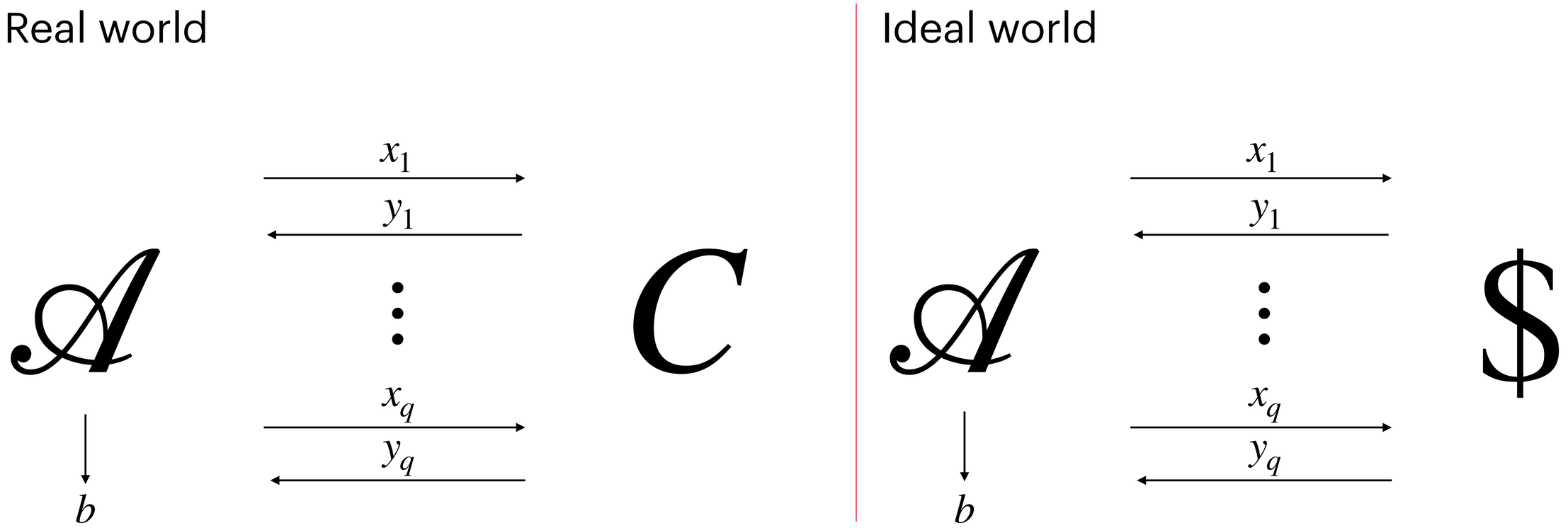
Evasive Properties

A Gap in the Quantum Oracles Zoo

Ashwin Jha
Ruhr University of Bochum

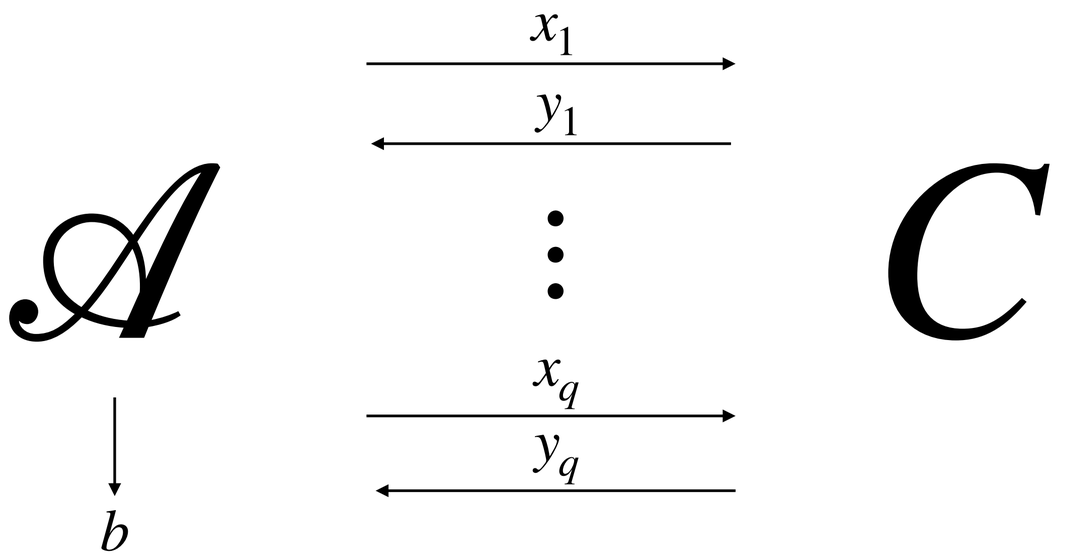
The Indistinguishability Game

The Indistinguishability Game

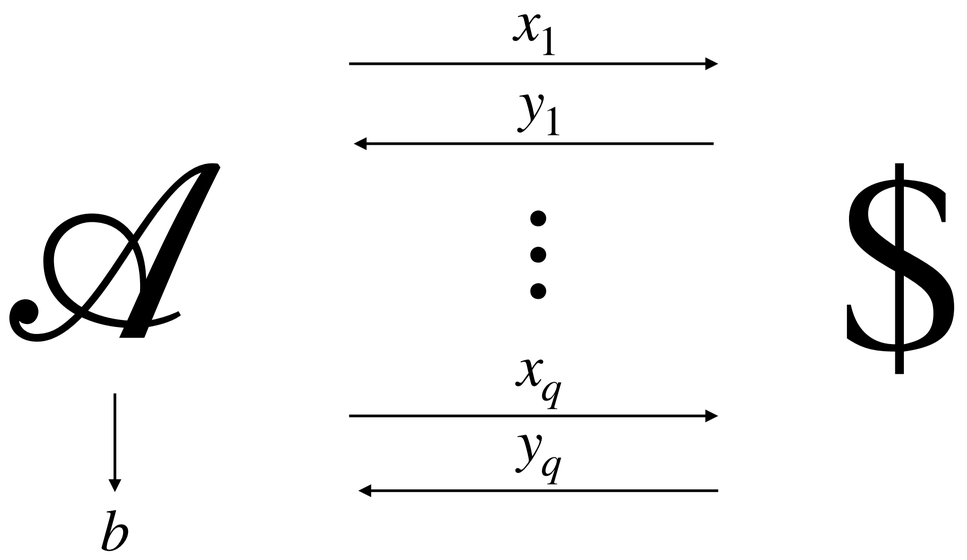


The Indistinguishability Game

Real world



Ideal world

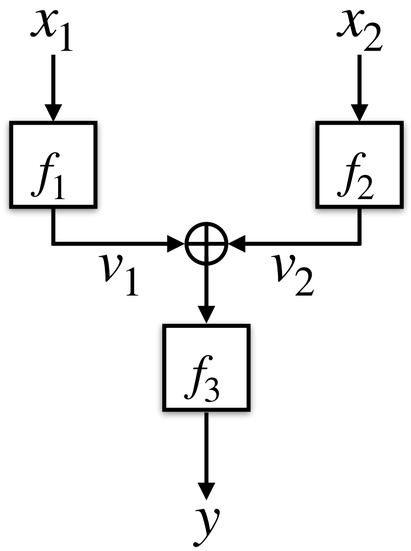


$$\mathbf{Adv}^{\$}_{C}(\mathscr{A}) := \left|\Pr\left(b = 1 \text{ in the real world}\right) - \Pr\left(b = 1 \text{ in the ideal world}\right)\right|$$

Typical Proofs in the Classical World

Typical Proofs in the Classical World

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

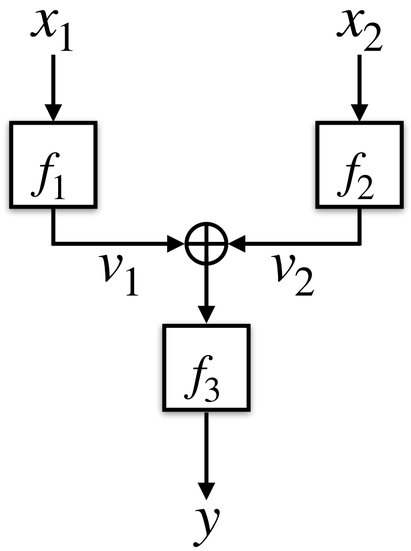


LRWQ

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

Typical Proofs in the Classical World

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



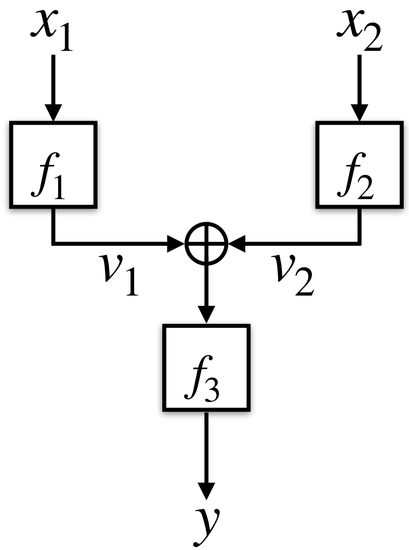
$$f_1, f_2, f_3 \xleftarrow{\$} \mathscr{F}(n, n)$$

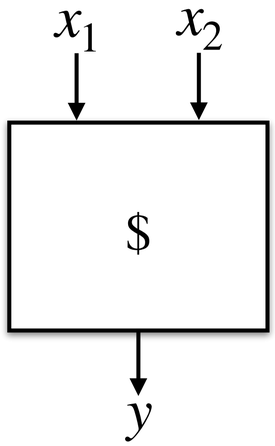
Theorem [Liskov-Rivest-Wagner 2002]

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

Typical Proofs in the Classical World

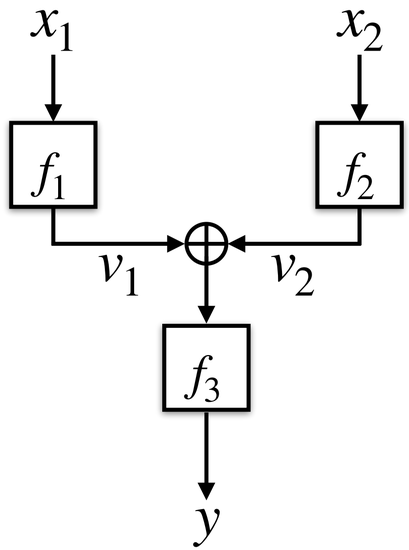
The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]

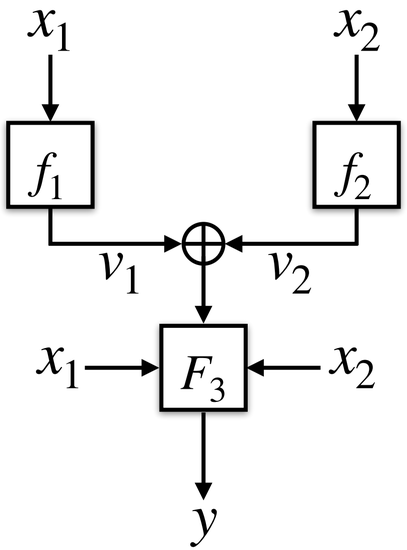




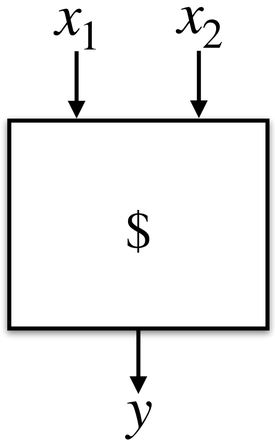
Typical Proofs in the Classical World

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





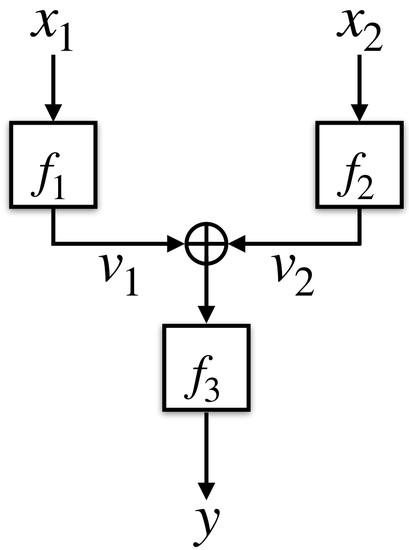
LRWQ'

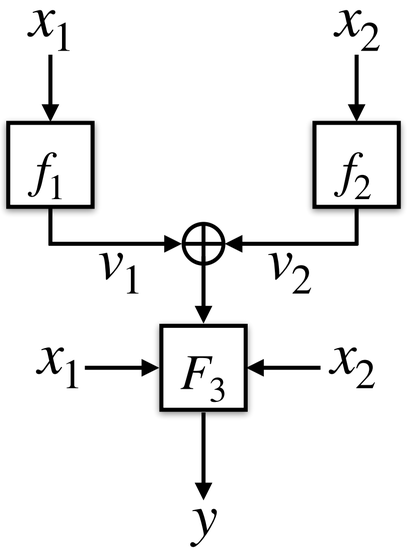


$$F_3 \xleftarrow{\$} \mathscr{F}(3n, n)$$

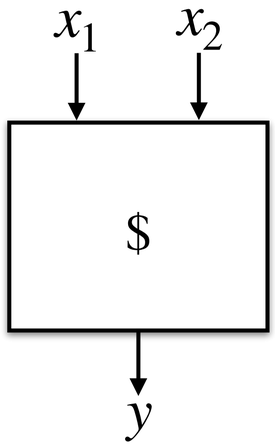
Typical Proofs in the Classical World

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



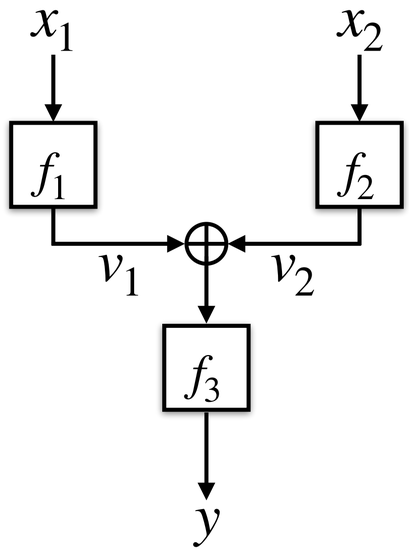


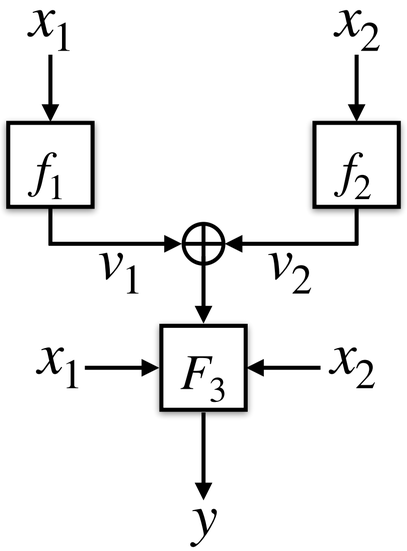
$\equiv$



Typical Proofs in the Classical World

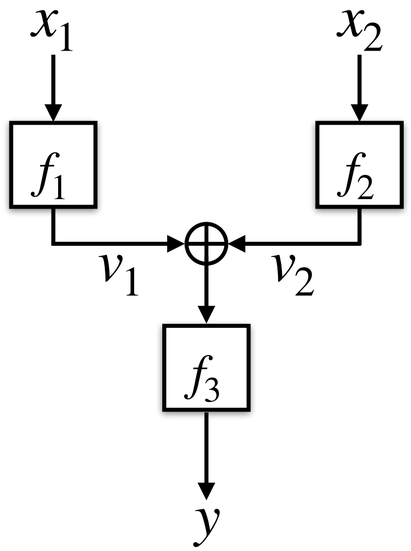
The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]

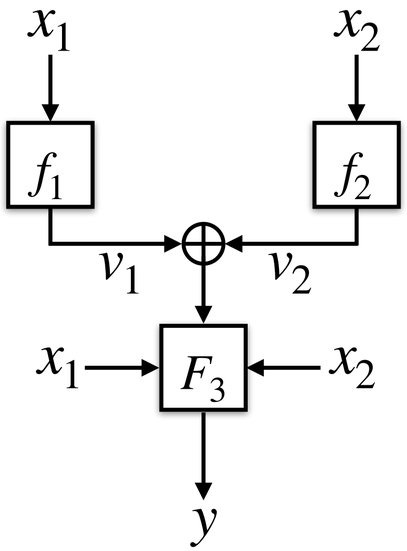




Typical Proofs in the Classical World

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





$$f_1(x_1) := g(00 \parallel 0^{2n} \parallel x_1)$$
$$f_2(x_2) := g(01 \parallel 0^{2n} \parallel x_2)$$
$$f_3(v_1 \oplus v_2) := g(10 \parallel 0^{2n} \parallel v_1 \oplus v_2)$$
$$F_3(x_1, x_2, v_1 \oplus v_2) := g(11 \parallel x_1 \parallel x_2 \parallel v_1 \oplus v_2)$$

$$g \xleftarrow{\$} \mathcal{F}(3n+2, n)$$

Typical Proofs in the Classical World

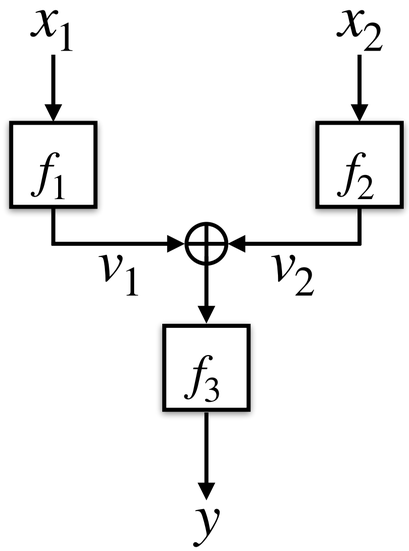
The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]

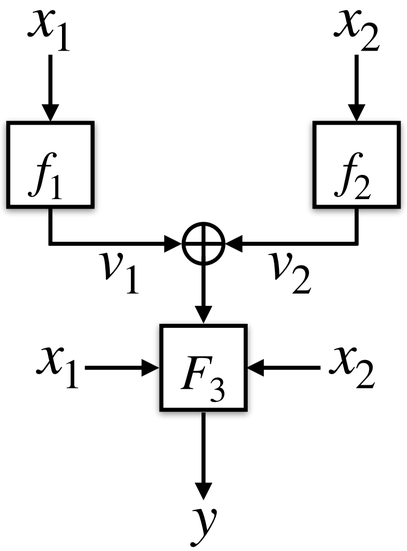
Database and Lazy Sampling

- 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 $d(x) = y \xleftarrow{\$} \{0,1\}^n$
  - Return $d(x)$

Typical Proofs in the Classical World

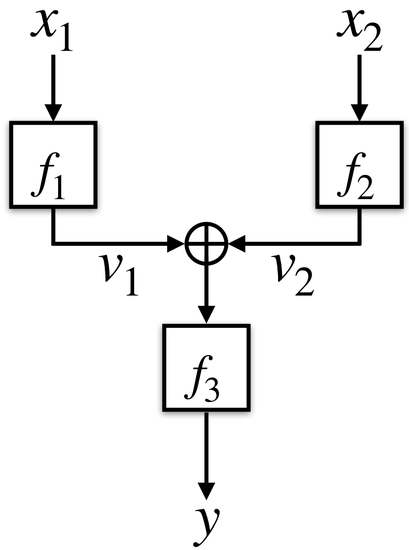
The Case of LRWQ [Liskov-Rivest-Wagner 2002, Hosoyamada-Iwata 2020]

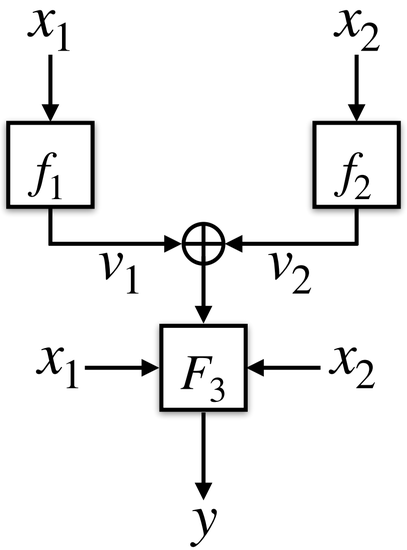




Typical Proofs in the Classical World

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





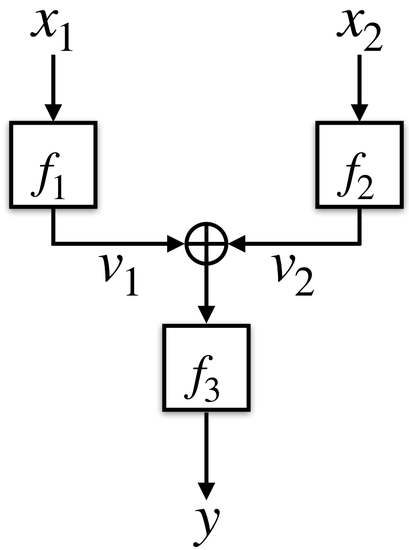
If for all $i \in [q]$ and $j \leq i - 1$

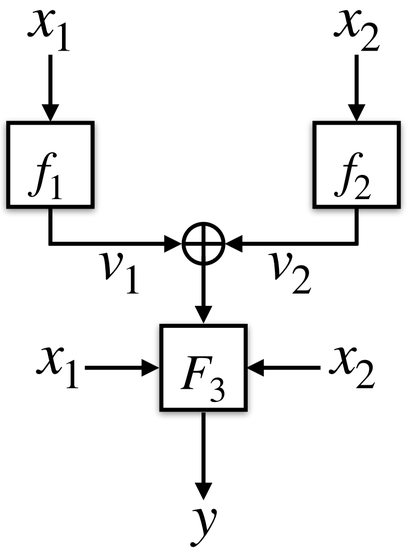
$$v_1^i \oplus v_2^i \neq v_1^j \oplus v_2^j$$

then LRWQ and LRWQ' *behave identically*.

Typical Proofs in the Classical World

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





If for all $i \in [q]$ and $j \leq i - 1$

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

then LRWQ and LRWQ' *behave identically*.

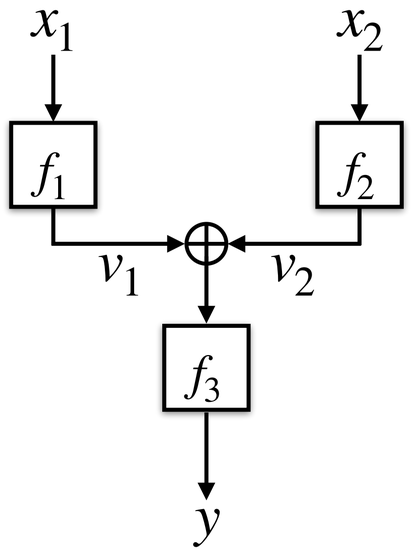
Bad Databases

A database d is *bad* if there exists entries $(x_1, v_1), (x_1', v_1'), (x_2, v_2), (x_2', v_2') \in d$ such that

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

Typical Proofs in the Classical World

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



$$\mathbf{Adv}^{\$}_{\mathrm{LRWQ}}(\mathscr{A}) \leq \Pr\left(d_q \text{ is bad}\right)$$

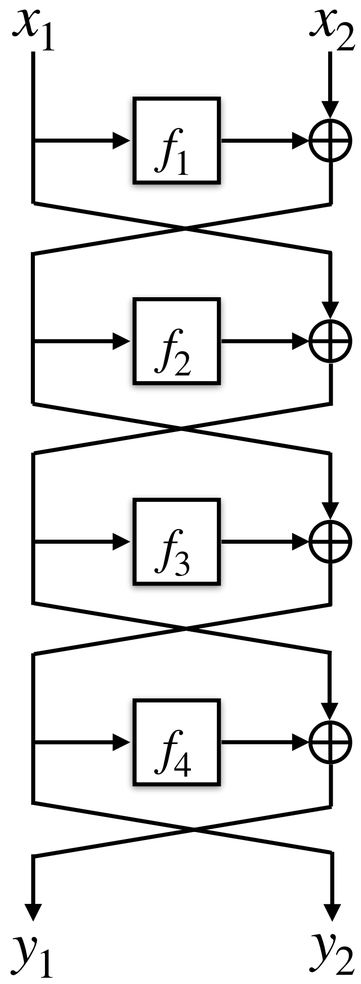
$$\leq \sum_{i=1}^{q} \Pr\left(d_i \text{ is bad } \wedge\ d_{<i} \text{ was good}\right)$$

$$\leq \sum_{i=1}^{q} O\left(\frac{i-1}{2^n}\right) \leq O\left(\frac{q^2}{2^n}\right)$$

d_i : The database snapshot at query index i .

Typical Proofs in the Classical World

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

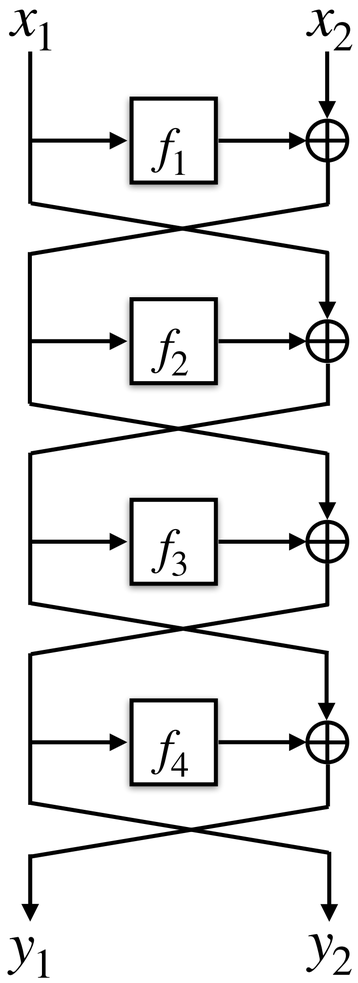


LR4

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

Typical Proofs in the Classical World

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



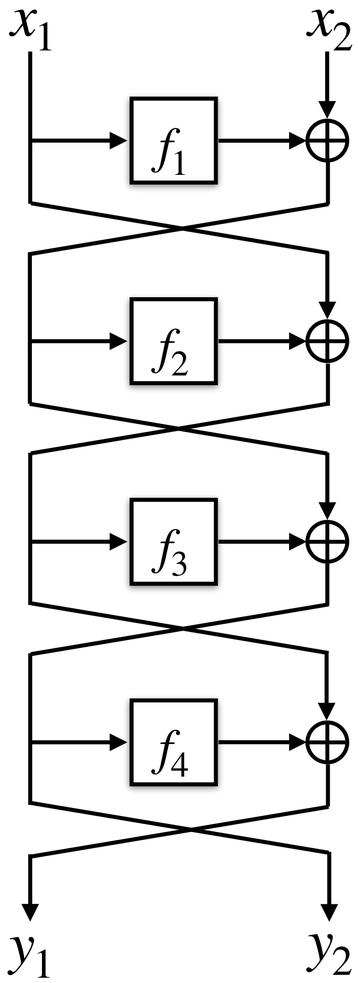
$$f_1, f_2, f_3, f_4 \xleftarrow{\$} \mathscr{F}(n,n)$$

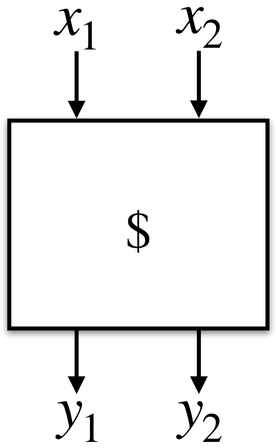
Theorem [Luby-Rackoff 1988]

$$\mathbf{Adv}^{\$}_{\mathsf{LR4}}(\mathscr{A}) = O\left(\frac{q^2}{2^n}\right)$$

Typical Proofs in the Classical World

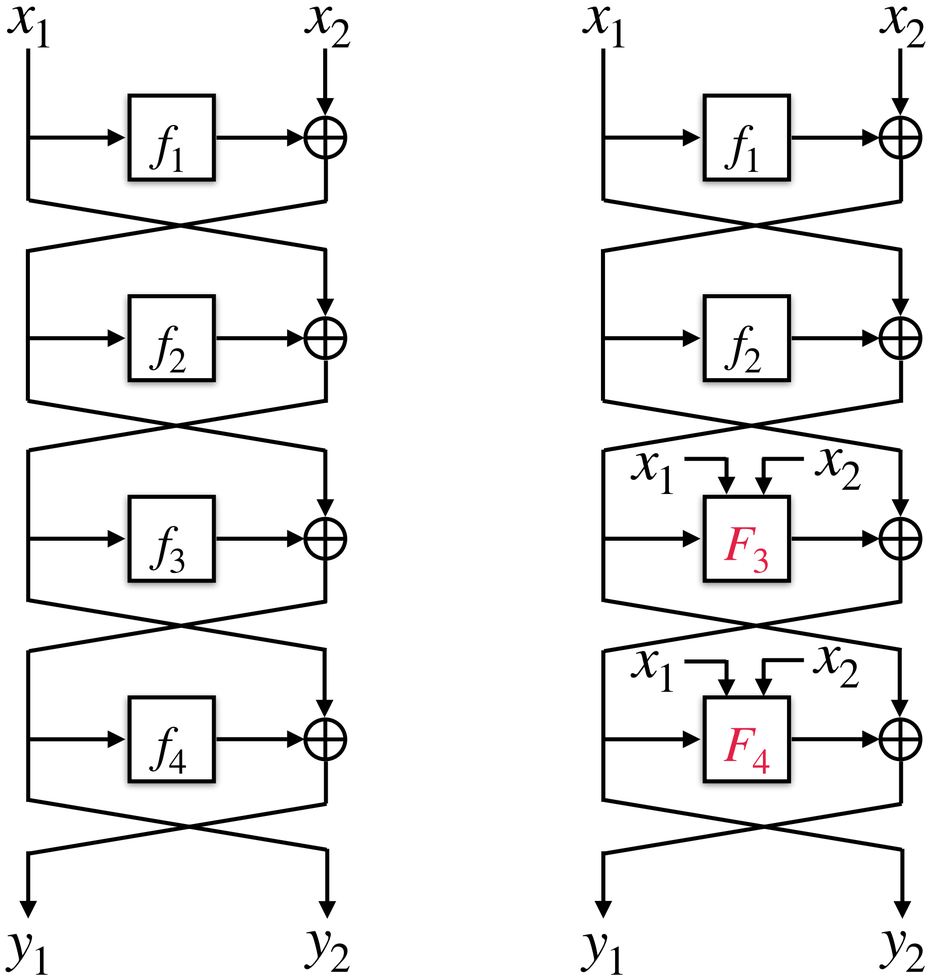
The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]



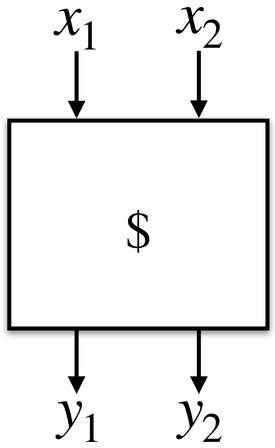


Typical Proofs in the Classical World

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

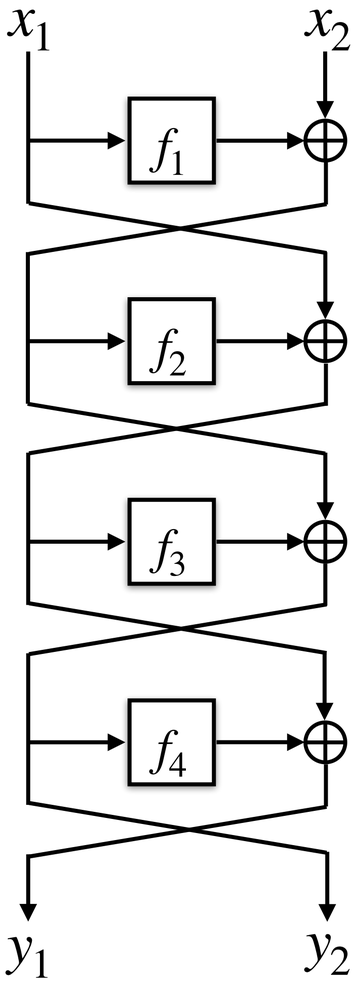


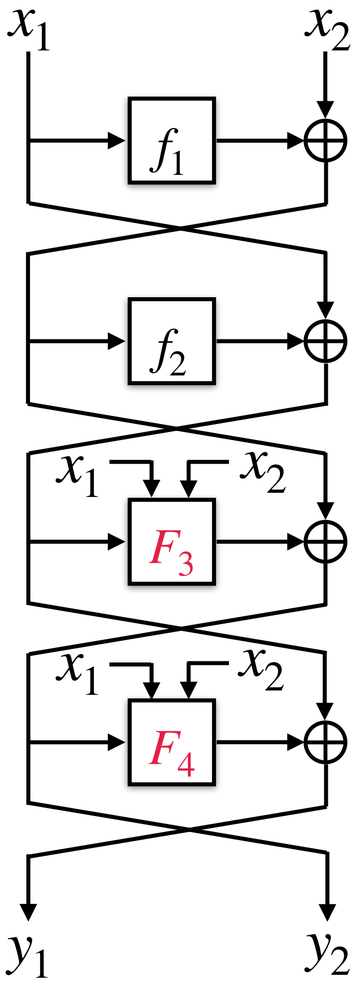
LR4'



Typical Proofs in the Classical World

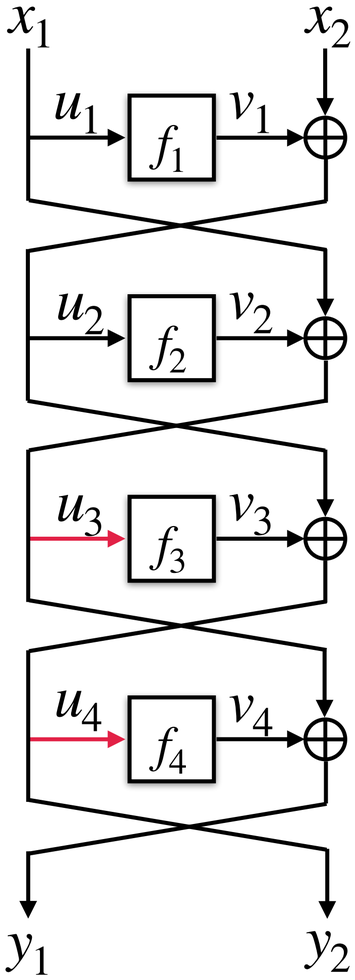
The Case of 4-round Luby-Rackoff [Luby-Rackoff 1988]

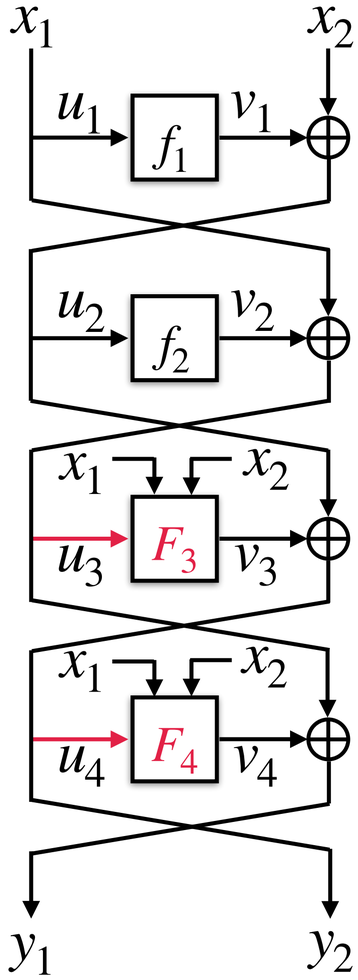




Typical Proofs in the Classical World

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





If for all $i \in [q]$ and $j \leq i - 1$

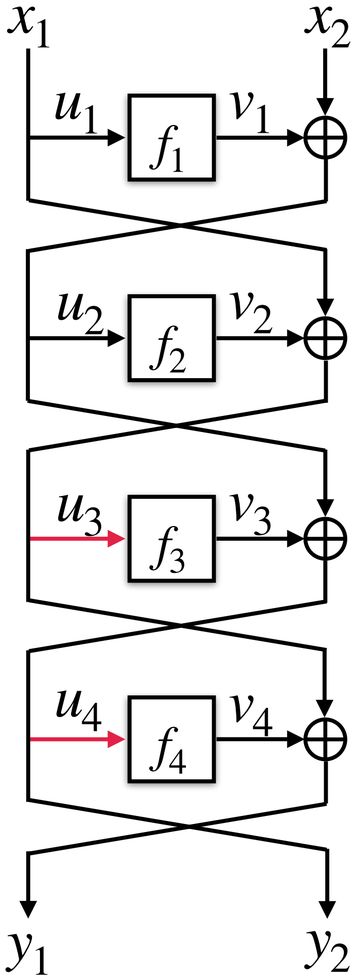
$$v_2^i \oplus u_1^i \neq v_2^j \oplus u_1^j$$

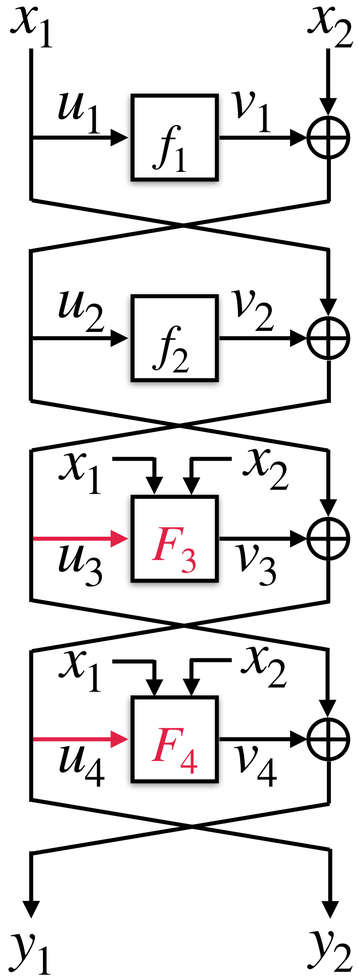
$$v_3^i \oplus u_2^i \neq v_3^j \oplus u_2^j$$

then LR4 and LR4′ *behave identically*.

Typical Proofs in the Classical World

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





Bad Databases

A database d is *bad* if

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

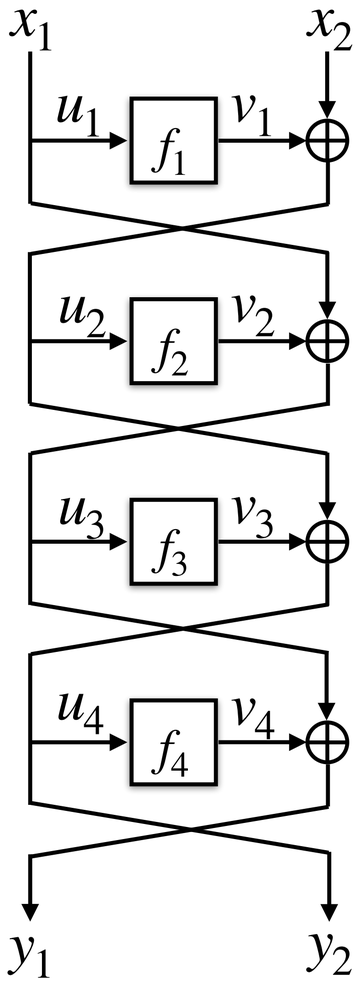
$$v_2 \oplus u_1 = v_2' \oplus u_1'$$

- or, there exists entries $(u_2, v_2), (u_2', v_2'), (u_3, v_3), (u_3', v_3') \in d$ such that

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

Typical Proofs in the Classical World

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



$$\mathbf{Adv}^{\$}_{\mathsf{LR4}}(\mathscr{A}) \leq \Pr\left(d_q \text{ is bad}\right) \leq O\left(\frac{q^2}{2^n}\right)$$

The Quantum World

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 $\mathbb{C}^{2^n}$.
  - $\mathcal{Y} = \{0,1\}^n$ is mapped to the basis $\mathcal{B}_{\mathcal{Y}} = \left\{ |0\rangle, \ldots, |2^n - 1\rangle \right\}$ of $\mathbb{C}^{2^n}$.
  - The state of Q is given by $|\phi\rangle_Q \in \mathcal{U}\left(\mathbb{C}^{2^n}\right)$, where

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

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!

* Self-adjoint matrices

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

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

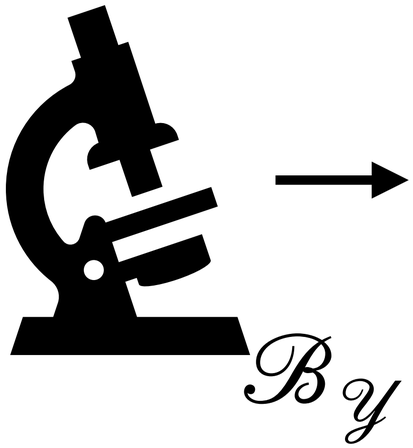
$$\langle\phi|\psi\rangle = 1 \text{ or } \langle\phi|\psi\rangle = 0$$

* Self-adjoint matrices

The Quantum World

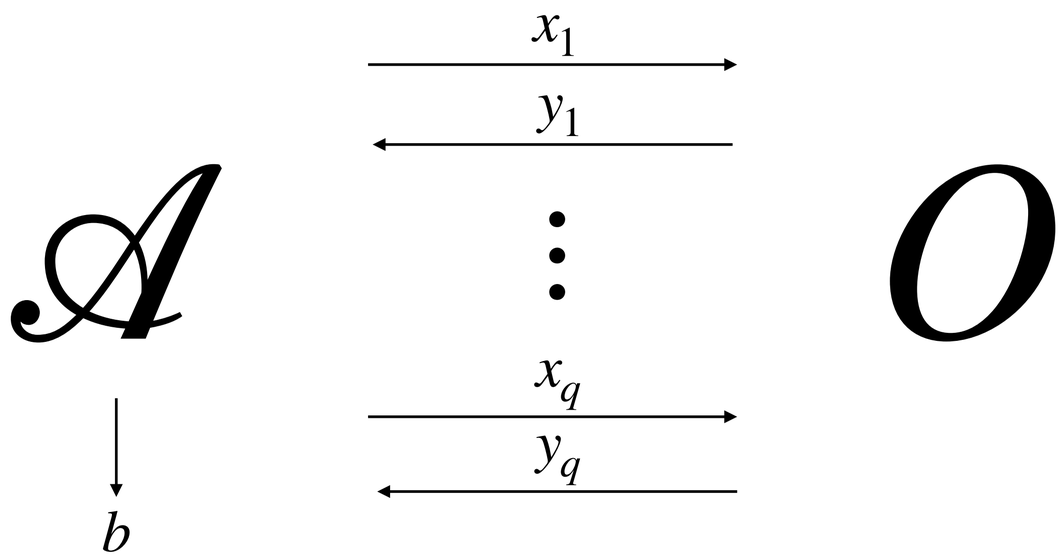
Basics of Quantum Computing

- Measurement collapses the state to some basis element probabilistically.

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

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

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

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 $\mathscr{H}_{\mathscr{A}} = \mathscr{H}_{in} \otimes \mathscr{H}_{out} \otimes \mathscr{H}_{work}$.
- $\mathbf{A}_i$ operates on $\mathscr{H}_{\mathscr{A}}$ and $\mathbf{O}$ only operates on $\mathscr{H}_{in} \otimes \mathscr{H}_{out}$.

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 $\mathscr{H}_{\mathscr{A}} = \mathscr{H}_{in} \otimes \mathscr{H}_{out} \otimes \mathscr{H}_{work}$.
- $\mathbf{A}_i$ operates on $\mathscr{H}_{\mathscr{A}}$ and $\mathbf{O}$ only operates on $\mathscr{H}_{in} \otimes \mathscr{H}_{out}$.
- Stateful Oracle: $\mathbf{O}$ operates on $\mathscr{H}_{in} \otimes \mathscr{H}_{out} \otimes \mathscr{H}_{db}$.
  - State space of this updated game is given by $\mathscr{H}_{\mathscr{A}} \otimes \mathscr{H}_{db}$.

Simulating a Random Function

Simulating a 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 a Random Function

The Recording Problem

- Random unitary representation:
  - Sample $f \xleftarrow{\$} \mathcal{F}(m,n)$ 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 *easily* detect this!

Zhandry's Compressed Oracle

[Zhandry 2019, Chung et al. 2020]

Zhandry's Compressed Oracle

[Zhandry 2019, Chung et al. 2020]

- Standard Oracle

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

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

$$|\,\widehat{\mathbf{0}}\,\rangle_{db} = \frac{1}{2^n 2^{m/2}} \sum_{f \in \mathcal{F}(m,n)} |f\rangle_{db}$$

Zhandry's Compressed Oracle

[Zhandry 2019, Chung et al. 2020]

- Standard Oracle

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

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

$$|\,\widehat{\mathbf{0}}\,\rangle_{db}=\frac{1}{2^{n}2^{m/2}}\sum_{f\in\mathcal{F}(m,n)}|f\rangle_{db}$$

Still there is no recording!

Zhandry's Compressed Oracle

[Zhandry 2019, Chung et al. 2020]

- Standard Oracle

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

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

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

- Zhandry's core idea: $\mathscr{H}_{out}\otimes\mathscr{H}_{db}$ in the *Fourier basis* enables some recording

$$\mathbf{SO}\,|x\rangle_{in}\,|\,\hat{y}\,\rangle_{out}\otimes|\hat{f}\rangle_{db}=|x\rangle_{in}\,|\,\hat{y}\,\rangle_{out}\otimes|\hat{f}+\hat{\delta}_{xy}\rangle_{db}$$

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

Zhandry's Compressed Oracle

[Zhandry 2019, Chung et al. 2020]

- $\mathscr{H}_{db}$ is equivalent to the product space

$$\bigotimes_{x} \mathscr{H}_{db[x]}$$

- Cell and Database Compression

$$\mathbf{C}_x := |\hat{0}\rangle\langle\perp|_{db[x]} + |\perp\rangle\langle\hat{0}|_{db[x]} + \sum_{\hat{y}\neq\hat{0}} |\hat{y}\rangle\langle\hat{y}|_{db[x]} \qquad \mathbf{C} = \bigotimes_{x} (\mathbf{I}_{m+n} \otimes \mathbf{C}_x)$$

- Compressed Oracle

$$\mathbf{CO} := \mathbf{C} \circ \mathbf{SO} \circ \mathbf{C}$$

Zhandry's Compressed Oracle

Databases and Properties [Zhandry 2019, Chung et al. 2020]

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 $\mathscr{D}$.

- $\mathscr{D}$ has a one-to-one correspondence with $\mathscr{H}_{db}$

$$d \longmapsto \bigotimes_x |\, d(x) \rangle_{db[x]}$$

- Each property $\mathscr{P} \subset \mathscr{D}$ corresponds to the subspace $\mathrm{span}(\mathscr{P}) \leq \mathscr{H}_{db}$

Zhandry's Compressed Oracle

Transition Capacity [Chung et al. 2020]

- How to quantify the probability of transition from $\overline{\mathscr{P}}$ to $\mathscr{P}$?

Zhandry's Compressed Oracle

Transition Capacity [Chung et al. 2020]

- How to quantify the probability of transition from $\overline{\mathscr{P}}$ to $\mathscr{P}$?
- For any $i \in [q]$, let $\mathscr{D}_{[i]} := \{d \in \mathscr{D} : |d| = i\}$ and $\mathscr{P}_{[i]} := \{d \in \mathscr{P} : |d| = i\}$

Transition Capacity

For any $\mathscr{P} \subset \mathscr{D} \backslash \{ | \perp \rangle \}$ the transition capacity at query index i is defined as:

$$\mathsf{TC}(\mathscr{P}, i) \leq \max_{\substack{x, d \\ d(x) = \perp}} \sqrt{\frac{\left| \left\{ y : d \cup \{(x, y)\} \in \mathscr{P}_{[i]} \right\} \right|}{2^n}}$$

where we maximise over all $d \in \overline{\mathscr{P}}_{[i-1]}$. $\mathsf{TC}(\mathscr{P}) := \sum_{i=1}^{q} \mathsf{TC}(\mathscr{P}, i)$.

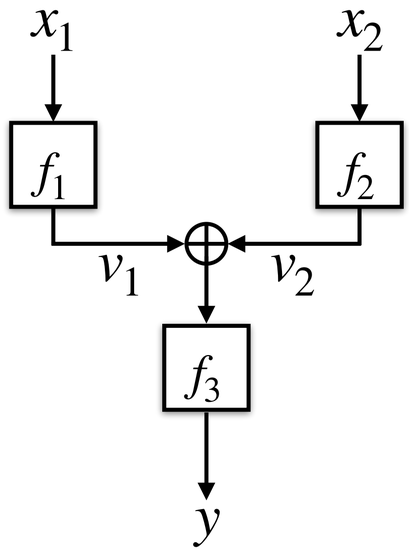
Proofs in the Quantum World

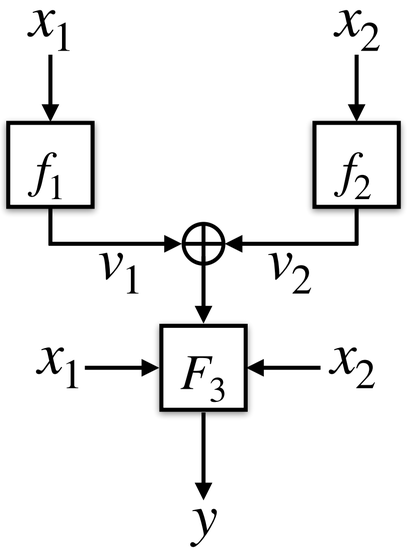
Major changes

- All internal functions are analysed in-sequence.
- Adversary's query pattern is unknown to the oracle.
- Only database entries are known.
- All the properties must be defined over the database entries only.

Proofs in the Quantum World

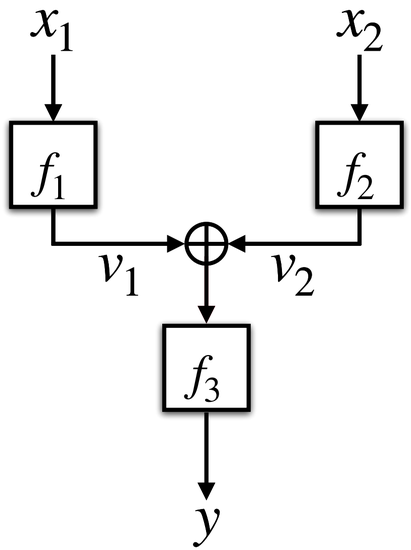
Revisiting the Case of LRWQ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023]

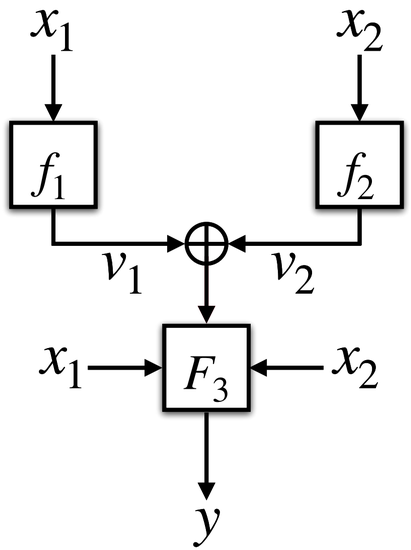




Proofs in the Quantum World

Revisiting the Case of LRWQ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023]





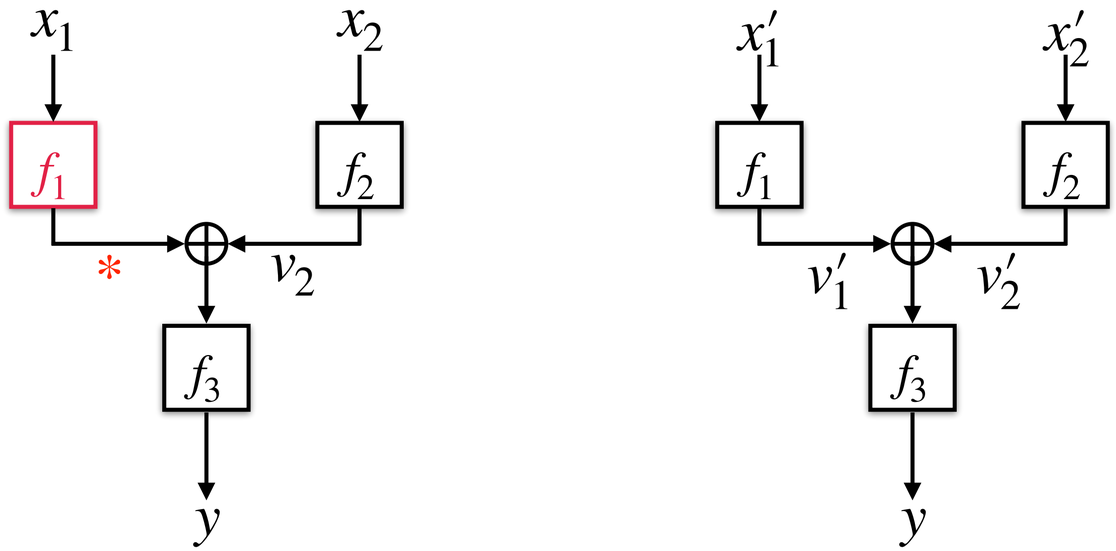
Bad Databases ($\mathscr{P}$)

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

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

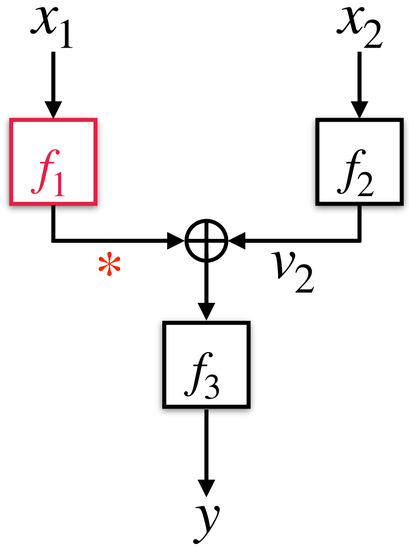
Proofs in the Quantum World

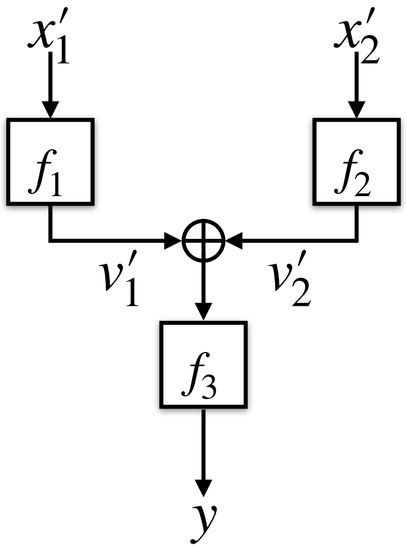
Revisiting the Case of LRWQ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023]



Proofs in the Quantum World

Revisiting the Case of LRWQ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023]





- On action of f_1 for a fresh x_1:

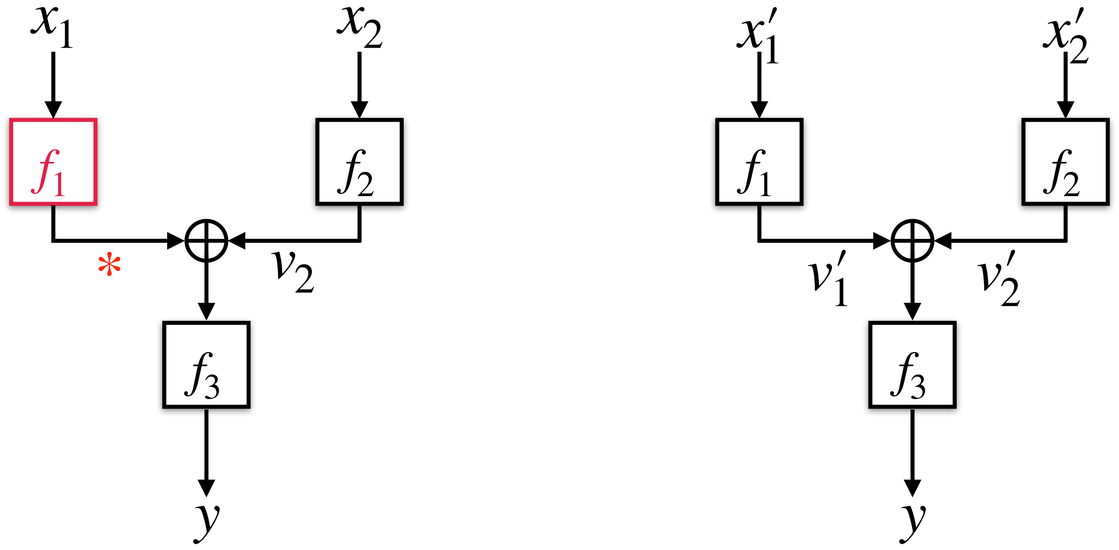
$$|\{y : y \oplus v_2 = v'_1 \oplus v'_2\}| = O(i^3)$$

- Similar bound for action of f_2.
- Combining the two:

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

Proofs in the Quantum World

Revisiting the Case of LRWQ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023]



- On action of f_1 for a fresh x_1:

$$|\{y : y \oplus v_2 = v'_1 \oplus v'_2\}| = O(i^3)$$

- Similar bound for action of f_2.
- Combining the two:

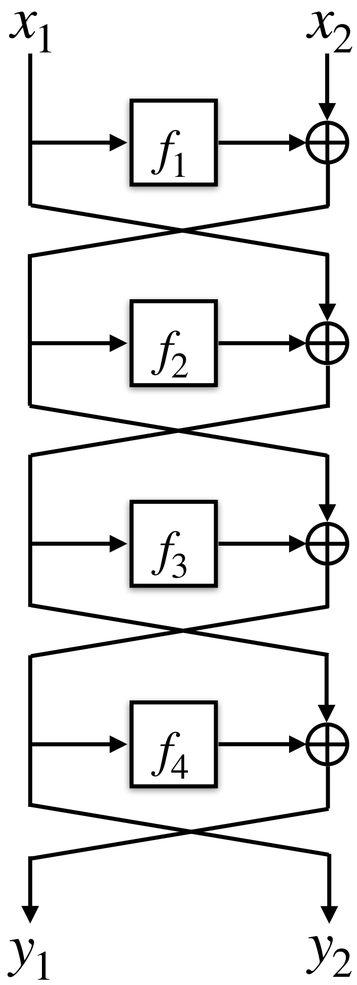
$$\mathrm{TC}(\mathscr{P}, i) = O\left(\sqrt{\frac{q^3}{2^n}}\right)$$

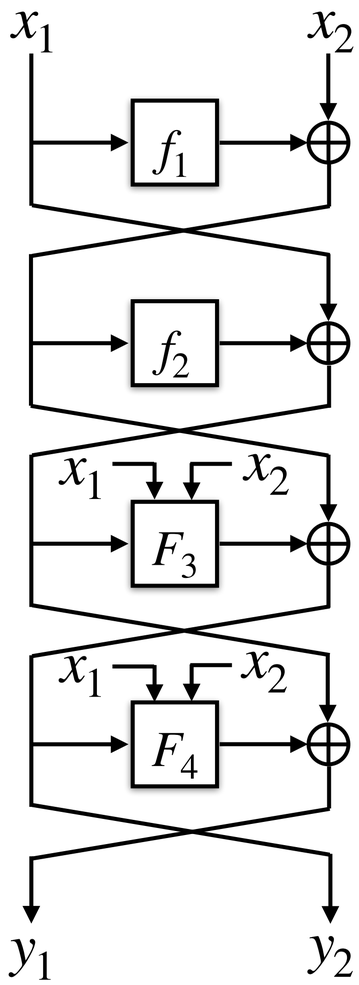
Theorem [Bhaumik et al. 2023]

$$\mathbf{Adv}^{\$}_{\mathrm{LRWQ}}(\mathscr{A}) = O(\mathrm{TC}(\mathscr{P})) = O\left(\sqrt{\frac{q^5}{2^n}}\right)$$

Proofs in the Quantum World

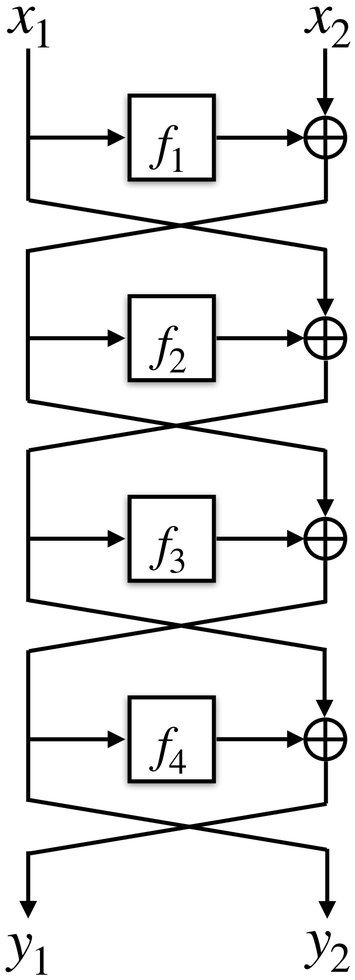
Revisiting the Case of LR4 [Hosoyamada-Iwata 2019, Bhaumik et al. 2024]

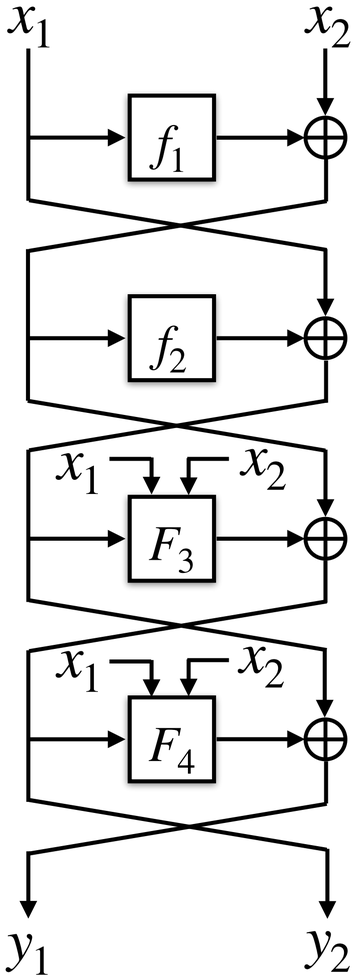




Proofs in the Quantum World

Revisiting the Case of LR4 [Hosoyamada-Iwata 2019, Bhaumik et al. 2024]





Bad Databases ($\mathscr{P}$)

A database d is *bad* if

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

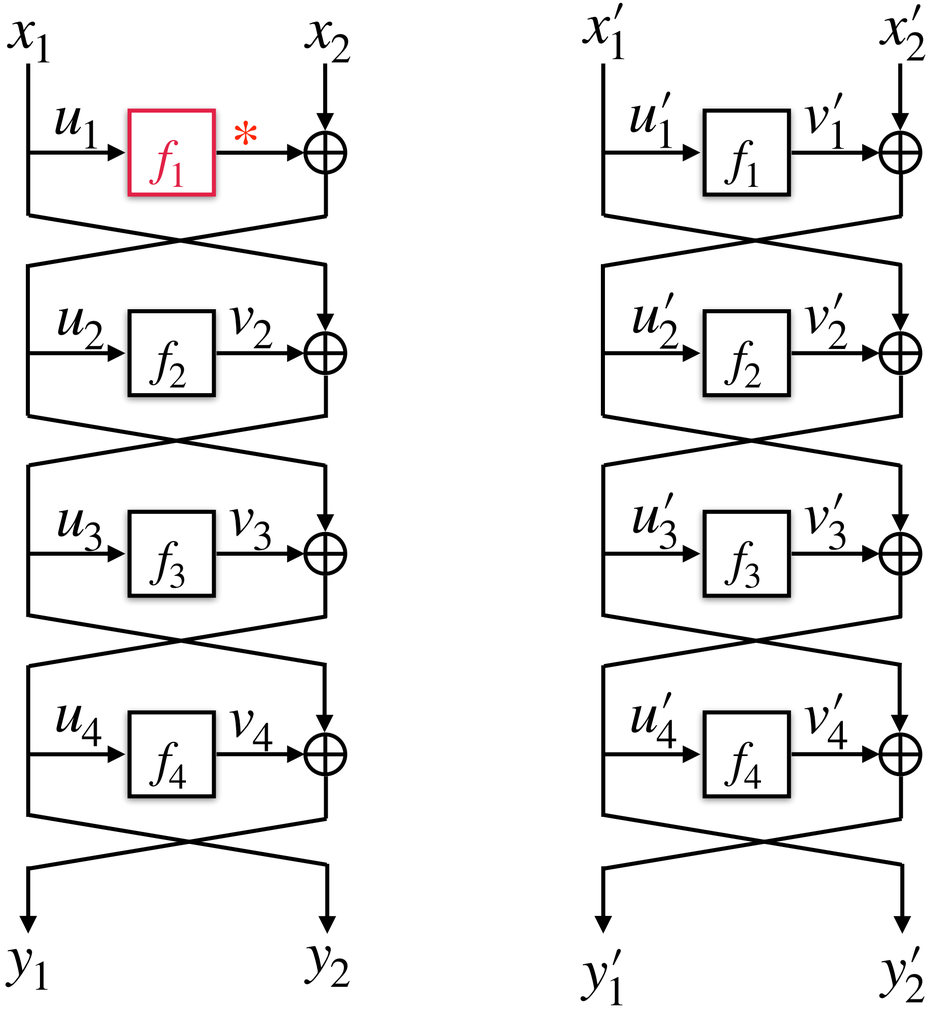
$$v_2 \oplus u_1 = v_2' \oplus u_1'$$

- or, there exists entries $(u_2, v_2), (u_2', v_2'), (u_3, v_3), (u_3', v_3') \in d$ such that

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

Proofs in the Quantum World

Revisiting the Case of LR4 [Hosoyamada-Iwata 2019, Bhaumik et al. 2024]

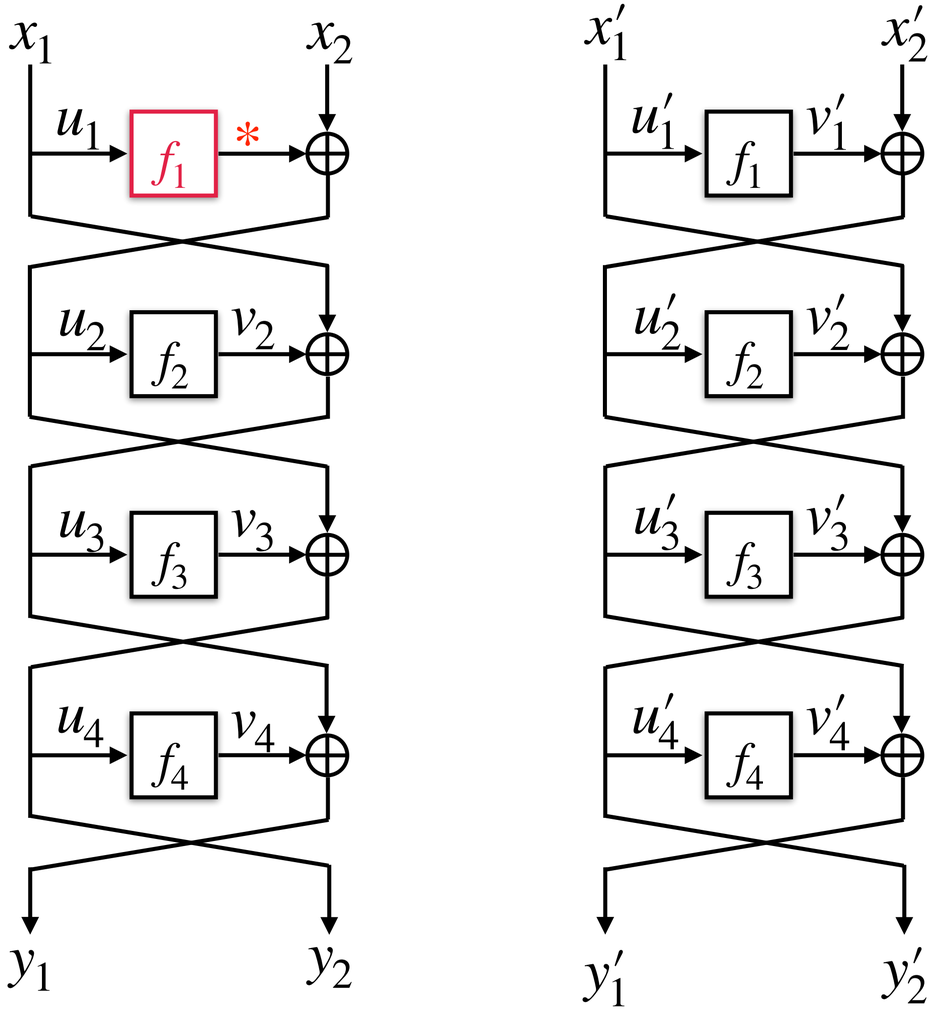


- On action of f_1 for a fresh x_1:

$$|\{y : x_1 \oplus v_2 = u'_1 \oplus v'_2\}| =$$

Proofs in the Quantum World

Revisiting the Case of LR4 [Hosoyamada-Iwata 2019, Bhaumik et al. 2024]



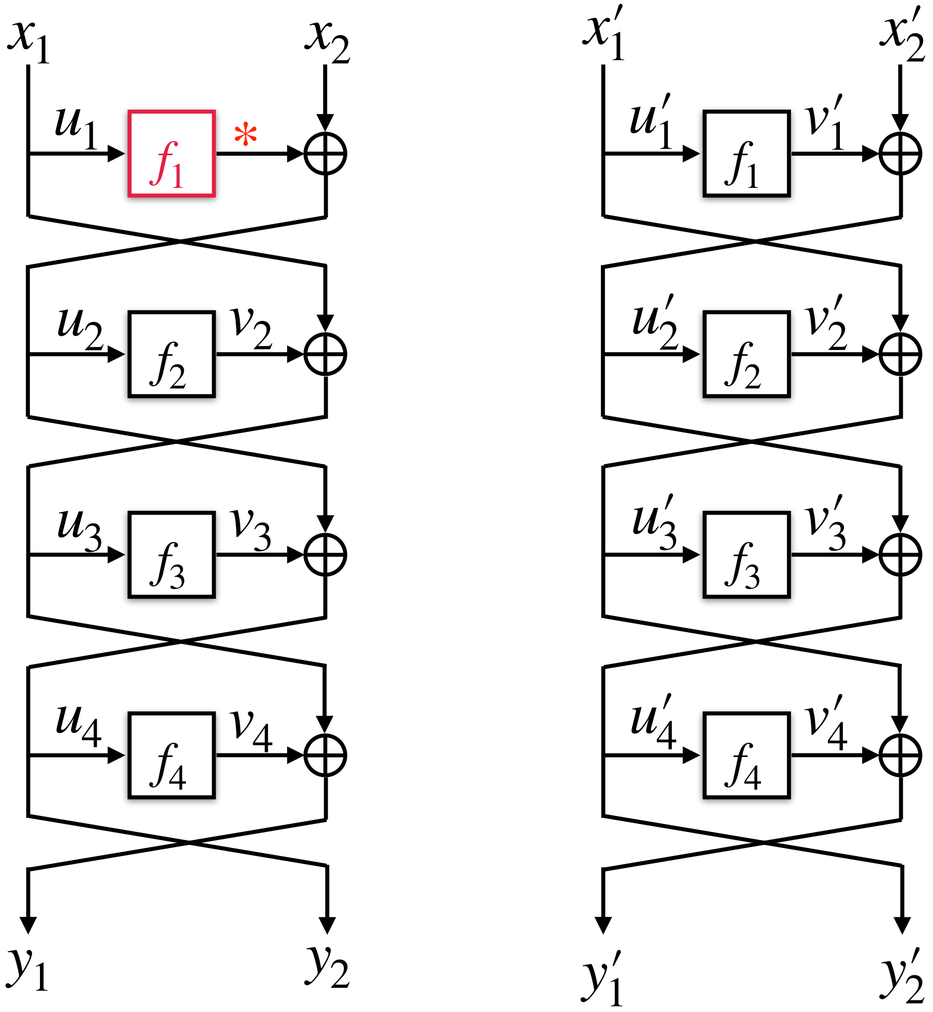
- On action of f_1 for a fresh x_1:

$$|\{y : x_1 \oplus v_2 = u'_1 \oplus v'_2\}| = O(2^n)$$

- TC($\mathscr{P}$) has a trivial upper bound
- This holds over any number of rounds

Proofs in the Quantum World

Revisiting the Case of LR4 [Hosoyamada-Iwata 2019, Bhaumik et al. 2024]



- On action of f_1 for a fresh x_1:

$$|\{y : x_1 \oplus v_2 = u'_1 \oplus v'_2\}| = O(2^n)$$

- TC($\mathscr{P}$) has a trivial upper bound
- This holds over any number of rounds
- Invalidates HI19 security claim
- *Open problem*: Q2 Security of LR4

Evasive Properties

Output-independent Relations

Any k-ary relation $R \subset (\mathcal{X} \times \mathcal{Y})^k$ is said to be output-independent if there exists $i \in [k]$ such that for all $(x_1, y_1), \ldots, (x_k, y_k) \in \mathcal{X} \times \mathcal{Y}$ and $y_i' \neq y_i$ it holds that

$$(\mathbf{x}, \mathbf{y}) \in R \iff (\mathbf{x}, \mathbf{y}') \in R$$

where

$$(\mathbf{x}, \mathbf{y}) = ((x_1, y_1), \ldots, (x_{i-1}, y_{i-1}), (x_i, y_i), (x_{i+1}, y_{i+1}), \ldots, (x_k, y_k)),$$
$$(\mathbf{x}', \mathbf{y}') = ((x_1, y_1), \ldots, (x_{i-1}, y_{i-1}), (x_i, y_i'), (x_{i+1}, y_{i+1}), \ldots, (x_k, y_k)) .$$

Evasive Properties

Property-indicators

Let $\mathscr{X} = \{0,1\}^m$ and $\mathscr{Y} = \{0,1\}^n \cup \{ \perp \}$. A k-ary relation $R \subset (\mathscr{X} \times \mathscr{Y})^k$ is said to be an indicator of property $\mathscr{P} \subset \mathscr{D}$ if for all $d \in \mathscr{P}$ there exists $(x_1, y_1), \ldots, (x_k, y_k) \in d$ such that

$$((x_1, y_1), \ldots, (x_k, y_k)) \in R$$

Evasive Properties

Property-indicators

Let $\mathscr{X} = \{0,1\}^m$ and $\mathscr{Y} = \{0,1\}^n \cup \{ \perp \}$. A k-ary relation $R \subset (\mathscr{X} \times \mathscr{Y})^k$ is said to be an indicator of property $\mathscr{P} \subset \mathscr{D}$ if for all $d \in \mathscr{P}$ there exists $(x_1, y_1), \ldots, (x_k, y_k) \in d$ such that

$$((x_1, y_1), \ldots, (x_k, y_k)) \in R$$

- Examples:
  - Collision-indicator: $\{((x, y), (x', y)) : x, x' \in \mathscr{X}, y \in \mathscr{Y} \setminus \{ \perp \}\}$
  - Zero-preimage-indicator: $\{(x,0) : x \in \mathscr{X}\}$
  - Cycle-indicator: $\{((x, y), (x', x)) : x, x', y \in \mathscr{Y} \setminus \{ \perp \}\}$

Evasive Properties

Evasive Properties

A property $\mathscr{P} \subset \mathscr{D}$ is said to be evasive if and only if all of the corresponding property-indicators are *output-independent*.

Evasive Properties

Evasive Properties

A property $\mathscr{P} \subset \mathscr{D}$ is said to be evasive if and only if all of the corresponding property-indicators are *output-independent*.

Examples:

- Period property (aka Simon's promise):

$$\{((x, \star), (x + p, \star)) : x \in \mathscr{X}\}$$

- Cycle property:

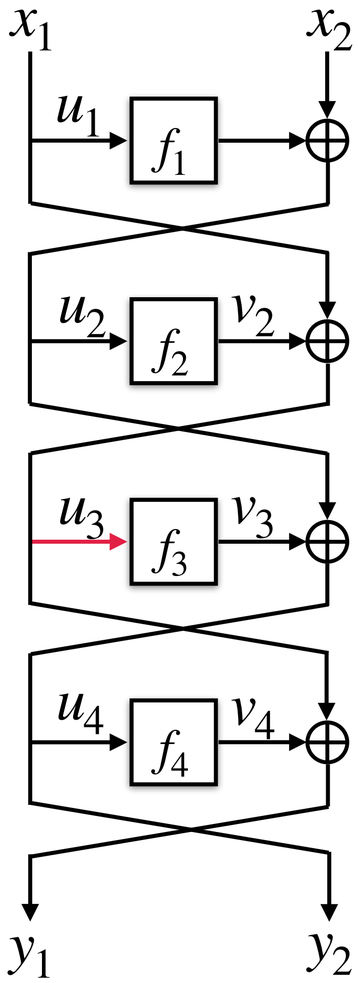
$$\{((x, y), (x', x)) : x, x', y \in \mathscr{Y} \setminus \{\perp\}\}$$

Evasive Properties

More Examples

Evasive Properties

More Examples



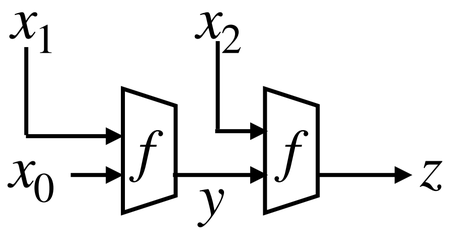
LR4-collision property

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

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

Evasive Properties

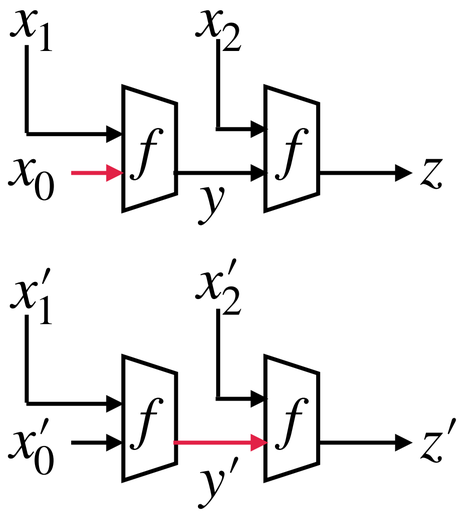
More Examples



Cascade construction [Merkle 1979, Damgård 1989, Preneel and van Oorschot 1999]

Evasive Properties

More Examples



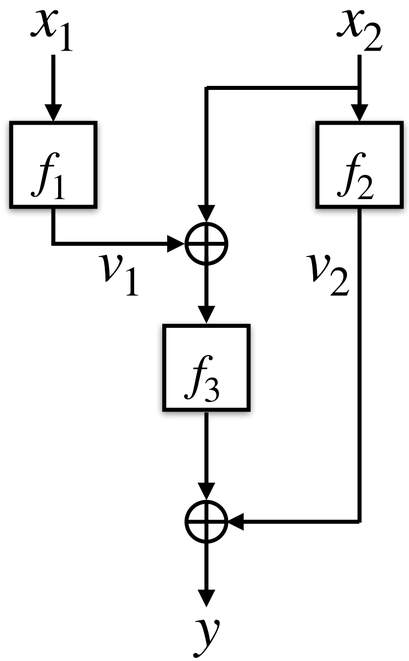
Cascade-collision property

There exists entries $(x_0, x_1, y), (x'_0, x'_1, y') \in d$ such that

$$y' = x_0$$

Evasive Properties

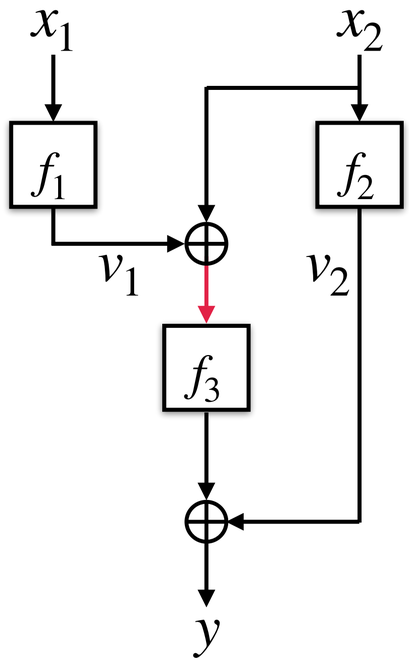
More Examples



LRQ [Bhaumik et al. 2023]

Evasive Properties

More Examples



LRQ-collision property

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

$$v_1 \oplus u_2 = v_1' \oplus u_2'$$

Evasive Properties

Even More Examples

- Iterated Permutations [Minaud and Seurin 2015]
- A variant of LR based on TBCs [Coron et al. 2010]
- Bad database property for TNT and LRWQ [Hosoyamada-Iwata 2020, Bhaumik et al. 2023, Mao et al. 2023]

Evasive Properties

Even More Examples

- Iterated Permutations [Minaud and Seurin 2015]
- A variant of LR based on TBCs [Coron et al. 2010]
- ~~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., $\mathsf{TC}(\mathscr{P}) = O(1)$.

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., $\mathsf{TC}(\mathscr{P}) = O(1)$.

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]

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 (reduction-based) approach.
  - Still, uses a per query progress measure and covered.

Conclusion

- Zhandry’s oracle has transformed the study of average-case quantum query complexity.
- Several new results in quantum provable security.

Conclusion

- Zhandry's oracle has transformed the study of average-case quantum query complexity.
- Several new results in quantum 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.

If you think you understand quantum mechanics, you don't understand quantum mechanics.

- Richard P. Feynman

Thank you!