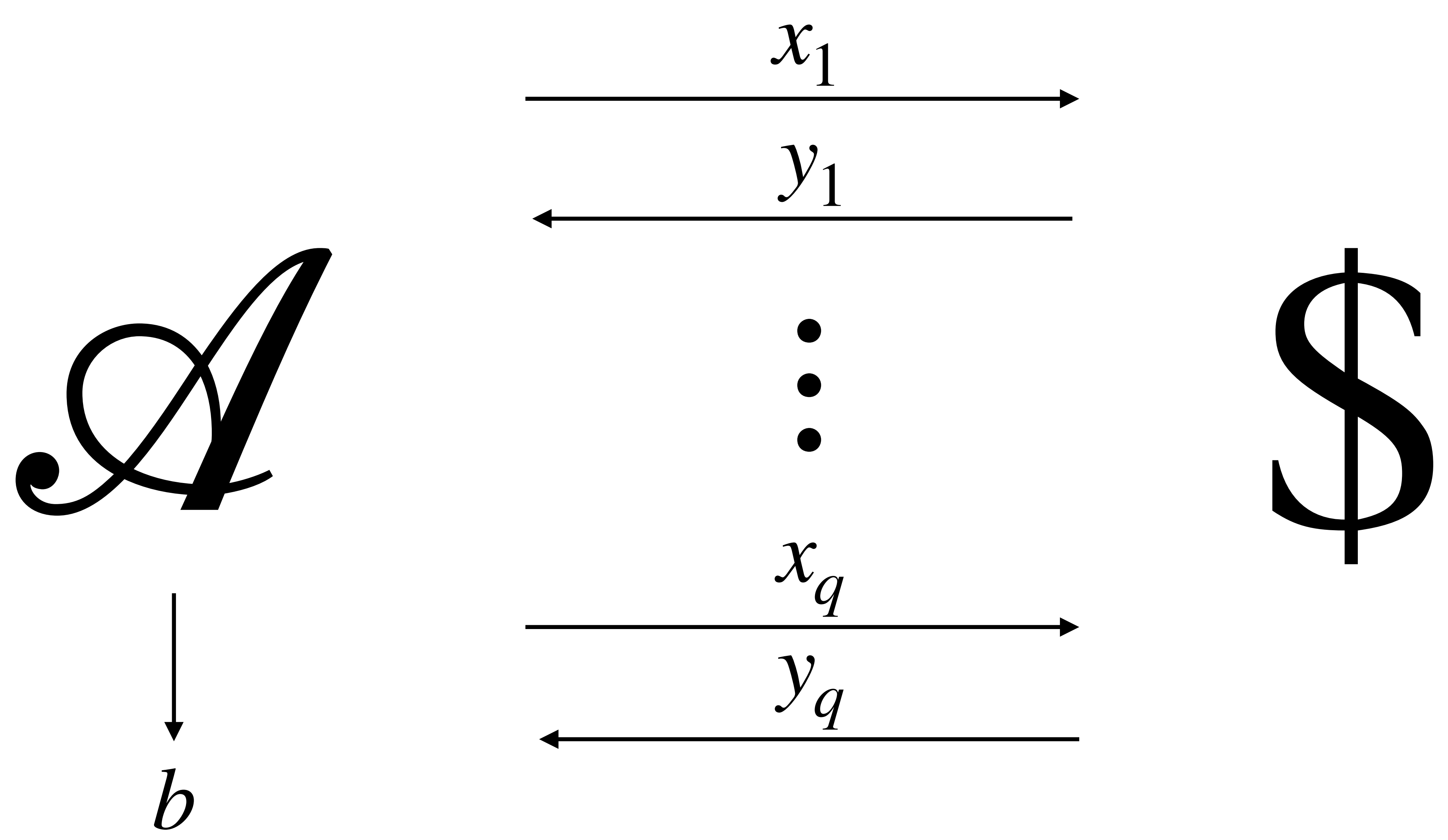


# The Indistinguishability Game

Real world




Ideal world

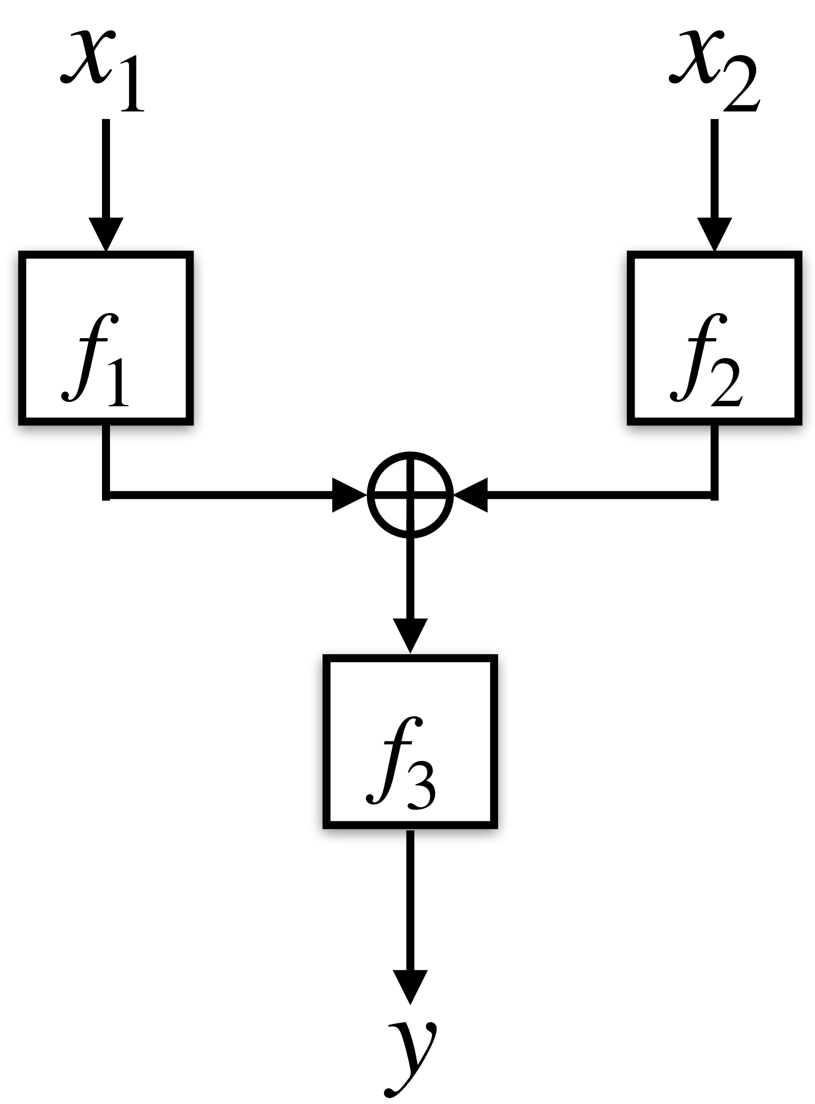



$$\mathbf{Adv}_C^{\$}(\mathscr{A}) := \left|\Pr\left(b = 1 \text{ in the real world}\right) - \Pr\left(b = 1 \text{ in the ideal world}\right)\right|$$

# Typical Proofs in the Classical World

# Typical Proofs in the Classical World

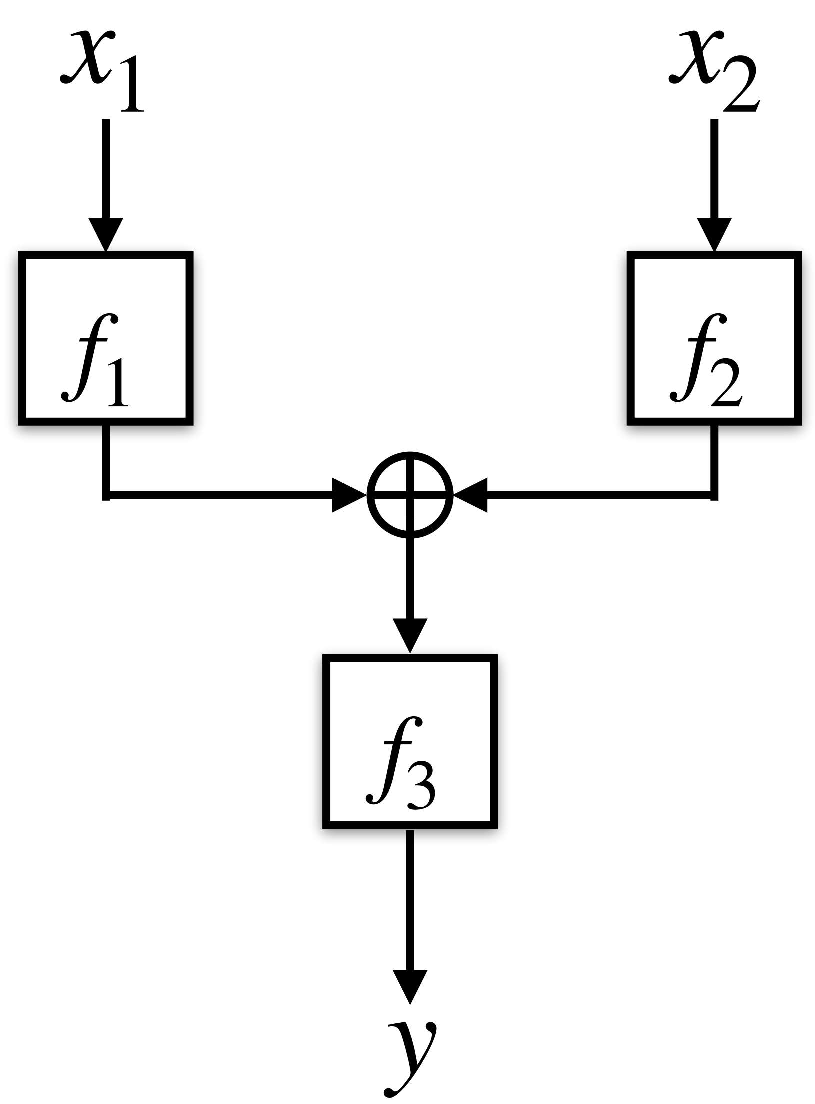
## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]




$$f_1, f_2, f_3 \longleftarrow_{\$} \mathscr{F}(n, n)$$

# Typical Proofs in the Classical World

## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]



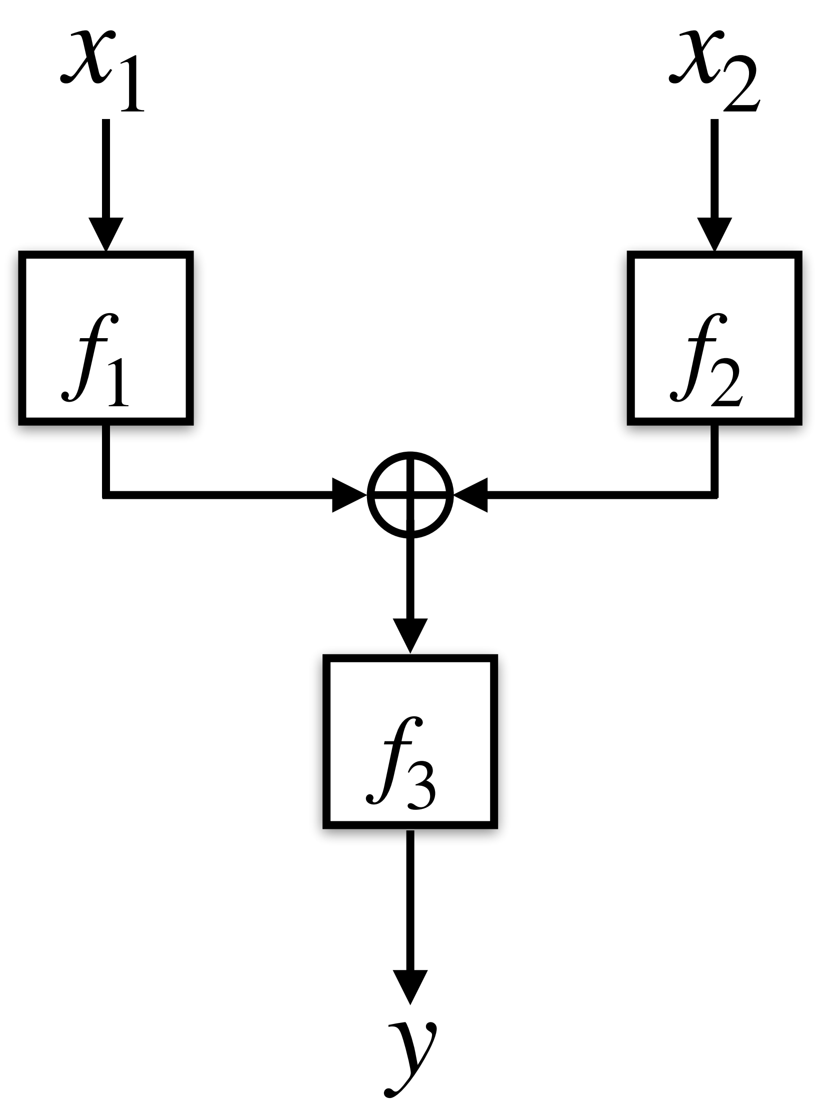

$$f_1, f_2, f_3 \longleftarrow_{\$} \mathcal{F}(n, n)$$

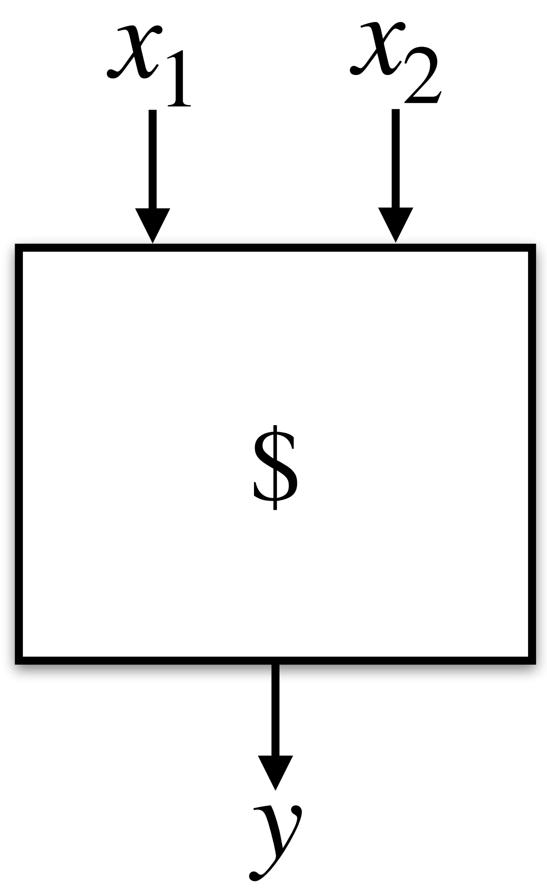
**Theorem** [Liskov-Rivest-Wagner 2002]

$$\mathbf{Adv}^{\$}_{\mathsf{LRWQ}}(\mathcal{A}) = O\left(\frac{q^2}{2^n}\right)$$

# Typical Proofs in the Classical World

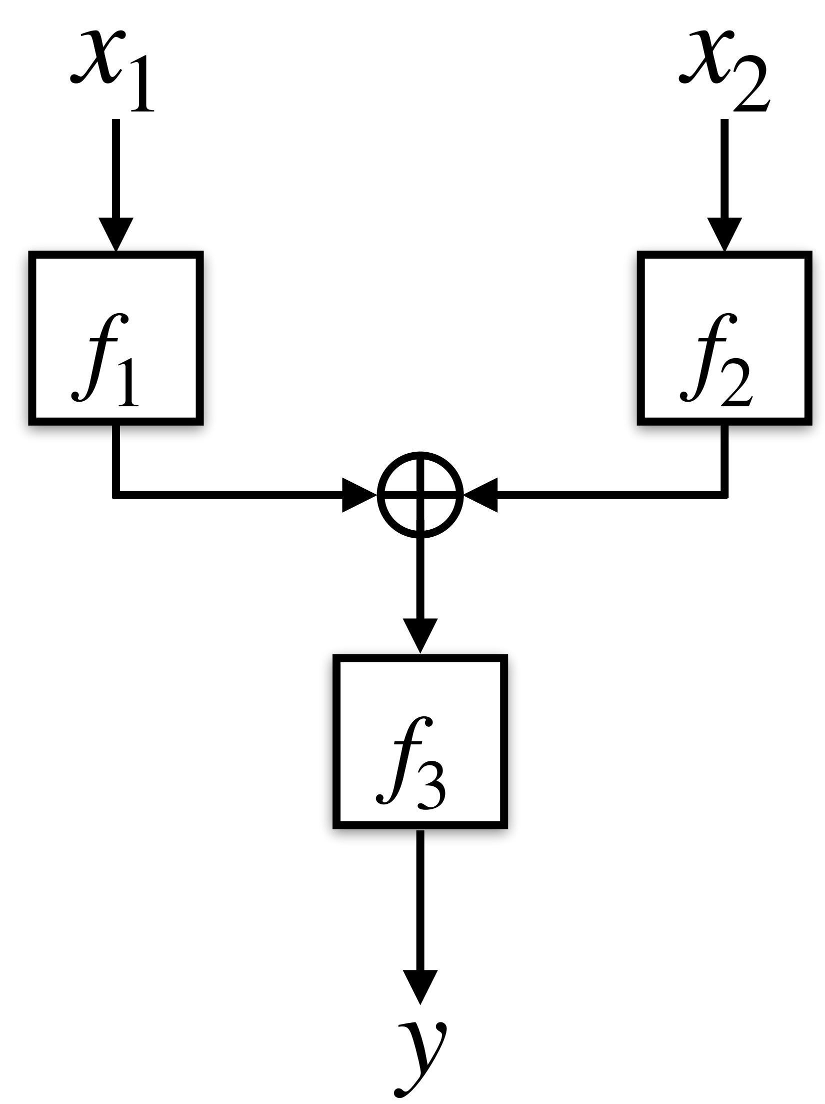
**The Case of LRWQ** [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]

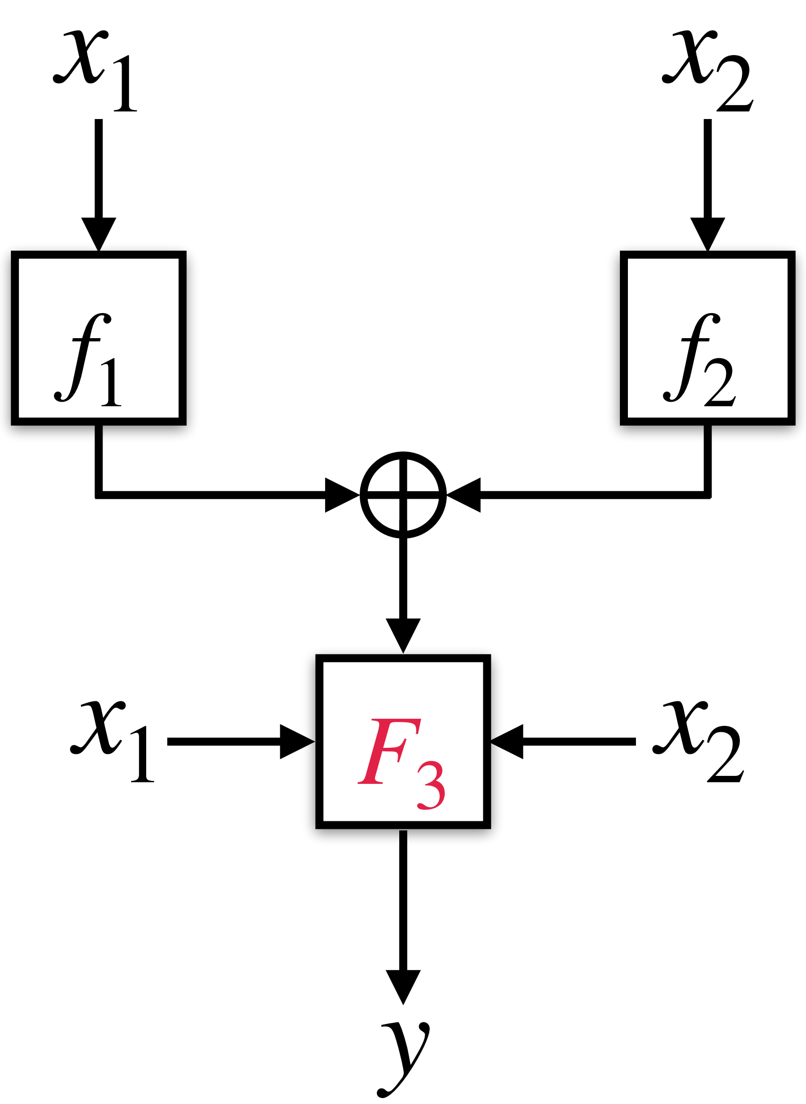


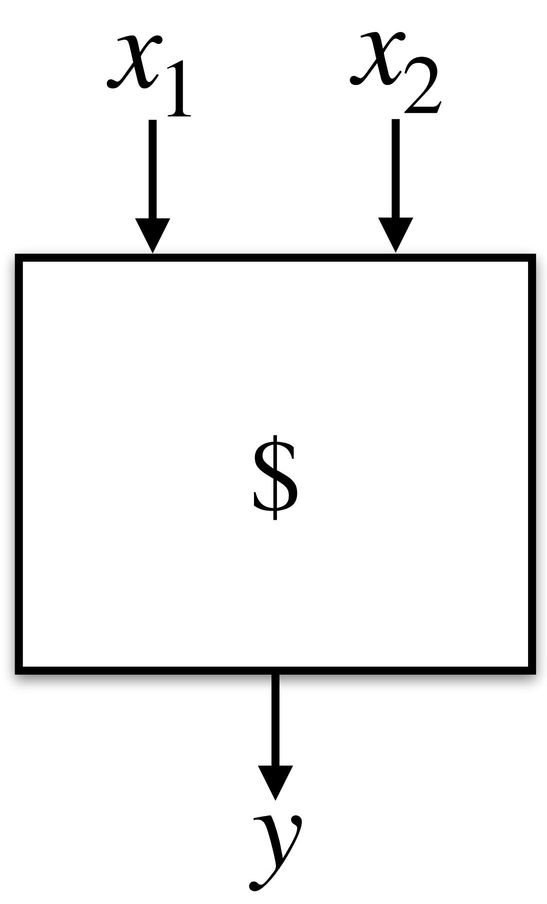
# Typical Proofs in the Classical World

## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]



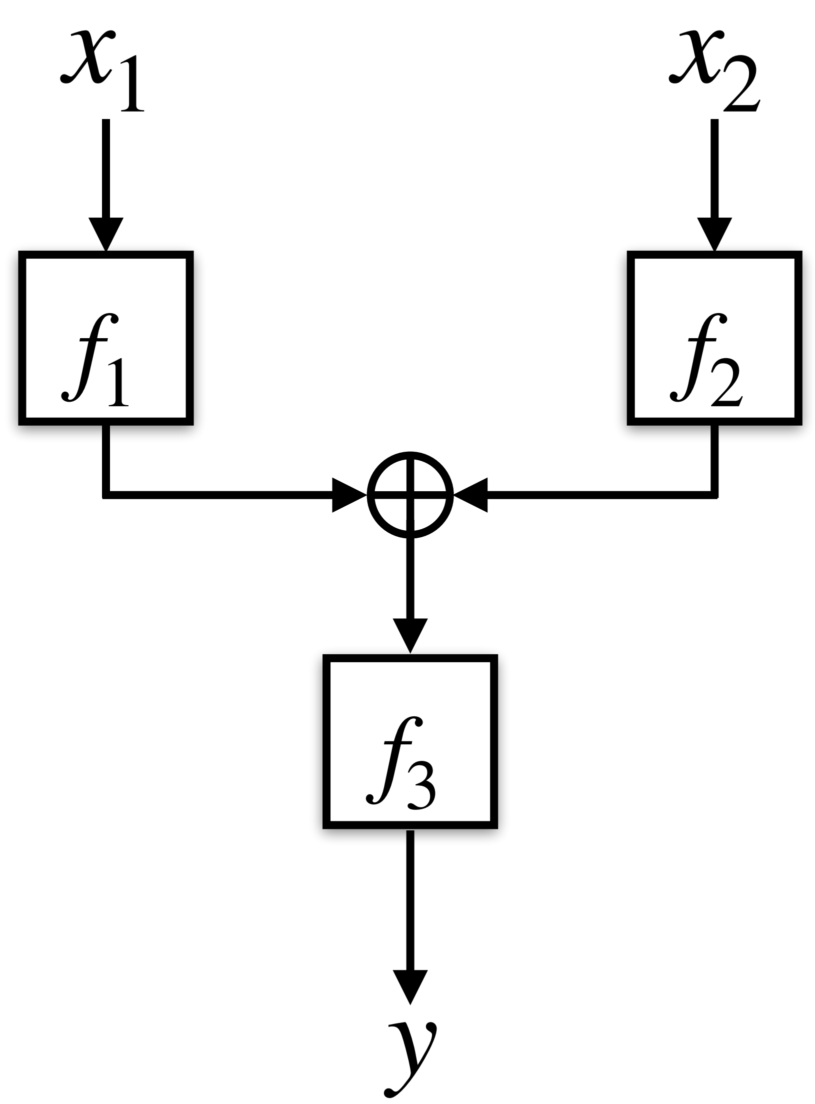

LRWQ′

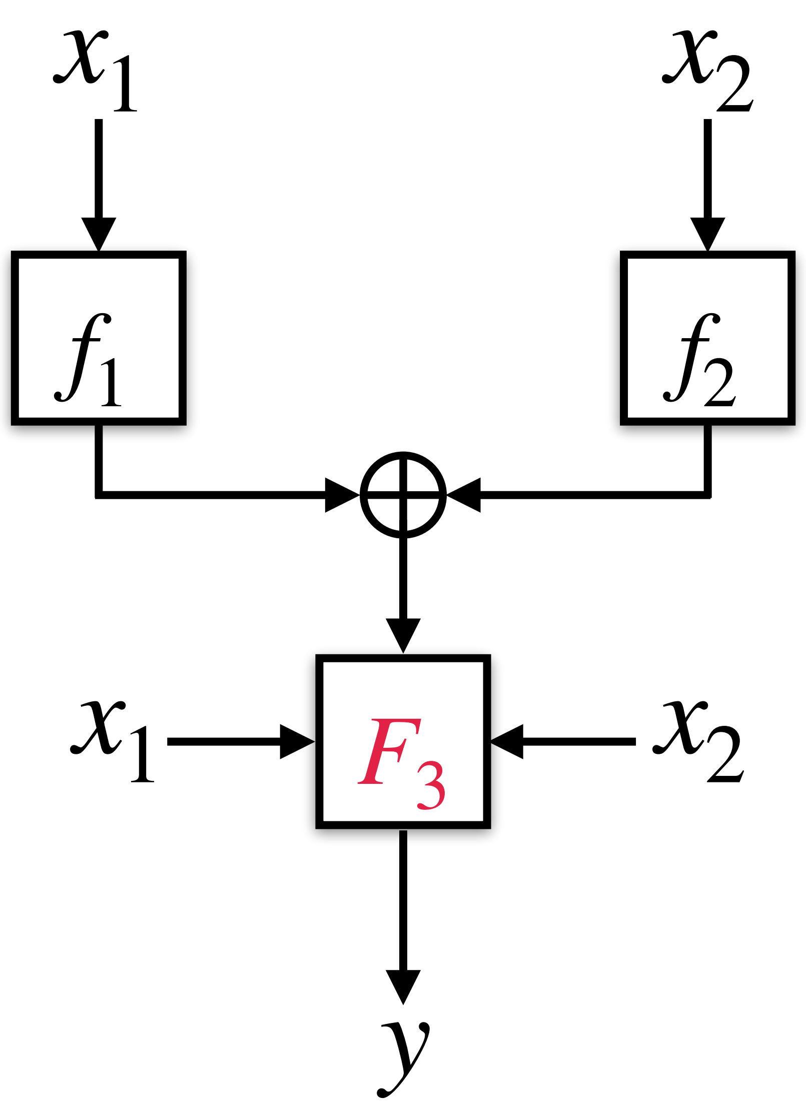



$$F_3 \longleftarrow_{\$} \mathscr{F}(3n, n)$$

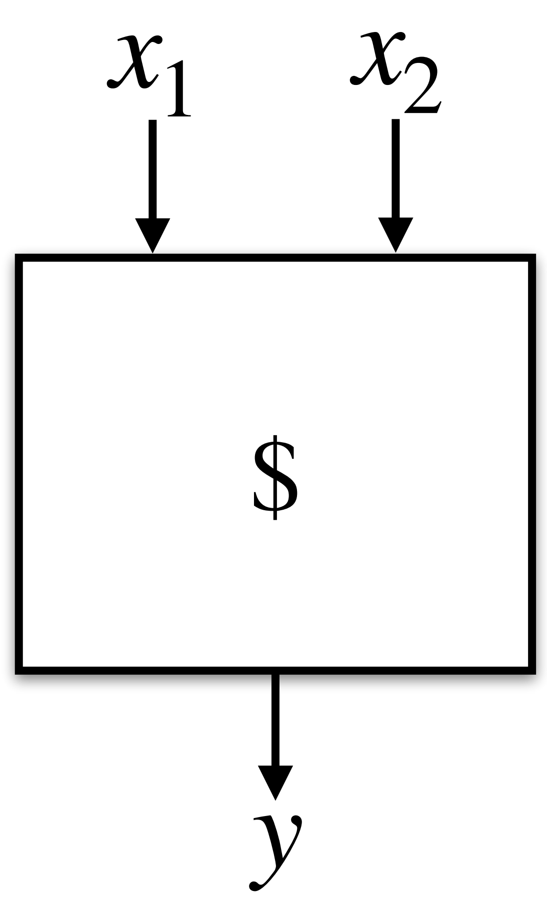
# Typical Proofs in the Classical World

## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]



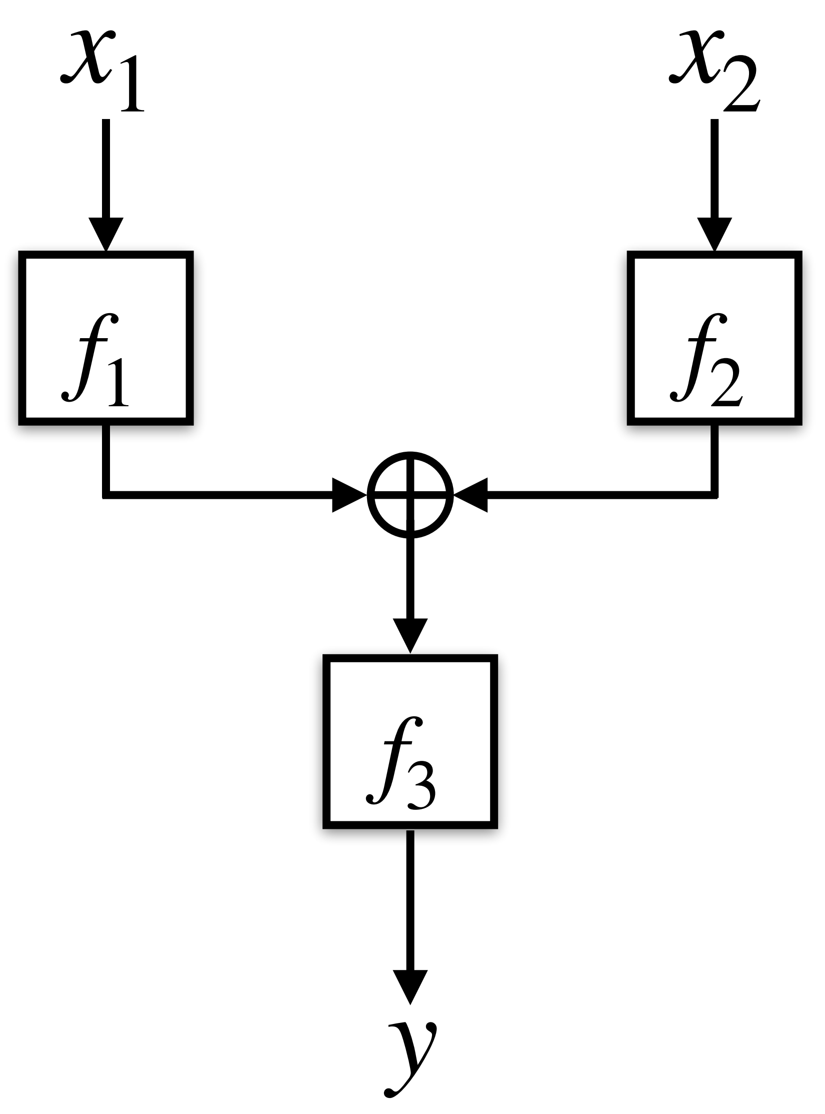



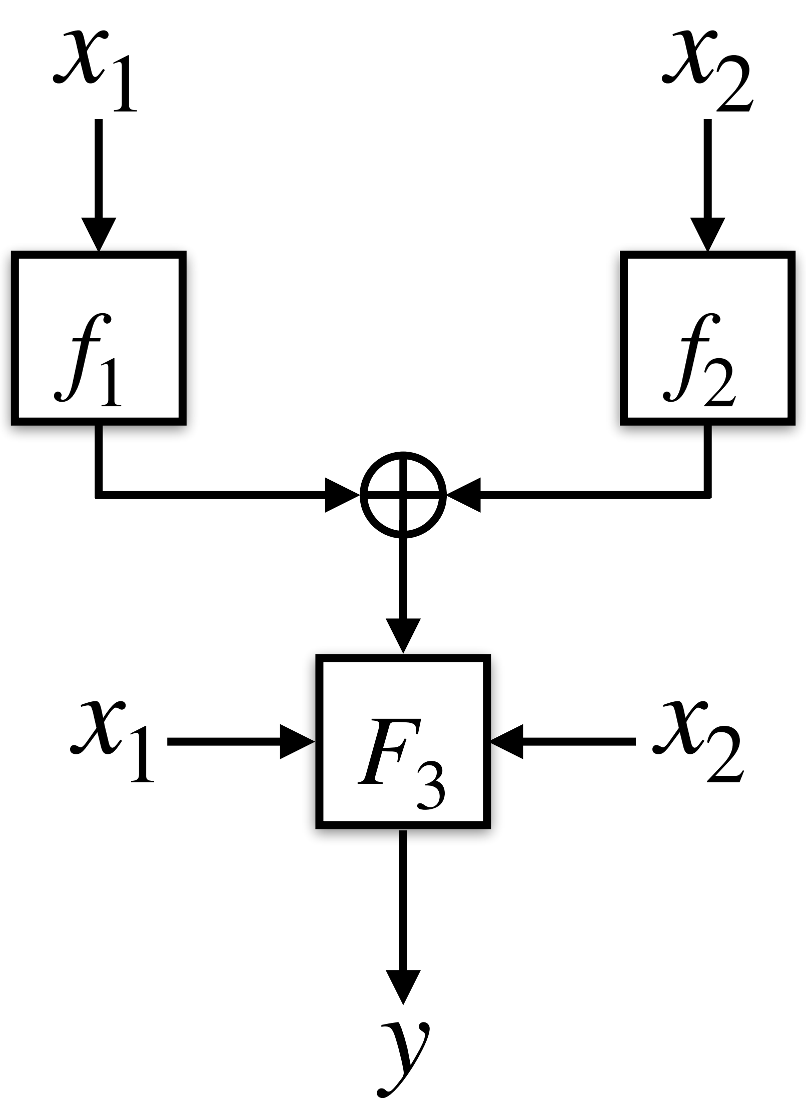

$\approx$



# Typical Proofs in the Classical World

**The Case of LRWQ** [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]




$$g \longleftarrow_{\$} \mathscr{F}(3n+2, n)$$

$$f_1(x_1) = g(00 \parallel 0^{2n} \parallel x_1)$$
$$f_2(x_2) = g(01 \parallel 0^{2n} \parallel x_2)$$
$$f_3(u) = g(10 \parallel 0^{2n} \parallel u)$$
$$F_3(x_1, x_2, u) = g(11 \parallel x_1 \parallel x_2 \parallel u)$$

# Typical Proofs in the Classical World

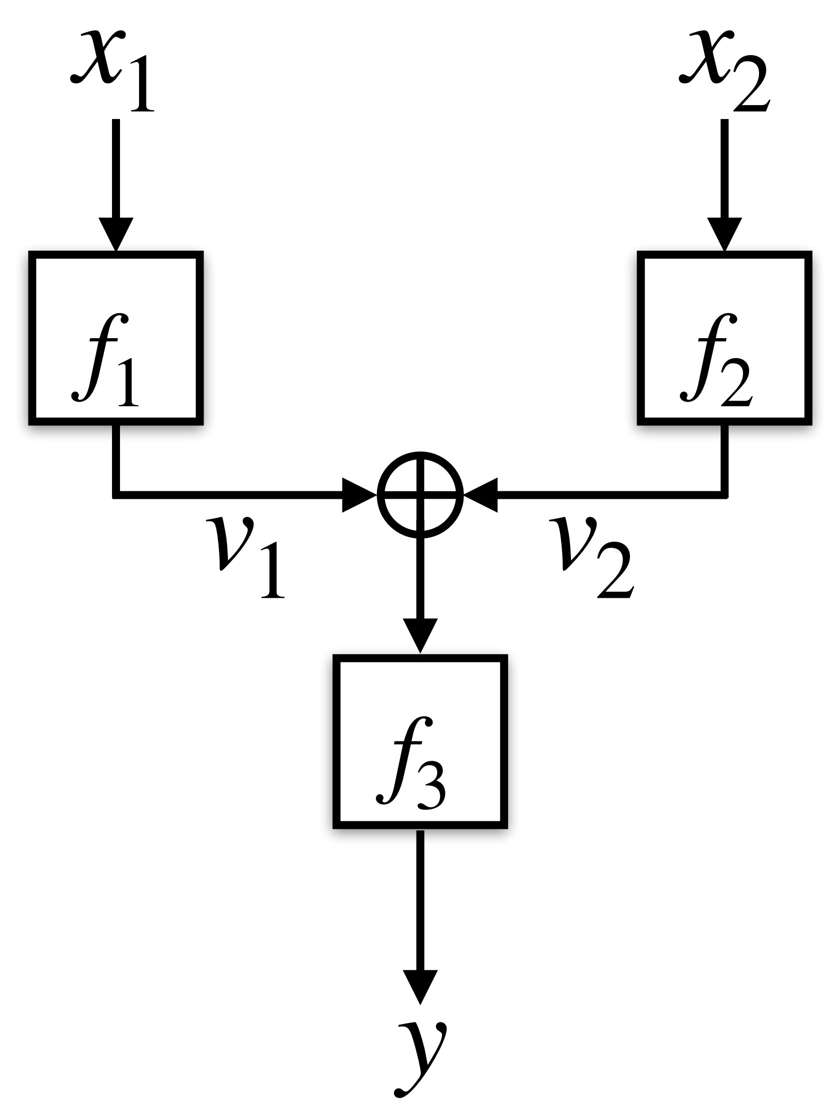
## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]

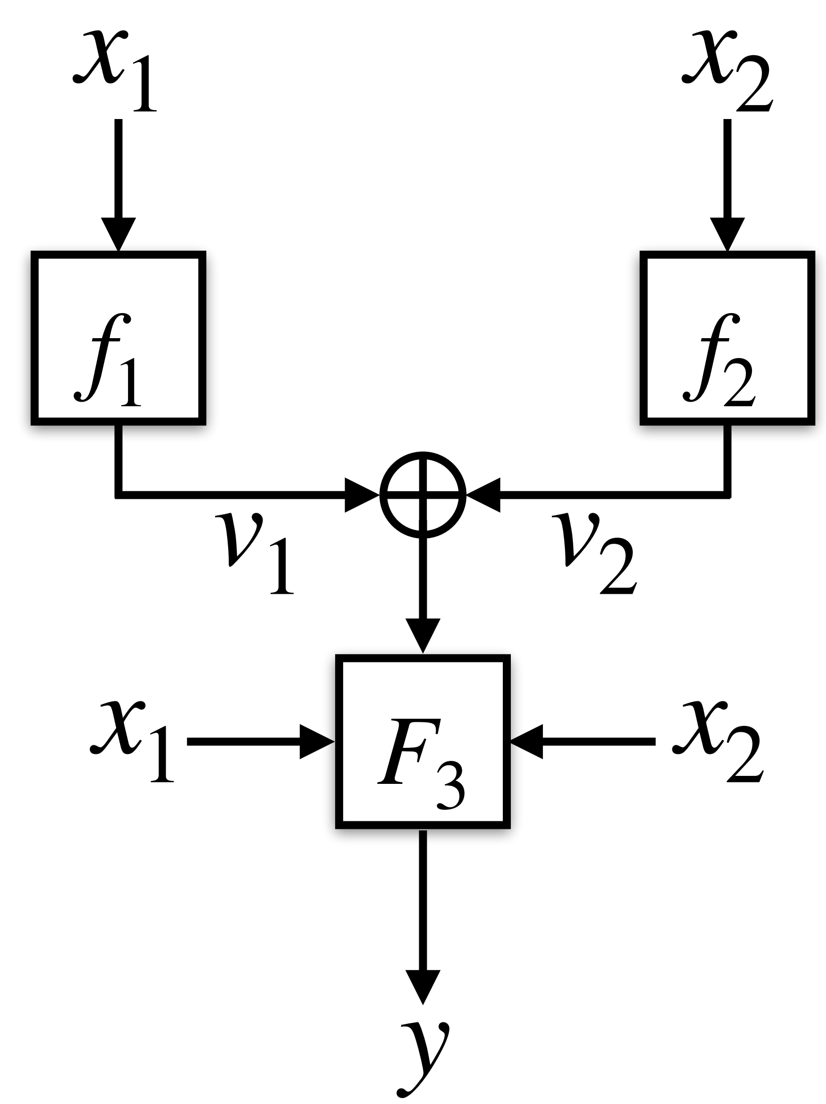
### Database and Lazy Sampling

- A database $d$ is a partial function $d : \{0,1\}^{3n+2} \to \{0,1\}^n \cup \{ \perp \}$.
- The random function $g$ can be lazy sampled and recorded as follows:
  - If $d(x) = \perp$ , then $d(x) = v \xleftarrow{}_{\$} \{0,1\}^n$
  - Return $d(x)$

# Typical Proofs in the Classical World

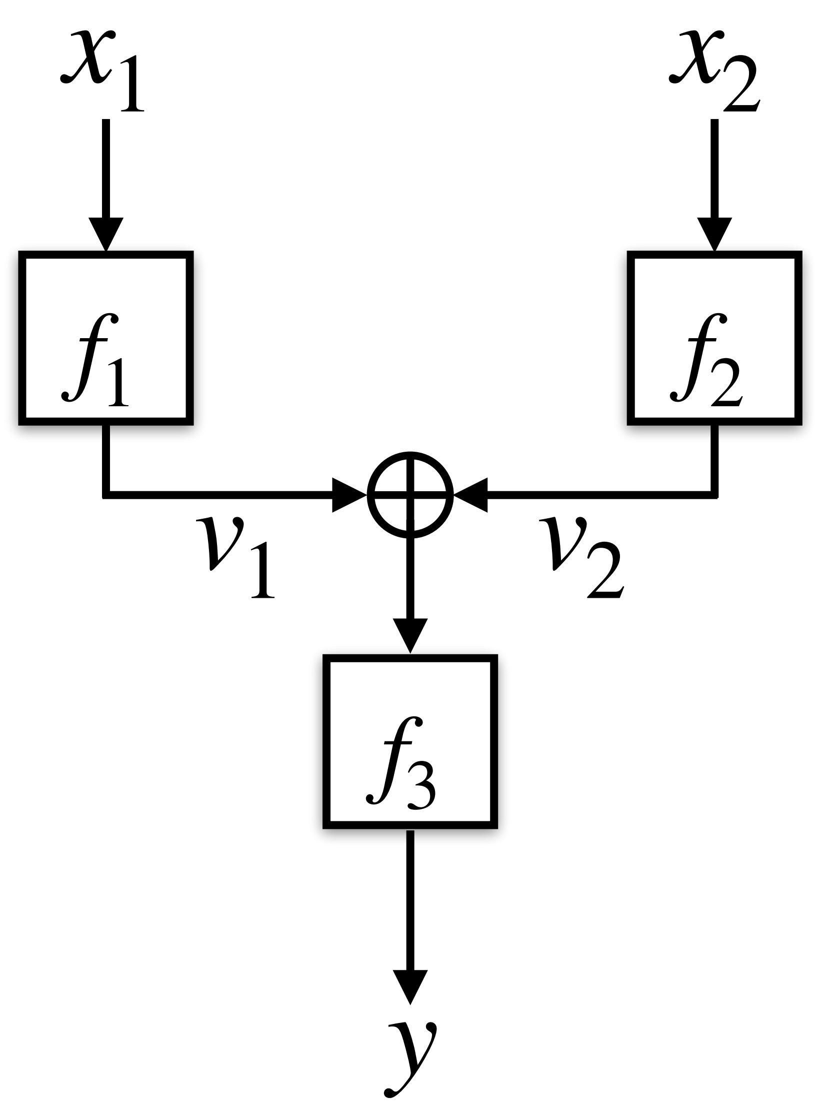
## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]

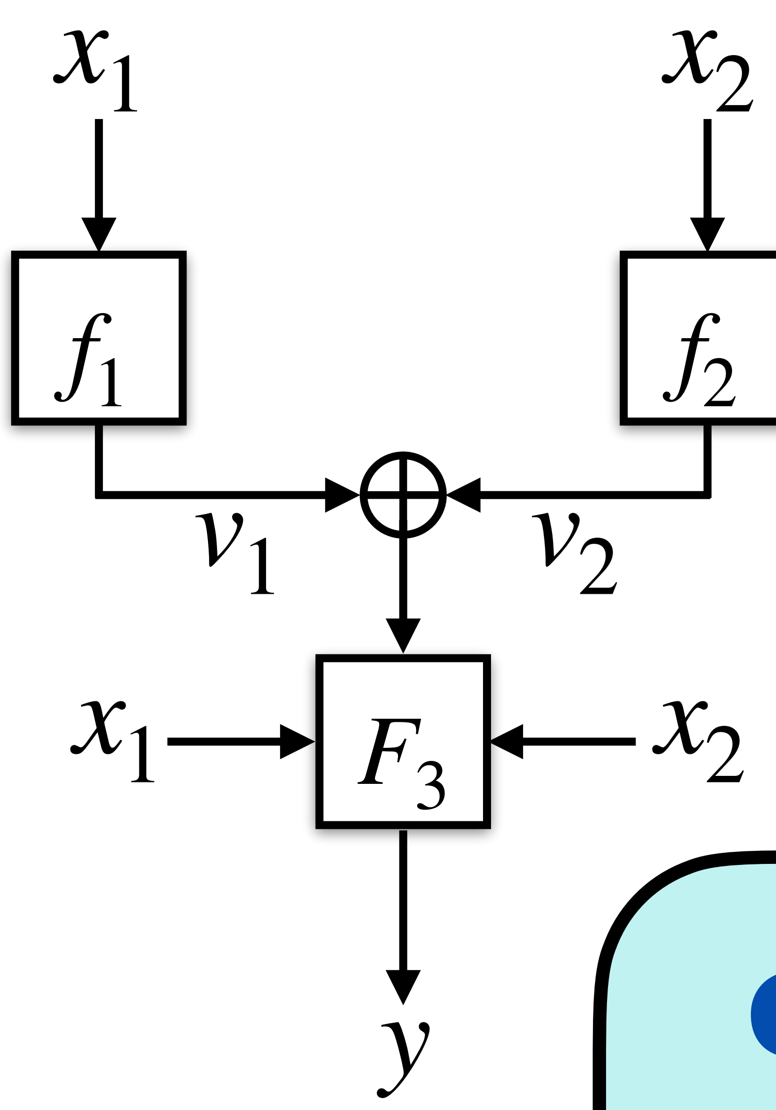


# Typical Proofs in the Classical World

## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]




**Good Databases**

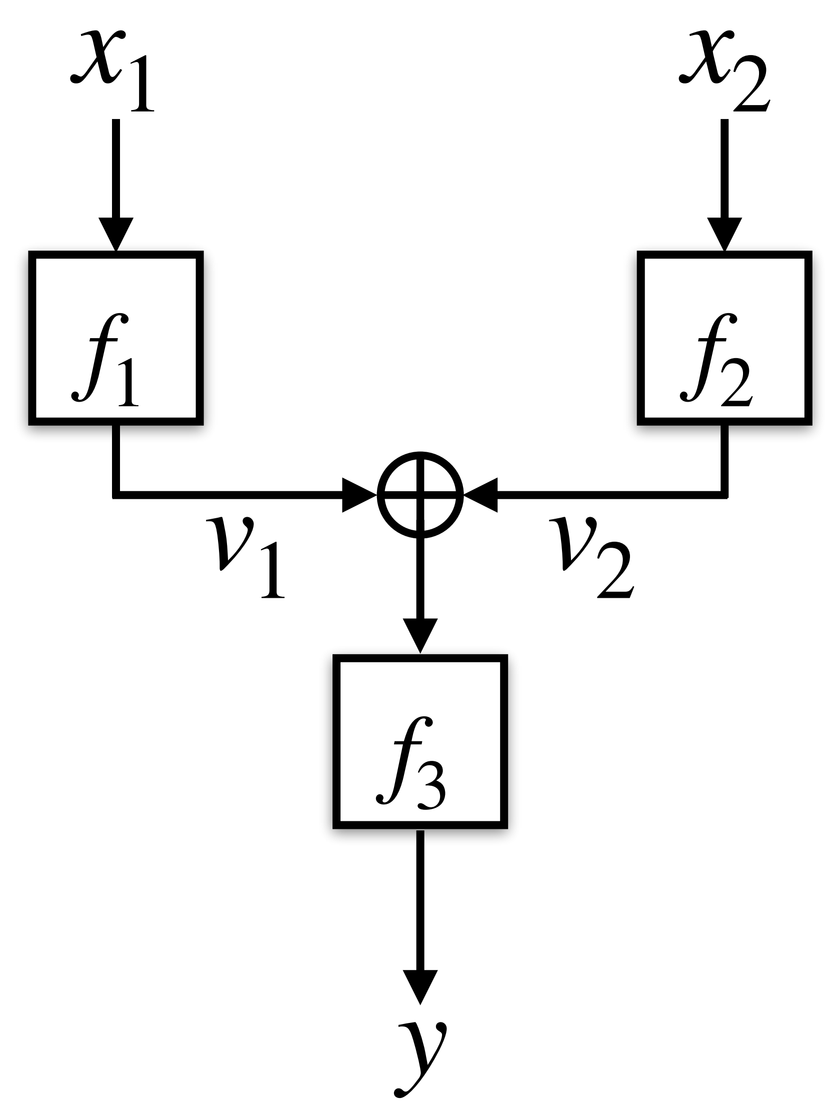
For any $i \in [q]$ and $j \leq i - 1$ if

$$v_1^i \oplus v_2^i \neq v_1^j \oplus v_2^j$$

then LRWQ and LRWQ′ behave identically.

# Typical Proofs in the Classical World

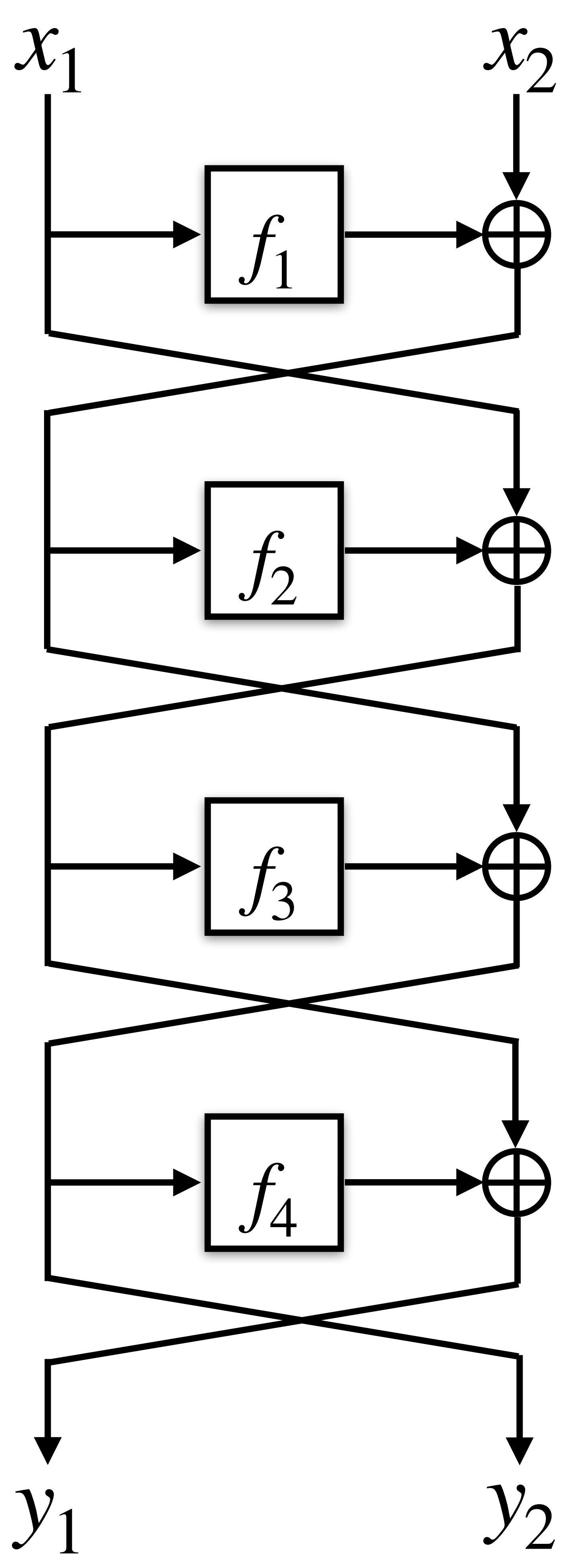
## The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]




$$
\begin{aligned}
\mathbf{Adv}^{\$}_{\mathsf{LRWQ}}(\mathscr{A}) &\leq \Pr\left(d_q \text{ is bad}\right) \\
&\leq \sum_{i=1}^{q} \Pr\left(d_i \text{ is bad} \mid d_{i-1} \text{ was good}\right) \\
&\leq \sum_{i=1}^{q} O\left(\frac{i-1}{2^n}\right) \leq O\left(\frac{q^2}{2^n}\right)
\end{aligned}
$$

# Typical Proofs in the Classical World

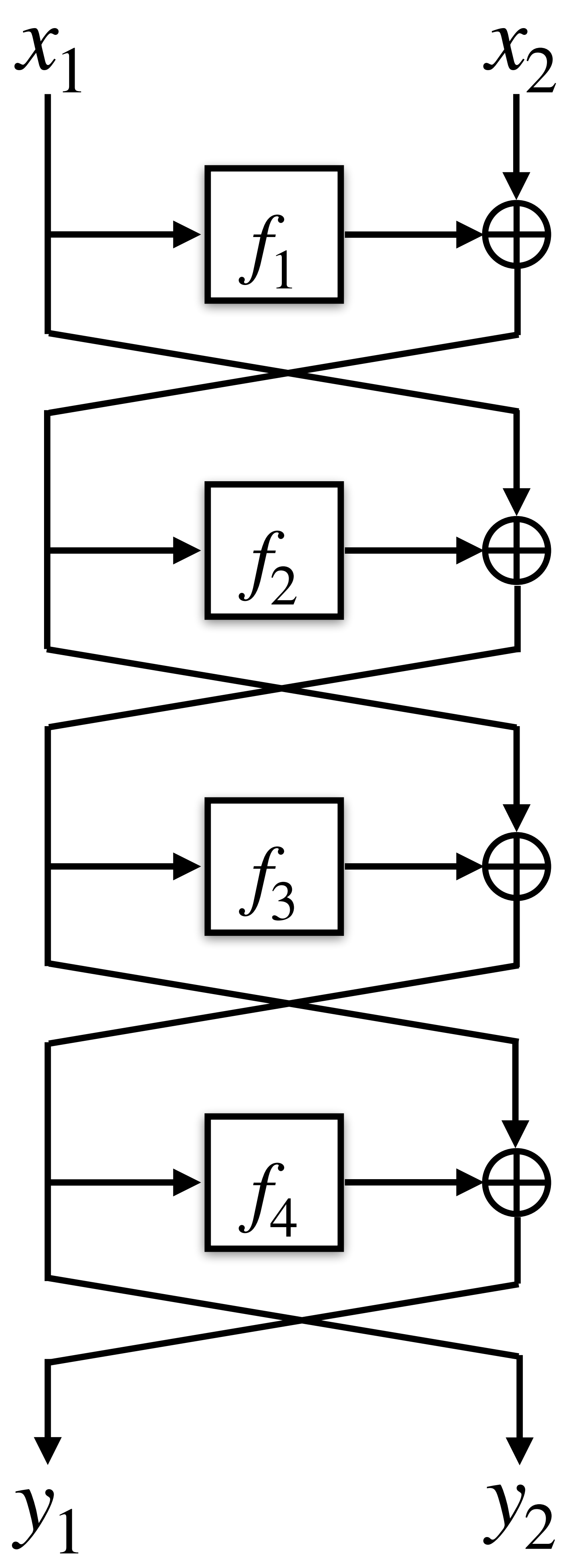
## The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]




$$f_1, f_2, f_3, f_4 \longleftarrow_{\$} \mathscr{F}(n, n)$$

# Typical Proofs in the Classical World

## The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]



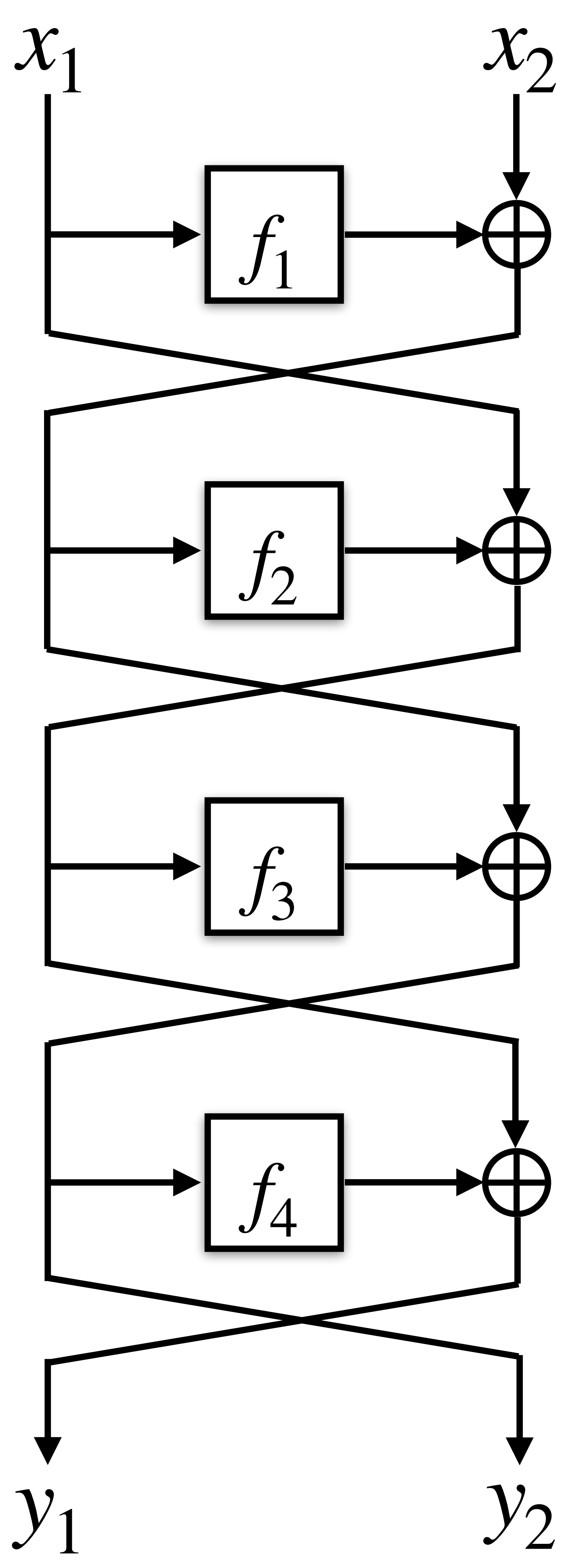

$$f_1, f_2, f_3, f_4 \longleftarrow_{\$} \mathscr{F}(n, n)$$

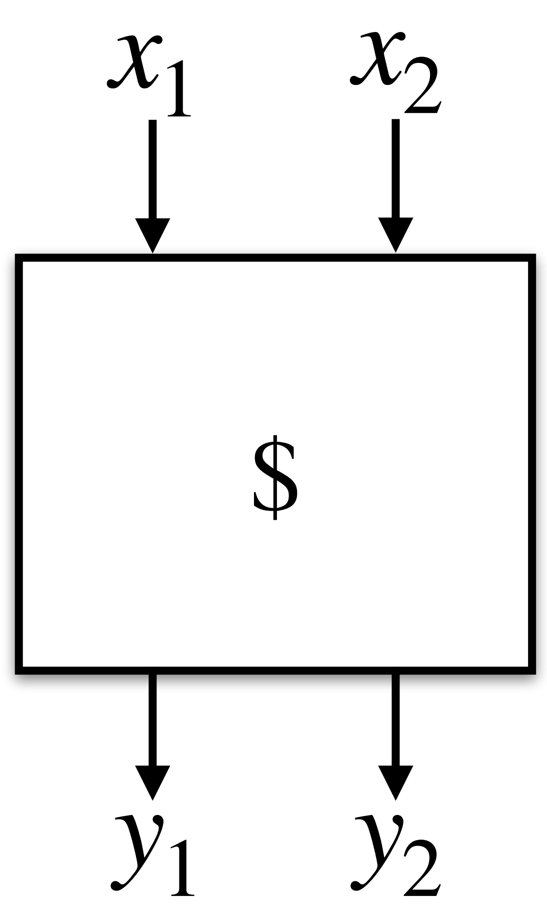
**Theorem** [Luby-Rackoff 1988]

$$\mathbf{Adv}^{\$}_{\mathsf{4LR}}(\mathscr{A}) = O\left(\frac{q^2}{2^n}\right)$$

# Typical Proofs in the Classical World

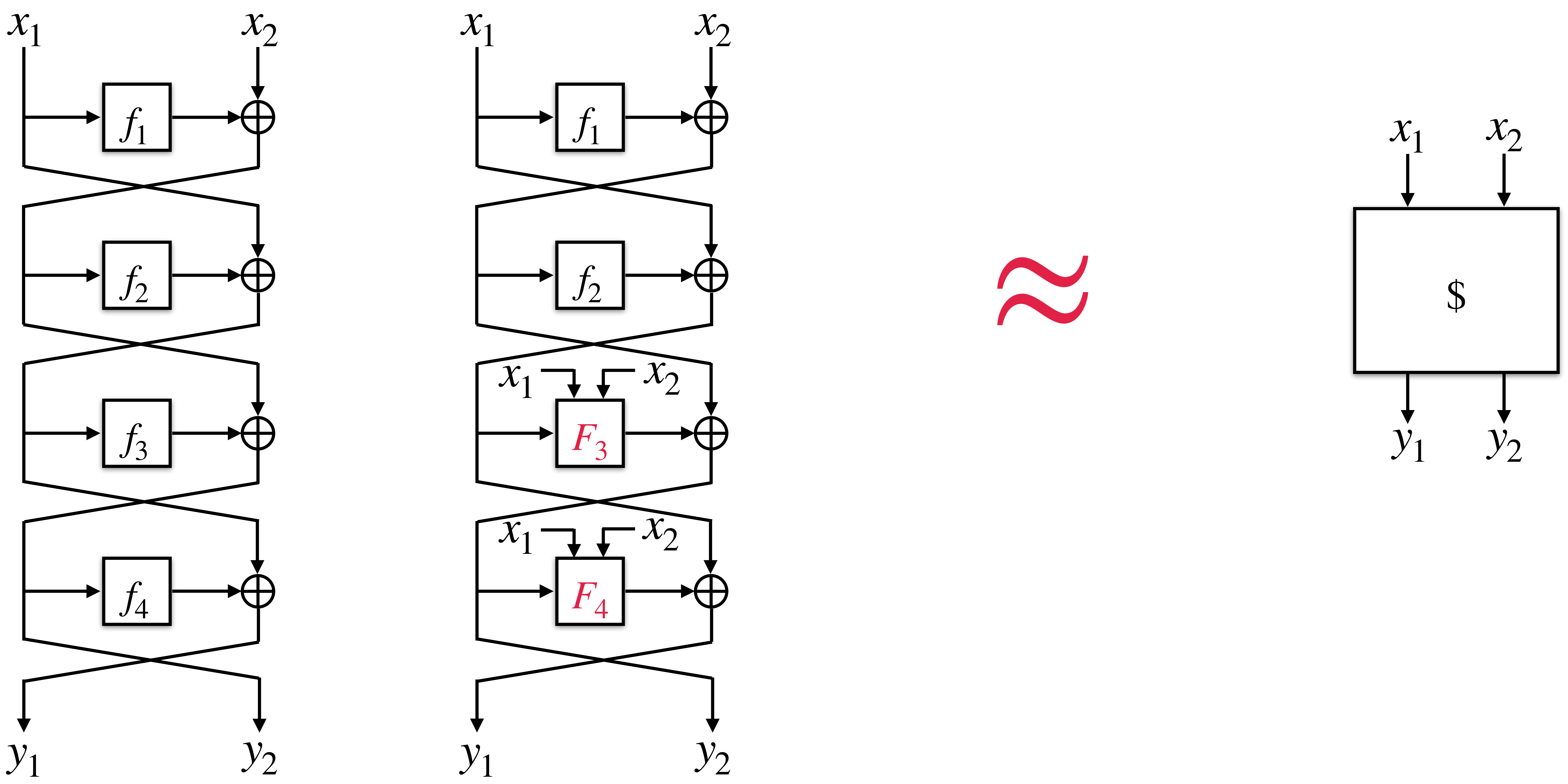
## The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]



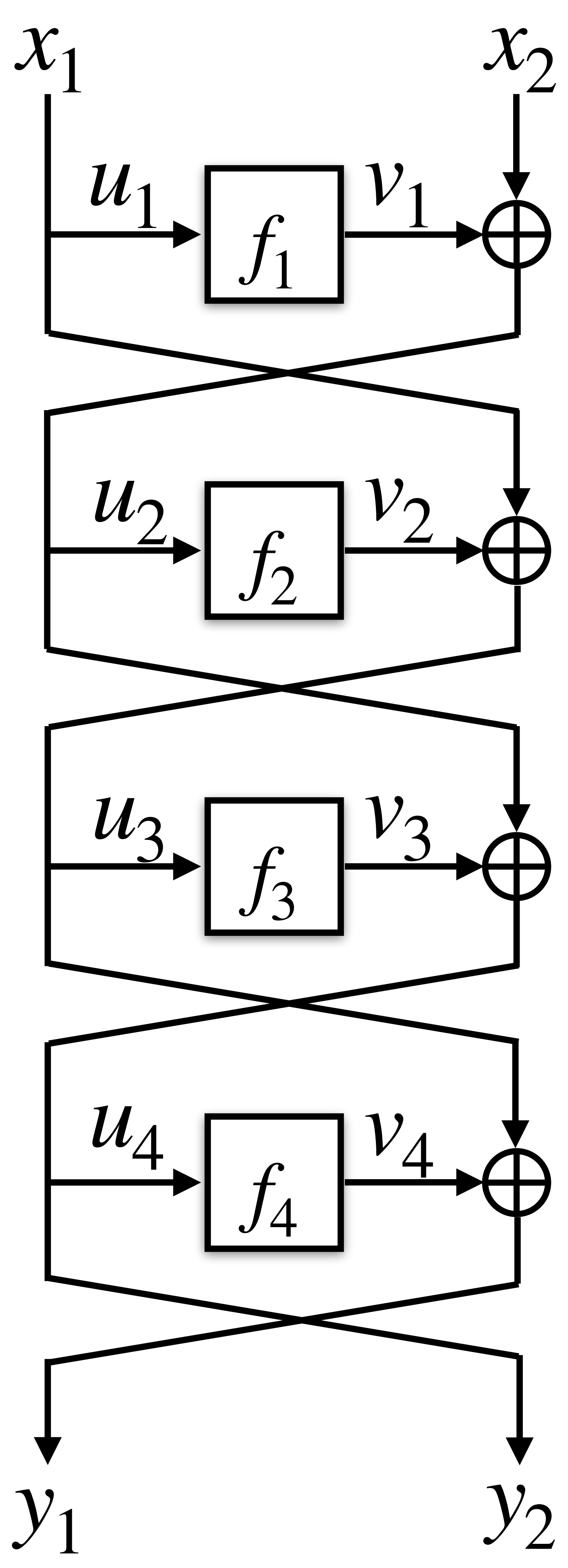
# Typical Proofs in the Classical World

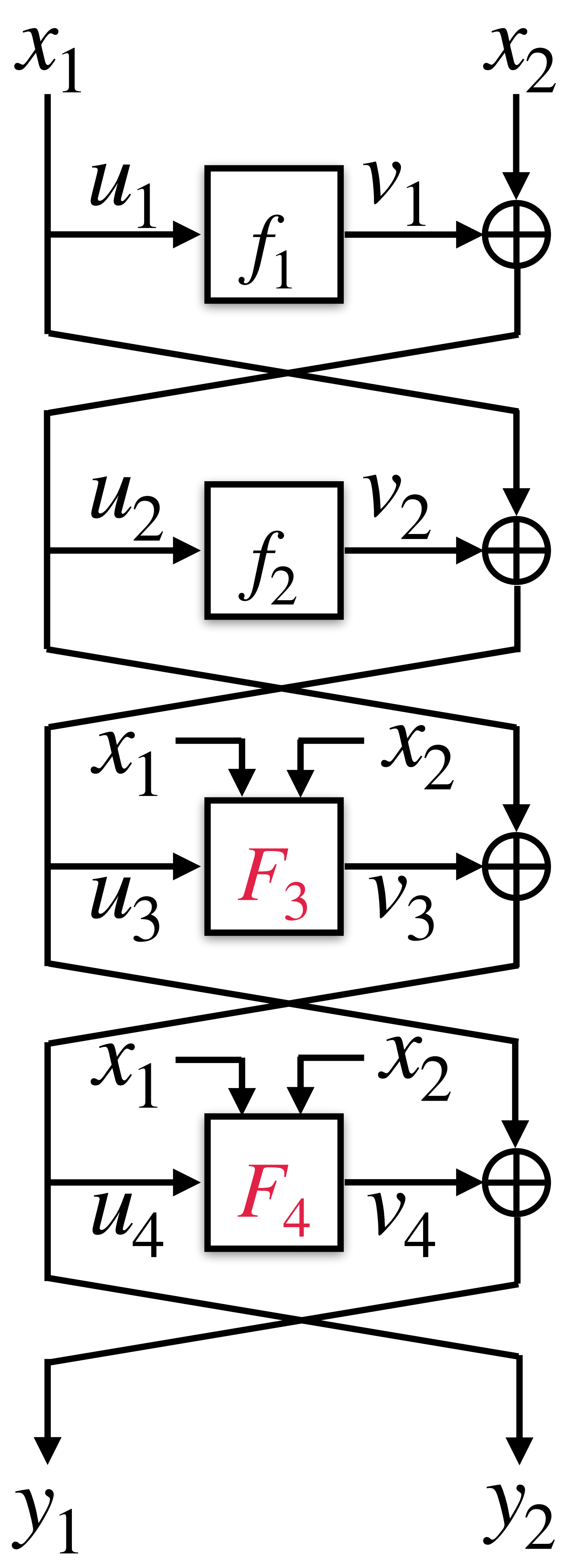
## The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]



# Typical Proofs in the Classical World

## The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]




**Bad Databases**

- For any $i \in [q]$ and $j \leq i - 1$

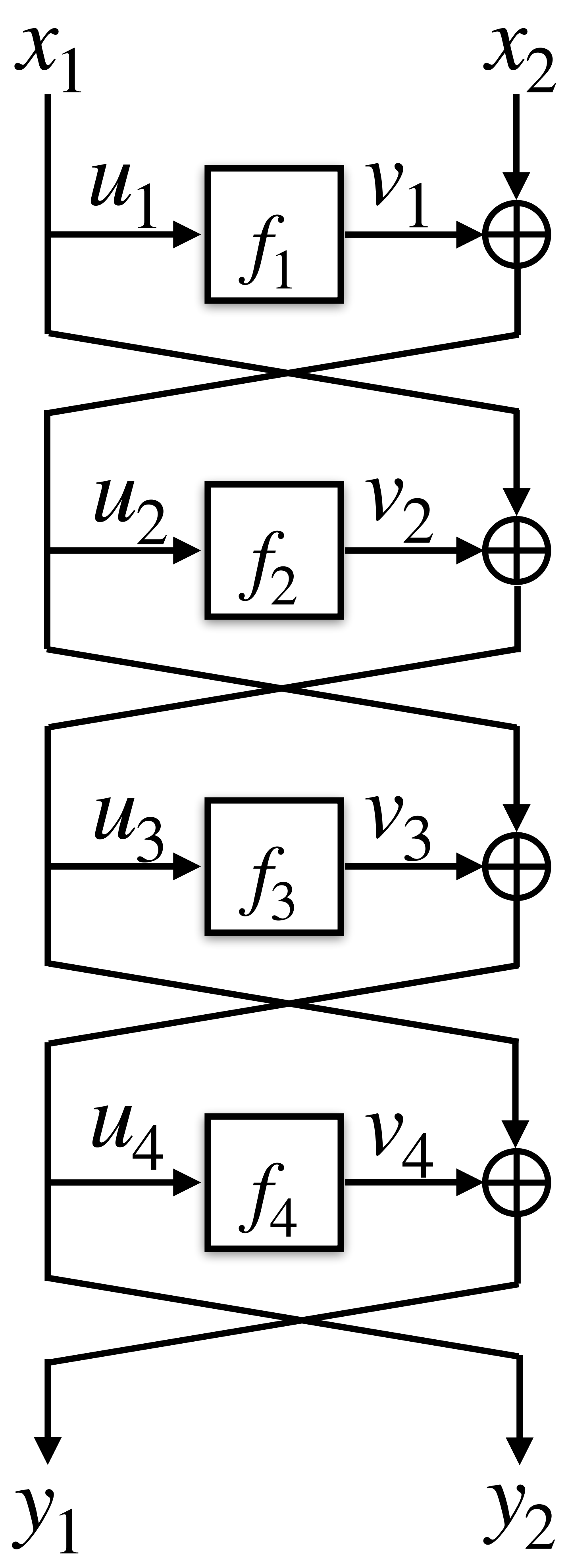
$$v_2^i \oplus u_1^i = v_2^j \oplus u_1^j$$

- For any $i \in [q]$ and $j \leq i - 1$

$$v_3^i \oplus u_2^i = v_3^j \oplus u_2^j$$

# Typical Proofs in the Classical World

## The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]




$$\mathbf{Adv}^{\$}_{\mathsf{4LR}}(\mathscr{A}) \leq \Pr\left(d_q \text{ is bad}\right) \leq O\left(\frac{q^2}{2^n}\right)$$

# The Quantum World

## Basics of Quantum Computing

# The Quantum World

## Basics of Quantum Computing

- Data (State) is represented by unit vectors in the complex Hilbert space.
  - Any $n$-qubit system $Q$ is defined by $\mathbb{C}^{2^n}$.
  - $\mathscr{Y} = \{0,1\}^n$ is mapped to the basis $\mathscr{B}_{\mathscr{Y}} = \left\{ |0\rangle, \ldots, |2^n - 1\rangle \right\}$ of $\mathbb{C}^{2^n}$.
  - The state of $Q$ is given by $|\phi\rangle_Q \in \mathscr{U}\left(\mathbb{C}^{2^n}\right)$, where

$$\mathscr{U}\left(\mathbb{C}^{2^n}\right) = \left\{ \sum_i \alpha_i |i\rangle \ : \ \sum_i |\alpha_i|^2 = 1 \right\}$$

# The Quantum World

## Basics of Quantum Computing

- All operations on a quantum state are unitary.*
- For any computable function $f : \mathcal{X} \to \mathcal{Y}$

$$\mathbf{U}_f |x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle.$$

- Copying is forbidden!

**No Cloning**

$$\begin{aligned} \mathbf{U}|\phi\rangle \otimes |\rho\rangle &= |\phi\rangle \otimes |\phi\rangle \\ \mathbf{U}|\psi\rangle \otimes |\rho\rangle &= |\psi\rangle \otimes |\psi\rangle \end{aligned} \implies \langle \phi | \psi \rangle = \langle \phi | \psi \rangle^2$$

$\langle \phi | \psi \rangle = 1$ or $\langle \phi | \psi \rangle = 0$

* Self-adjoint matrices

# The Quantum World

## Basics of Quantum Computing

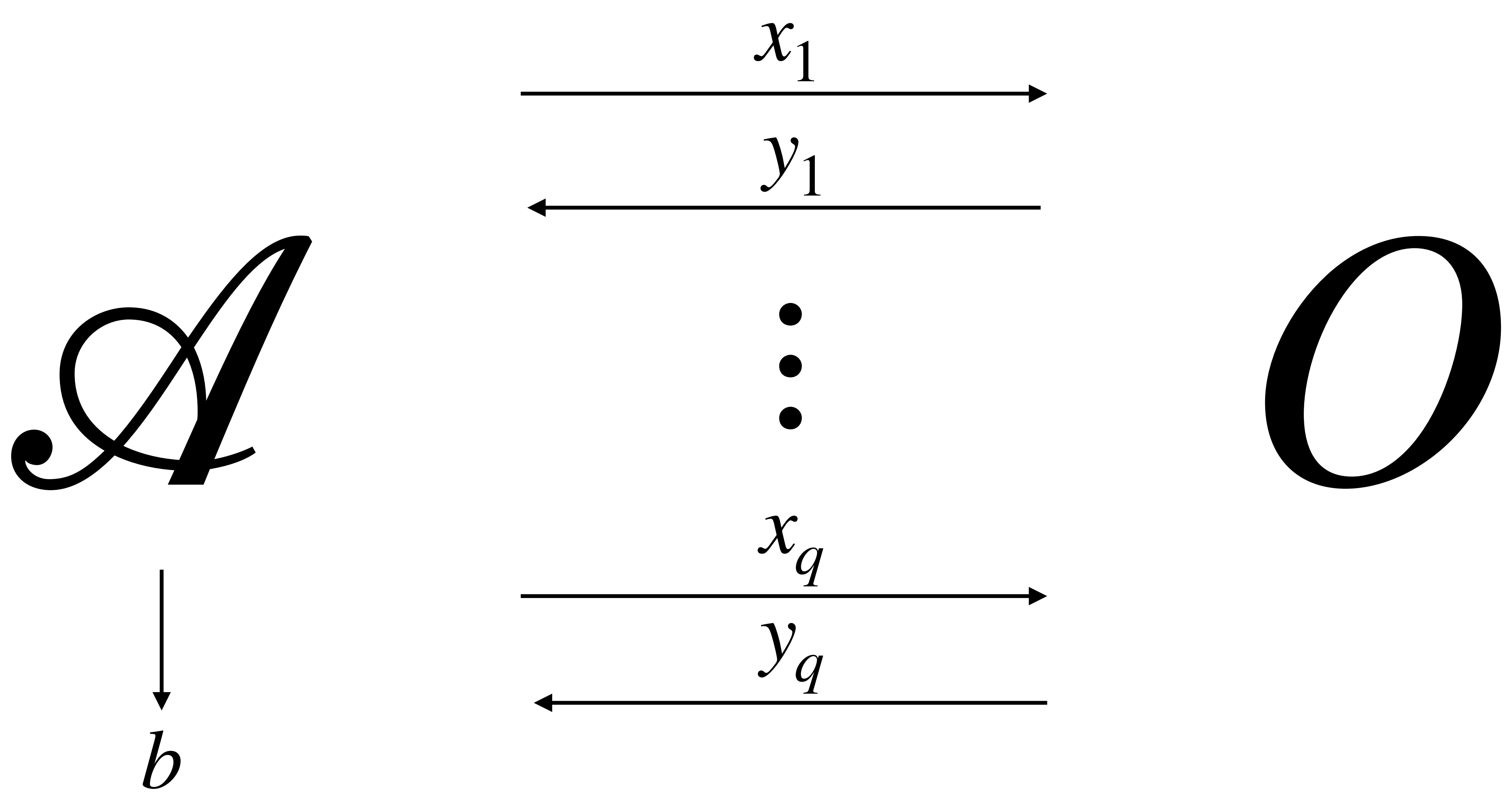
- Measurement collapses the state to one of the basis element probabilistically.

$|\phi\rangle_Q \longrightarrow$  $\longrightarrow |y\rangle$ with probability $|\langle y|\phi\rangle|^2$ .

$\mathscr{B}_{\mathscr{Y}}$

# The Quantum World

## Modelling Quantum Indistinguishability Game



# The Quantum World

## Modelling Quantum Indistinguishability Game

$$\mathbf{A}_q \quad \mathbf{A}_{q-1} \quad \cdots \quad \mathbf{A}_1 \quad \mathbf{A}_0$$

# The Quantum World

## Modelling Quantum Indistinguishability Game

$$\mathbf{A}_q\mathbf{O}\mathbf{A}_{q-1} \qquad \cdots \qquad \mathbf{A}_1\mathbf{O}\mathbf{A}_0$$

# The Quantum World

## Modelling Quantum Indistinguishability Game

$$|\phi_q\rangle = \mathbf{A}_q \mathbf{O} \mathbf{A}_{q-1} \quad \cdots \quad \mathbf{A}_1 \mathbf{O} \mathbf{A}_0 |\phi_0\rangle$$

- State space of the game is given by $\mathscr{H}_{\mathscr{A}} = \mathbb{C}^{2^m} \otimes \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^w}$.
- $\mathbf{A}_i$ operates on $\mathscr{H}_{\mathscr{A}}$ and $\mathbf{O}$ only operates on $\mathbb{C}^{2^m} \otimes \mathbb{C}^{2^n}$.

# The Quantum World

## Modelling Quantum Indistinguishability Game

$$|\phi_q\rangle = \mathbf{A}_q\mathbf{O}\mathbf{A}_{q-1} \quad \cdots \quad \mathbf{A}_1\mathbf{O}\mathbf{A}_0|\phi_0\rangle$$

- State space of the game is given by $\mathscr{H}_{\mathscr{A}} = \mathbb{C}^{2^m} \otimes \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^w}$.
- $\mathbf{A}_i$ operates on $\mathscr{H}_{\mathscr{A}}$ and $\mathbf{O}$ only operates on $\mathbb{C}^{2^m} \otimes \mathbb{C}^{2^n}$.
- Stateful Oracle: $\mathbf{O}$ operates on $\mathbb{C}^{2^m} \otimes \mathbb{C}^{2^n} \otimes \mathscr{H}_{db}$.
  - State space of this updated game is given by $\mathscr{H}_{\mathscr{A}} \otimes \mathscr{H}_{db}$.

# Simulating Random Function

# Simulating Random Function

## The Recording Problem

- Random unitary representation:
  - Sample $f \xleftarrow{\$} \mathscr{F}(m, n)$ and give access to $\mathbf{RO} = \mathbf{U}_f$.
  - No provision for recording entries.
  - Defining badness is hard.

# Simulating Random Function

## The Recording Problem

- Random unitary representation:
  - Sample $f \longleftarrow_\$ \mathscr{F}(m, n)$ and give access to $\mathbf{RO} = \mathbf{U}_f$.
  - No provision for recording entries.
  - Defining badness is hard.
- Lazy Sampling (?)

$$\mathbf{U}'_f |x\rangle_{in} \otimes |y\rangle_{out} \otimes |\{\}\rangle_{db} = |x\rangle_{in} \otimes |y \oplus u\rangle_{out} \otimes |\{(x, u)\}\rangle_{db}$$

  - A curious adversary can detect this!

# Zhandry's Compressed Oracle

[Zhandry 2019]

- Standard Oracle

$$\mathbf{stO}\,|x\rangle_{in}\,|y\rangle_{out} \otimes |f\rangle_{db} = |x\rangle_{in}\,|y \oplus f(x)\rangle_{out} \otimes |f\rangle_{db}$$

- $\mathbf{stO} \approx \mathbf{RO}$ if the database state is initialised in

$$|\,\hat{\mathbf{0}}\,\rangle = \frac{1}{2^{n2^{m/2}}} \sum_{f \in \mathcal{F}(m,n)} |f\rangle$$

Still there is no recording!

# Zhandry's Compressed Oracle

[Zhandry 2019]

- Standard Oracle

$$\mathbf{stO}\,|x\rangle_{in}\,|y\rangle_{out} \otimes |f\rangle_{db} = |x\rangle_{in}\,|y \oplus f(x)\rangle_{out} \otimes |f\rangle_{db}$$

- $\mathbf{stO} \approx \mathbf{RO}$ if the database state is initialised in

$$|\,\hat{\mathbf{0}}\,\rangle = \frac{1}{2^{n2^{m}/2}} \sum_{f \in \mathcal{F}(m,n)} |f\rangle$$

- Zhandry's seminal idea: $\mathbf{stO}$ in the Fourier view enables some recording

$$\mathbf{stO}\,|x\rangle\,|\,\hat{y}\,\rangle \otimes |\hat{f}\rangle = |x\rangle\,|\,\hat{y}\,\rangle \otimes |\hat{f} + \hat{\delta}_{xy}\rangle$$

$$\delta_{xy}(z) = \begin{cases} y & \text{when } z = x, \\ 0 & \text{otherwise,} \end{cases}$$

# Zhandry's Compressed Oracle

## Databases and Compression

**Database and Properties**

Let $\mathscr{D} = \left\{d : \{0,1\}^m \to \{0,1\}^n \cup \{ \perp \}\right\}$. A property $\mathscr{P}$ is a subset of $\mathscr{D}$.

- Cell and Database Compression

$$\mathbf{comp}_x := |\,\hat{0}\,\rangle\langle\,\perp\,| + |\,\perp\,\rangle\langle\,\hat{0}\,| + \sum_{\hat{y}\neq\hat{0}} |\,\hat{y}\,\rangle\langle\,\hat{y}\,| \qquad \mathbf{comp} = \bigotimes_x (\mathbf{I}_{m+n} \otimes \mathbf{comp}_x)$$

- Compressed Oracle

$$\mathbf{cO} := \mathbf{comp} \circ \mathbf{stO} \circ \mathbf{comp}$$

# Zhandry's Compressed Oracle

## Transition Capacity

### Transition Capacity

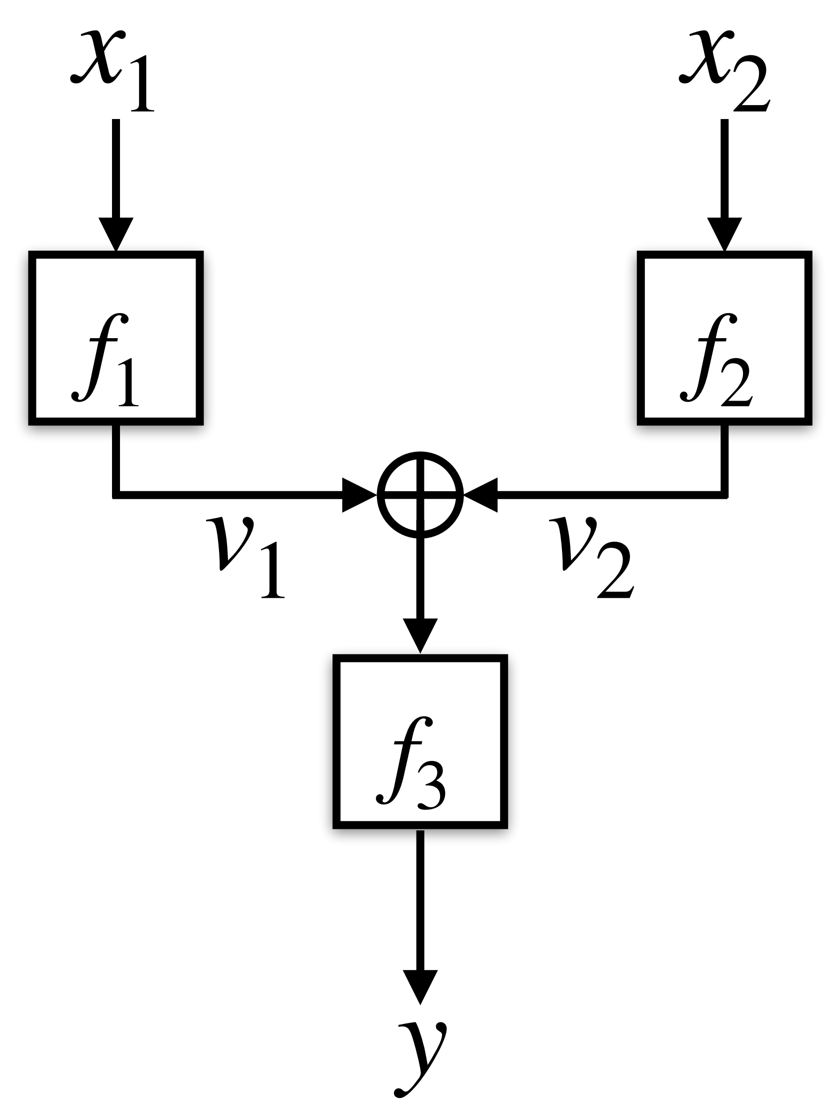
It measures the probability that a database not in property $\mathscr{P}$ transitions into $\mathscr{P}$ after a single query.

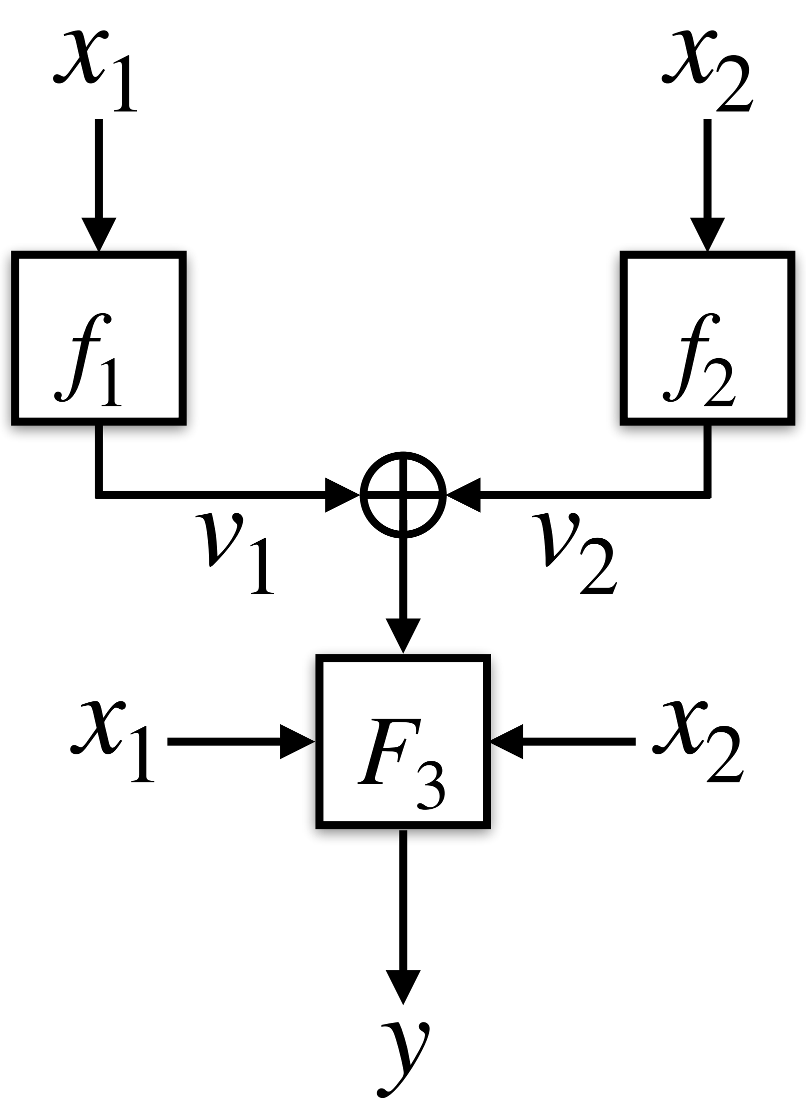
### Lemma [Chung et al. 2020]

$$\mathrm{TC}(\mathscr{P}) \leq \max_{x,d} O\left(\sqrt{\frac{|y \in \mathscr{Y} \,:\, d \cup (x,y) \in \mathscr{P}|}{2^n}}\right)$$

# Proofs in the Quantum World

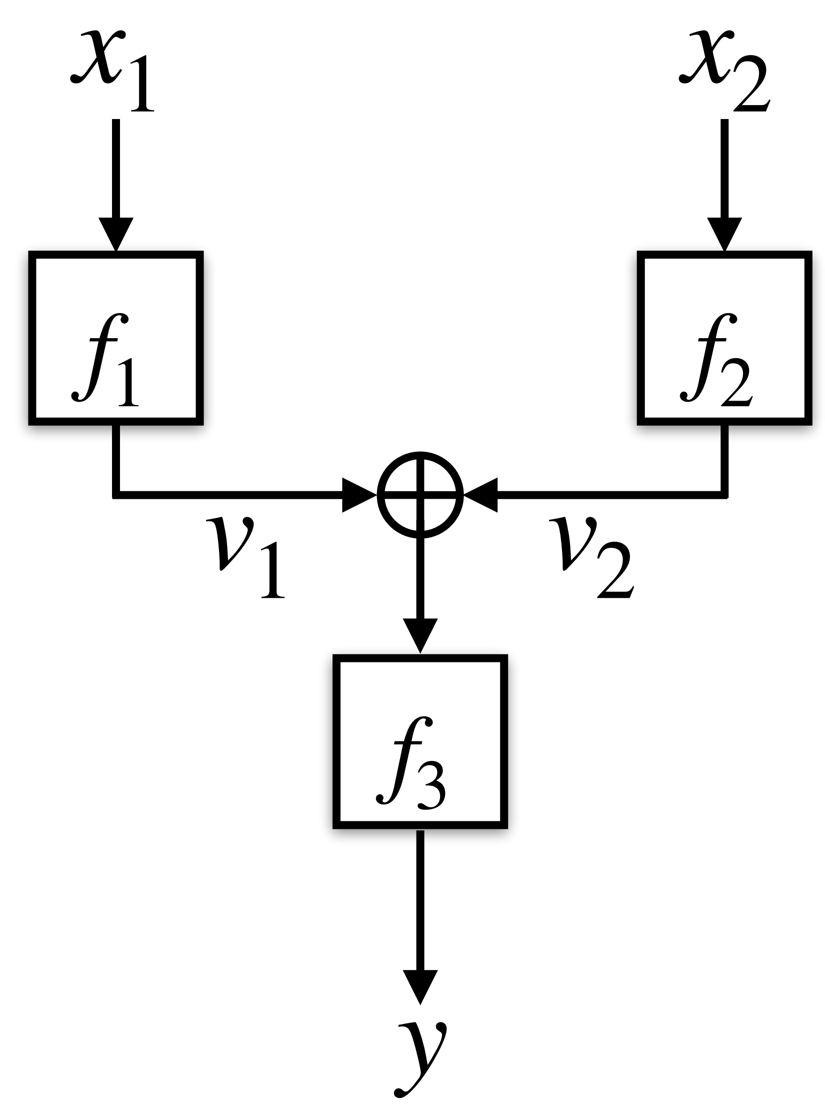
## Revisiting the Case of LRWQ

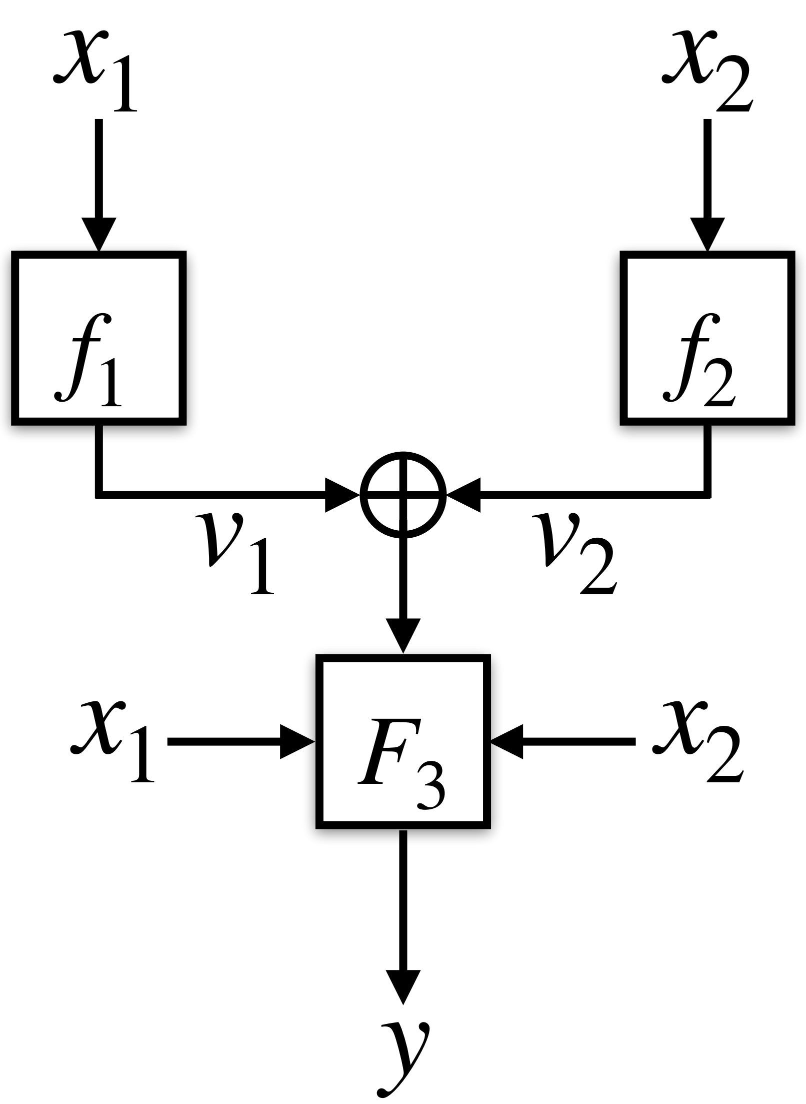


# Proofs in the Quantum World

## Revisiting the Case of LRWQ

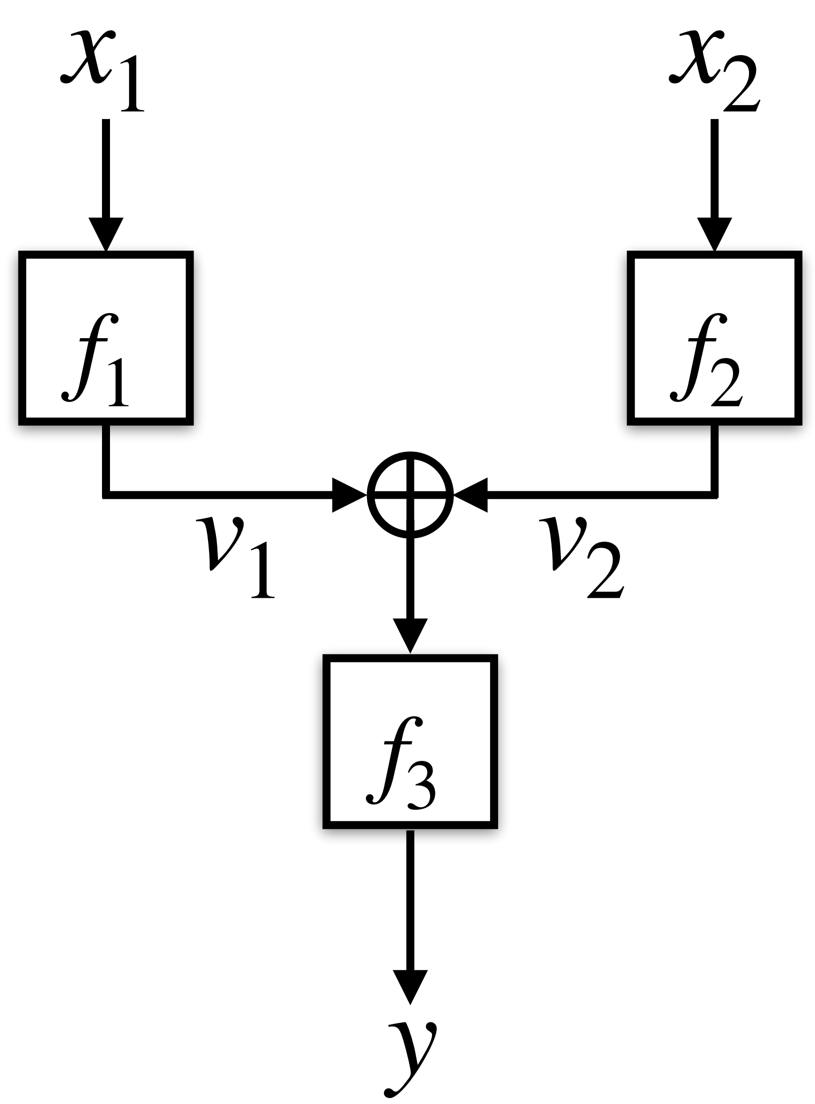


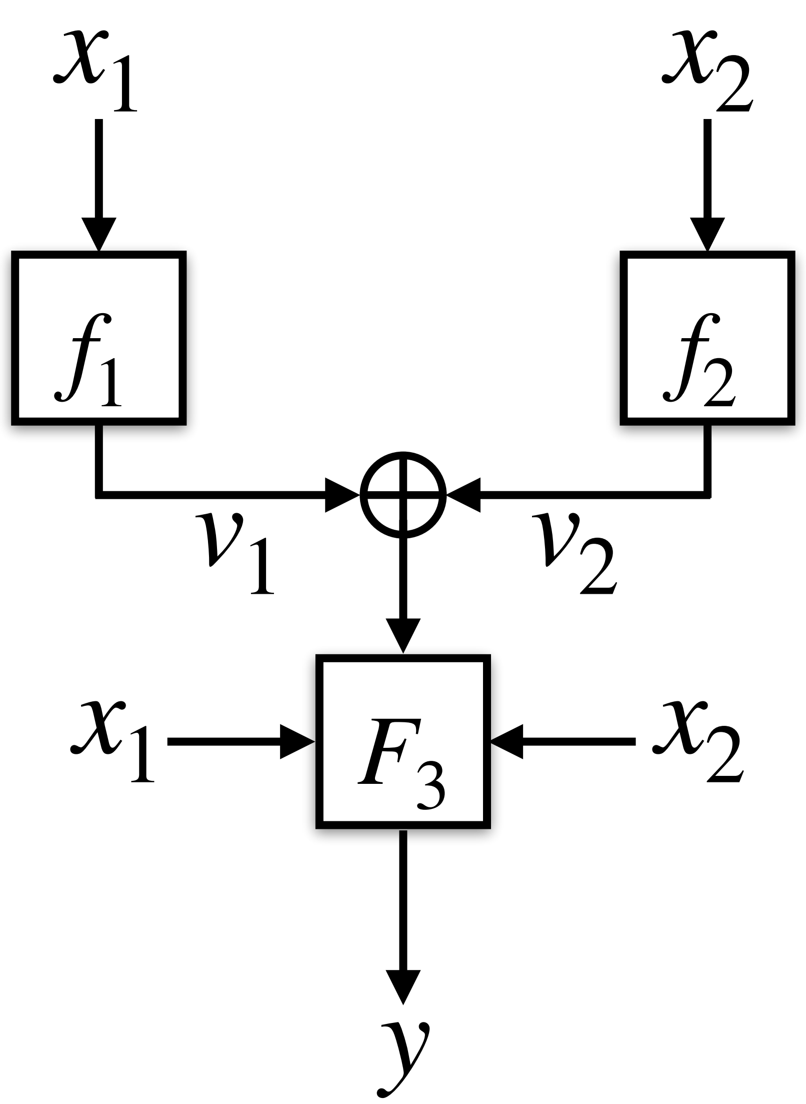




- Adversarial query pattern is unknown to the oracle.
- Only database entries are known.
- Action of each function is studied in sequence.
- All the properties must be defined over the database entries only.

# Proofs in the Quantum World

## Revisiting the Case of LRWQ



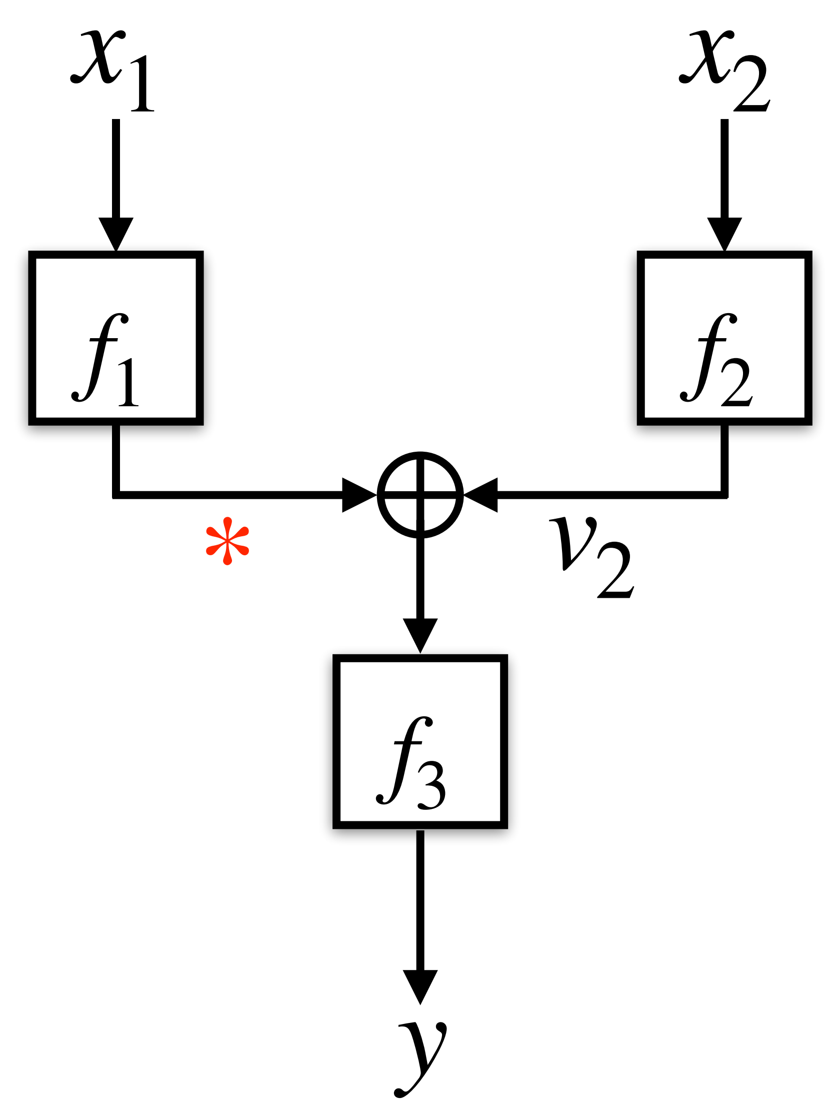

**Bad Databases ($\mathscr{P}$)**

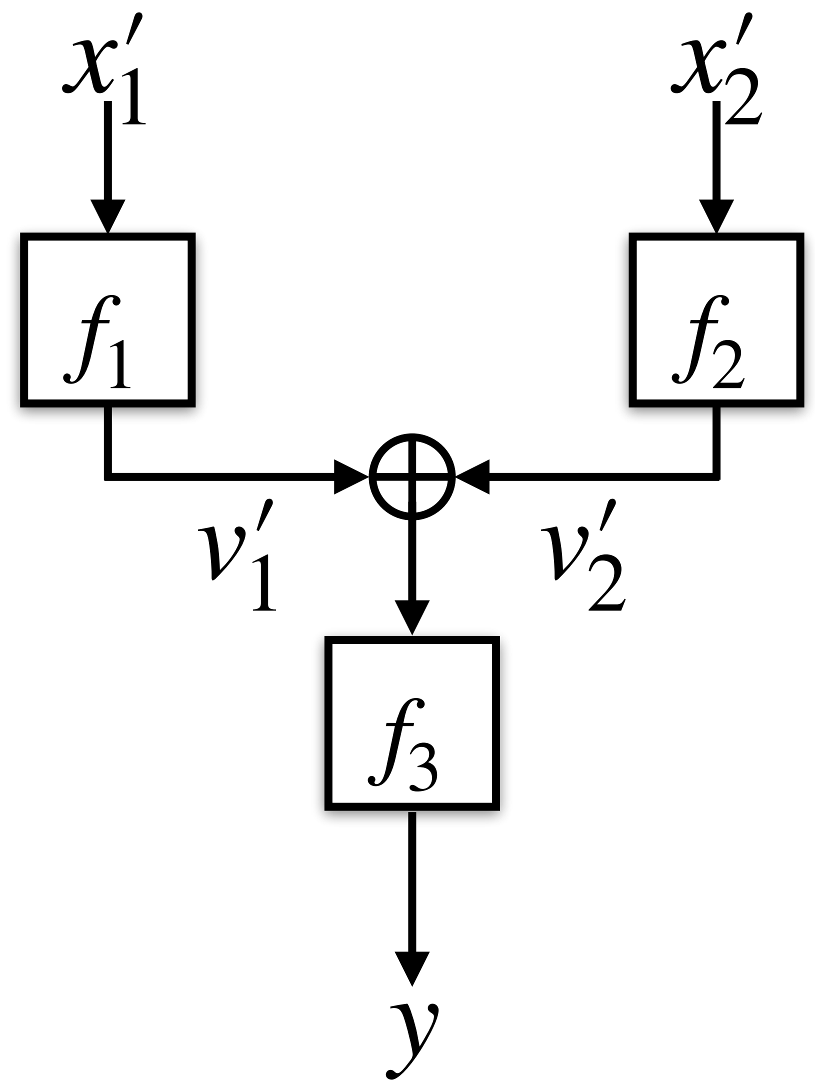
There exists entries $(x_1, v_1), (x_1', v_1'), (x_2, v_2), (x_2', v_2') \in d$ such that

$$v_1 \oplus v_2 = v_1' \oplus v_2'$$

# Proofs in the Quantum World

## Revisiting the Case of LRWQ



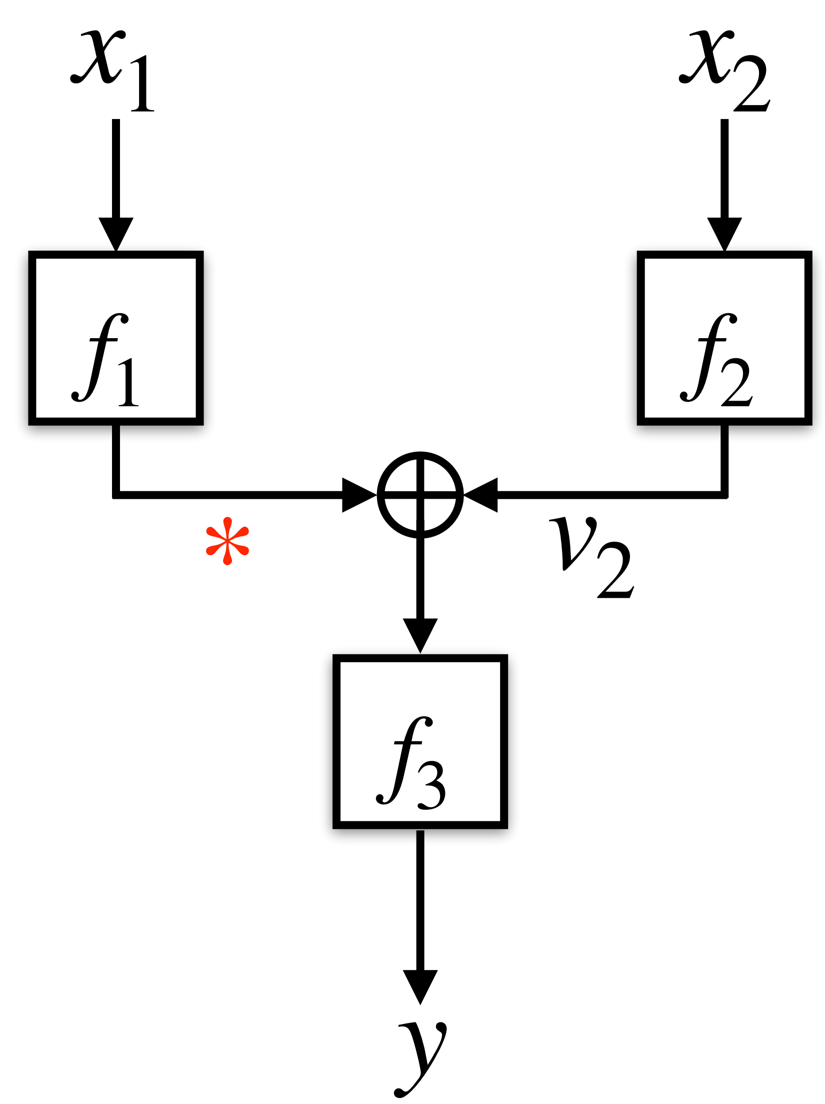



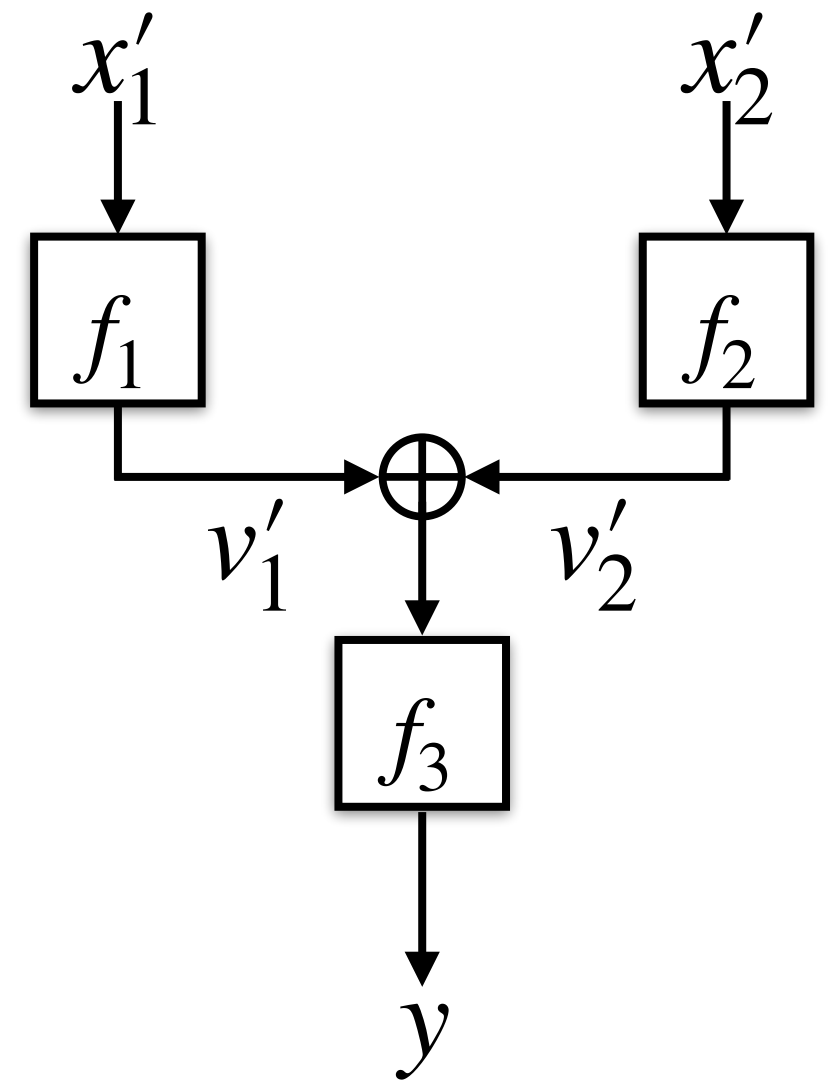

- On action of $f_1$ for a fresh $x_1$:
  - $|\{y : y \oplus v_2 = v'_1 \oplus v'_2\}| = O(q^3)$
- Similar bound for action of $f_2$.
- Combining the two:

$$\mathrm{TC}(\mathscr{P}) = O\left(\sqrt{\frac{q^3}{2^n}}\right)$$

# Proofs in the Quantum World

## Revisiting the Case of LRWQ



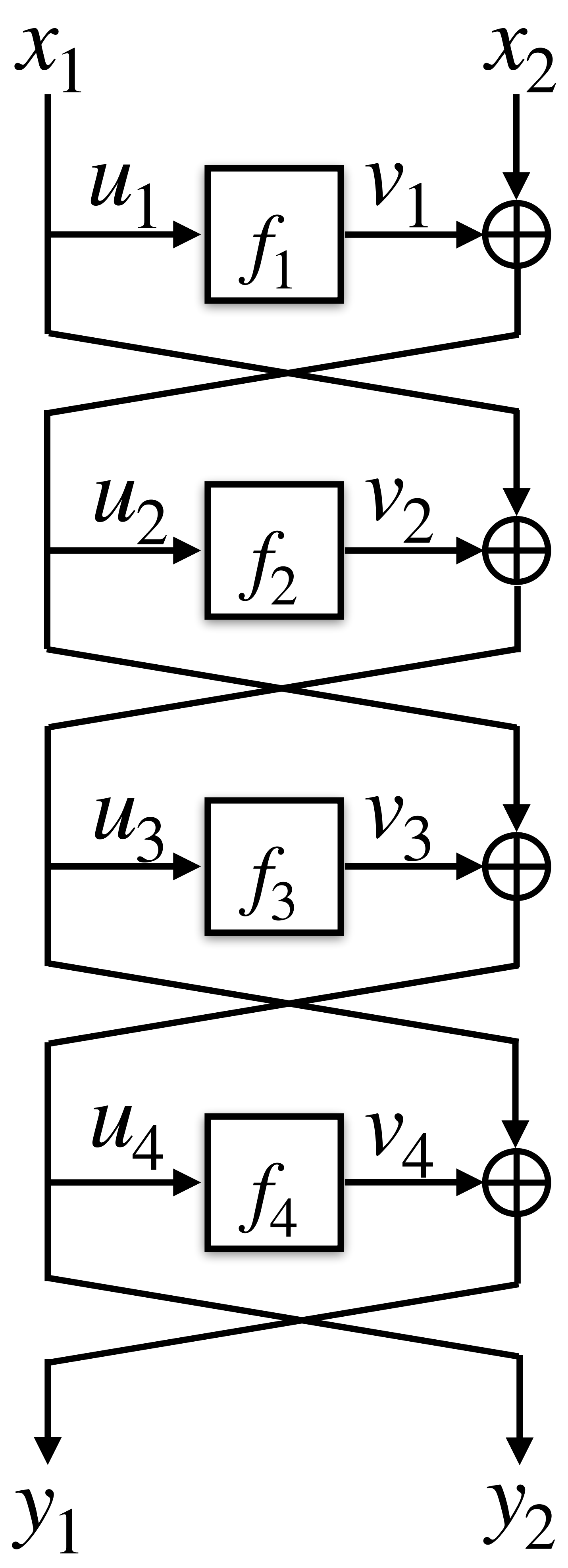

- On action of $f_1$ for a fresh $x_1$:
  - $|\{y : y \oplus v_2 = v_1' \oplus v_2'\}| = O(q^3)$
- Similar bound for action of $f_2$.
- Combining the two:

$$\mathrm{TC}(\mathscr{P}) = O\left(\sqrt{\frac{q^3}{2^n}}\right)$$

Using the TDD framework [Bhaumik et al. 2023 and 2024], $\mathbf{Adv}^{\$}_{\mathsf{LRWQ}}(\mathscr{A}) = O\left(\sqrt{\frac{q^5}{2^n}}\right)$

# Proofs in the Quantum World

## Revisiting the Case of 4LR [Hosoyamada-Iwata 2019, Bhaumik et al. 2024]




### Bad Databases

- There exists entries $(u_1, v_1), (u_1', v_1'), (u_2, v_2), (u_2', v_2') \in d$ such that

$$v_2 \oplus u_1 = v_2' \oplus u_1'$$

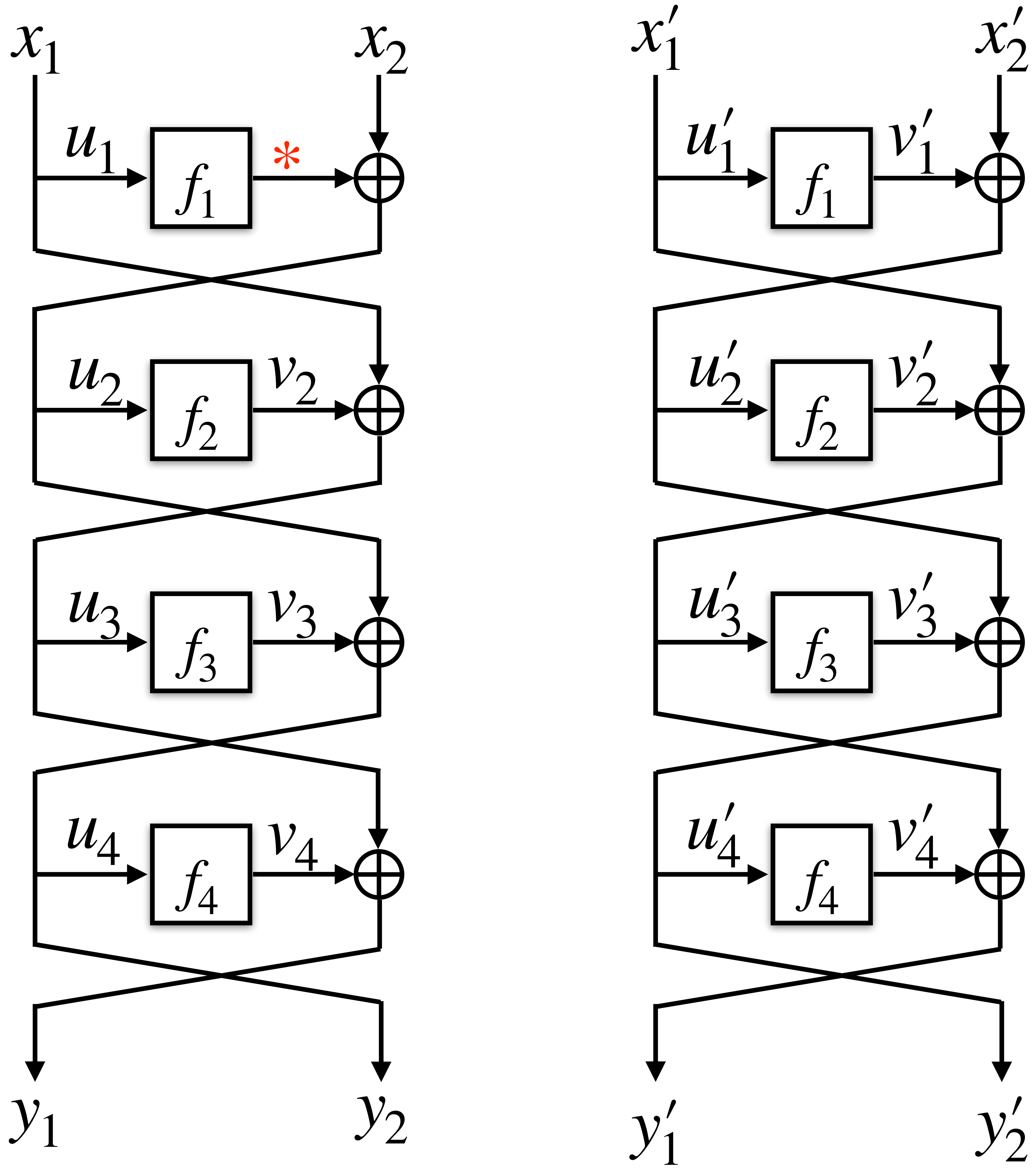
- For any $i \in [q]$ and $j \leq i - 1$

$$v_3 \oplus u_2 = v_3' \oplus u_2'$$

$$\vdots$$

# Proofs in the Quantum World

## Revisiting the Case of 4LR [Hosoyamada-Iwata 2019, Bhaumik et al. 2024]




- On action of $f_1$ for a fresh $x_1$:
  - $|\{y \,:\, x_1 \oplus v_2 = u'_1 \oplus v'_2\}| = O(2^n)$
- The property is independent of the oracle outputs.
- This results in a trivial upper bound!
- The phenomena persists even with arbitrarily large number of rounds.

# Evasive Properties

A property is said to be evasive if and only if its corresponding relation depends on certain oracle inputs while being independent of the corresponding oracle outputs.

- Some Examples:
  - Trivial example: Functions adhering to Simon's promise.
  - Bad database property for LRQ [Bhaumik et al. 2023].
  - Bad database property for LR.
  - Bad database property for TNT and LRWQ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023, Mao et al. 2023].

# Evasive Properties

A property is said to be evasive if and only if its corresponding relation depends on certain oracle inputs while being independent of the corresponding oracle outputs.

- Some Examples:
  - Trivial example: Functions adhering to Simon's promise.
  - Bad database property for LRQ [Bhaumik et al. 2023].
  - Bad database property for LR.
  - ~~Bad database property for TNT and LRWQ~~ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023, Mao et al. 2023].

Last one is more of a definitional problem!

# Evasive Properties

## An Impossibility Result

**Theorem (informal)**

The transition capacity for any evasive property $\mathscr{P}$ is trivial, i.e., $\mathsf{TC}(\mathscr{P}) \leq 1$.

Thus, the quantum identical-up to-bad argument only works for non-evasive properties.

# Evasive Properties

## An Impossibility Result

**Theorem (informal)**

The transition capacity for any evasive property $\mathscr{P}$ is trivial, i.e., $\mathrm{TC}(\mathscr{P}) \leq 1$.

Thus, the quantum identical-up to-bad argument only works for non-evasive properties.

The result also holds for multi-query progress measures.

# Evasive Properties

## Implications to Other Quantum Oracles

- Offshoots of Zhandry's oracle are covered:
  - Rosmanis's Oracle [Rosmanis 2021]
  - Unruh's oracle [Unruh 2023]
- MMW permutation oracle [Majenz-Malavolta-Walter 2024]
  - Slightly different (reductionist) approach.
  - Yet based on a progress measure and covered.

# Conclusion

- Zhandry's oracle has transformed the study of average-case quantum query complexity.
- Several new results in symmetric provable security.
- ZCO toolkit remains incomplete, particularly in handling the class of evasive properties.
- Incorporating more algebraic tools may offer solutions, though average-case analysis presents significant challenges.

# Conclusion

- Zhandry's oracle has transformed the study of average-case quantum query complexity.
- Several new results in symmetric provable security.
- ZCO toolkit remains incomplete, particularly in handling the class of evasive properties.
- Incorporating more algebraic tools may offer solutions, though average-case analysis presents significant challenges.

Thank you!