Mind the Bad Norms

Revisiting Compressed Oracle-based Quantum Indistinguishability Proofs

Ritam Bhaumik Benoît Cogliati **Jordan Ethan** Ashwin Jha

Asiacrypt2024 | December, 2024

Introduction

Classical vs Quantum Search

- **Assumption:** doubling key length is enough for quantum resistance.

Classical vs Quantum Search

- **Assumption:** doubling key length is enough for quantum resistance.
- **Not Enough:**

Classical vs Quantum Search

- **Assumption:** doubling key length is enough for quantum resistance.
- **Not Enough:**
    - Quantum cryptoanalysis [BNP18, BNPS18, BNPS19, KLLNP16],

Classical vs Quantum Search

- **Assumption:** doubling key length is enough for quantum resistance.
- **Not Enough:**
  - Quantum cryptoanalysis [BNP18, BNPS18, BNPS19, KLLNP16],
  - Collision finding [CNPS17, HSX17, KLLÂP16],

Classical vs Quantum Search

- **Assumption:** doubling key length is enough for quantum resistance.
- **Not Enough:**
  - Quantum cryptoanalysis [BNP18, BNPS18, BNPS19, KLLNP16],
  - Collision finding [CNPS17, HSX17, KLLÂP16],
  - Generalized birthday problem [GNPS18],

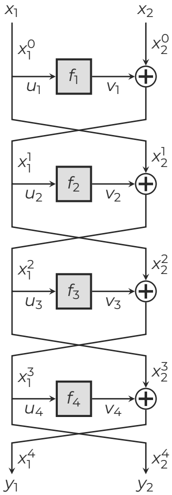
Classical vs Quantum Search

- **Assumption:** doubling key length is enough for quantum resistance.
- **Not Enough:**
  - Quantum cryptoanalysis [BNP18, BNPS18, BNPS19, KLLNP16],
  - Collision finding [CNPS17, HSX17, KLLÂP16],
  - Generalized birthday problem [GNPS18],
  - Quantum attacks on symmetric schemes [BSS22, KM10, KM12].

Classical vs Quantum Search

- **Assumption:** doubling key length is enough for quantum resistance.
- **Not Enough:**
  - Quantum cryptoanalysis [BNP18, BNPS18, BNPS19, KLLNP16],
  - Collision finding [CNPS17, HSX17, KLLÂP16],
  - Generalized birthday problem [GNPS18],
  - Quantum attacks on symmetric schemes [BSS22, KM10, KM12].
- Classical proofs $\Rightarrow$ Quantum proofs?

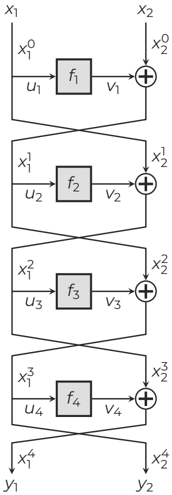
The Luby-Rackoff Construction



[3]**Figure 1:** 4 Rounds Luby-Rackoff (LR4)

- Introduced by Luby and Rackoff [LR88] to build a PRP from PRFs.

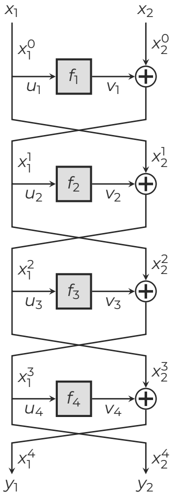
The Luby-Rackoff Construction



[3]**Figure 1:** 4 Rounds Luby-Rackoff (LR4)

- Introduced by Luby and Rackoff [LR88] to build a PRP from PRFs.
- **Classical Security:** secure from $r \geq 3$

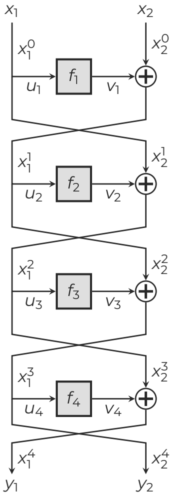
The Luby-Rackoff Construction



[3]**Figure 1:** 4 Rounds Luby-Rackoff (LR4)

- Introduced by Luby and Rackoff [LR88] to build a PRP from PRFs.
- **Classical Security:** secure from $r \geq 3$
- **Quantum Security:**

The Luby-Rackoff Construction



[3]**Figure 1:** 4 Rounds Luby-Rackoff (LR4)

- Introduced by Luby and Rackoff [LR88] to build a PRP from PRFs.
- **Classical Security:** secure from $r \geq 3$
- **Quantum Security:**
    1. qCPA attack for LR3 [KM10] & qCCA attack for LR4 [IHM+19]

The Luby-Rackoff Construction

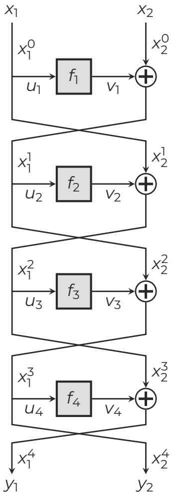
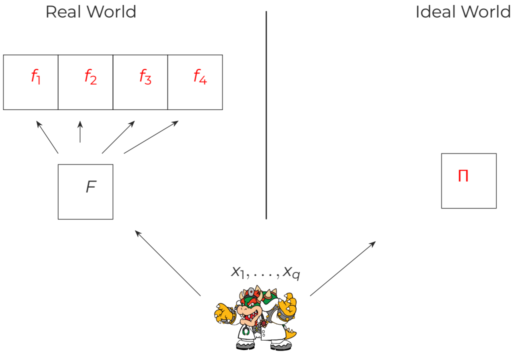


Figure 1: 4 Rounds Luby-Rackoff (LR4)

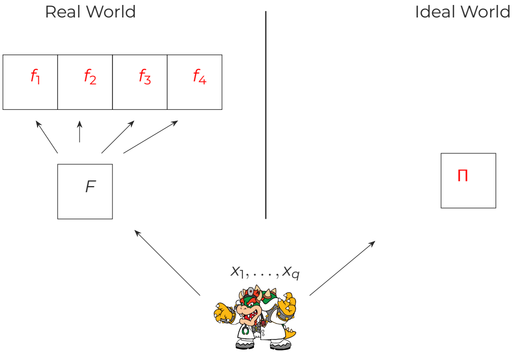
- Introduced by Luby and Rackoff [LR88] to build a PRP from PRFs.
- **Classical Security:** secure from $r \geq 3$
- **Quantum Security:**
  1. qCPA attack for LR3 [KM10] & qCCA attack for LR4 [IHM$^+$19]
  2. qCPA proof for LR4 [HI19] - we revisit this proof and identify some challenges.

Quantum CPA Distinguishing Game



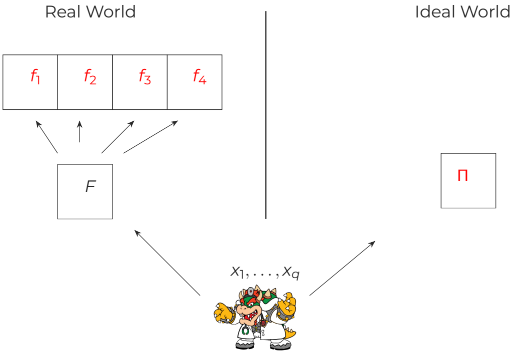
- $F, \Pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ and $f_1, f_2, f_3, f_4 : \{0,1\}^n \to \{0,1\}^n$.

Quantum CPA Distinguishing Game



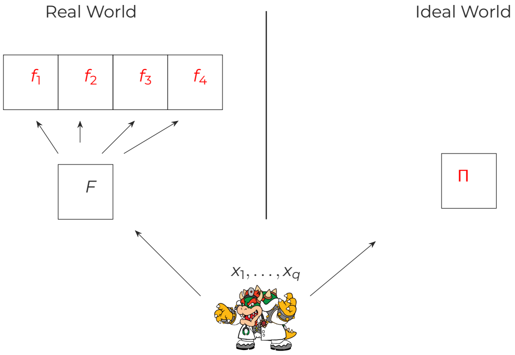
- $F, \Pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ and $f_1, f_2, f_3, f_4 : \{0,1\}^n \to \{0,1\}^n$.
- **Assumptions:**

Quantum CPA Distinguishing Game



- $F, \Pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ and $f_1, f_2, f_3, f_4 : \{0,1\}^n \to \{0,1\}^n$.
- **Assumptions:**
  1. primitives f_1, f_2, f_3, f_4 are random;

Quantum CPA Distinguishing Game



- $F, \Pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ and $f_1, f_2, f_3, f_4 : \{0,1\}^n \to \{0,1\}^n$.
- **Assumptions:**
    1. primitives f_1, f_2, f_3, f_4 are random;
    2. **Q2 Model:** allow quantum (superposition) queries.

Quantum CPA
Proof of LR4 [HI19]

Quantum Implementation of LR4 [HI19]

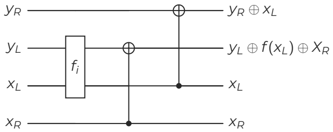


Figure 2: Round i of LR4 - O_{f_i}

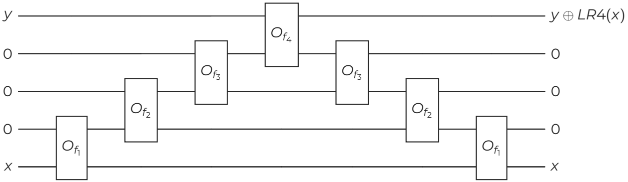


Figure 3: LR4

- **Action** = a call to the unitary O_{f_i}.
- Each O_{f_i} maintains a state - **Database**.

Modified LR4 - LR4'

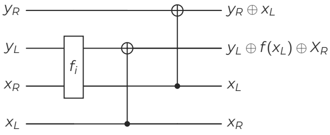


Figure 4: O_{f_i}

$\longrightarrow$

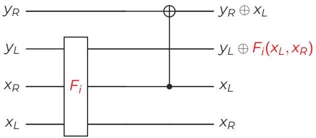


Figure 5: O_{F_i} where $F_i \twoheadleftarrow_{\$} RF$

- LR4' = LR4 with O_{F_i} instead of O_{f_i} for $i = 3, 4 \Rightarrow$ LR4' IND from Π

Modified LR4 - LR4'

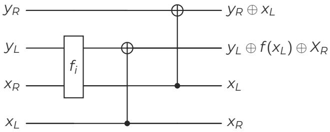


Figure 4: O_{f_i}

$\longrightarrow$

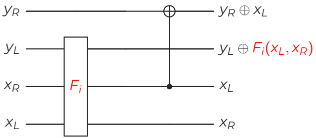


Figure 5: O_{F_i} where $F_i \twoheadleftarrow_\$ RF$

- LR4' = LR4 with O_{F_i} instead of O_{f_i} for $i = 3, 4 \Rightarrow$ LR4' IND from Π
- **Hybrid Distance:** enough to bound distance from LR4 to LR4'.

Two-Domain Distance (TDD) Technique [BCEJ23]

- **Single Compressed Oracle:** Record all intermediate functions with random $\Gamma : \{0,1\}^{4+2nq} \to \{0,1\}^n$ where for $i \leq 4, j = 3, 4$

$$f_i(x) = \Gamma([8+i]_2 || x || 0 \ldots 0),$$

$$F_j(x_1, x_2, x_3) = \Gamma([10+j]_2 || x_1 || x_2 || x_3 || 0 \ldots 0).$$

Two-Domain Distance (TDD) Technique [BCEJ23]

- **Single Compressed Oracle:** Record all intermediate functions with random $\Gamma : \{0,1\}^{4+2nq} \to \{0,1\}^n$ where for $i \leq 4, j = 3, 4$

$$f_i(x) = \Gamma([8+i]_2 || x || 0 \ldots 0),$$
$$F_j(x_1, x_2, x_3) = \Gamma([10+j]_2 || x_1 || x_2 || x_3 || 0 \ldots 0).$$

- **Bad Databases:** defined as $d^{\mathbf{R}}$ (resp. $d^{\mathbf{I}}$) with a collision on inputs to f_3 (resp. F_3) or f_4 (resp. F_4).

Two-Domain Distance (TDD) Technique [BCEJ23]

- **Single Compressed Oracle:** Record all intermediate functions with random $\Gamma : \{0,1\}^{4+2nq} \to \{0,1\}^n$ where for $i \leq 4, j = 3, 4$

$$f_i(x) = \Gamma([8+i]_2 || x || 0 \ldots 0),$$
$$F_j(x_1, x_2, x_3) = \Gamma([10+j]_2 || x_1 || x_2 || x_3 || 0 \ldots 0).$$

- **Bad Databases:** defined as $d^{\mathbf{R}}$ (resp. $d^{\mathbf{I}}$) with a collision on inputs to f_3 (resp. F_3) or f_4 (resp. F_4).
- **1-to-1 mapping:** for any good database $d^{\mathbf{R}}$, $d^{\mathbf{R}} \mapsto [d^{\mathbf{R}}]_{\mathbf{I}}$.

Trivialization of Norm

- **Action Analysis:** apply O_{f_i} on $|\psi_g\rangle$ & bound norm of $|\psi'\rangle = O_{f_i}|\psi_g\rangle$ turning "*bad*".

Trivialization of Norm

- **Action Analysis:** apply O_{f_i} on $|\psi_g\rangle$ & bound norm of $|\psi'\rangle = O_{f_i}|\psi_g\rangle$ turning "*bad*".
- **Example:** bound "*bad*" norm of $O_{f_1}\left|\left(\psi_g^{\leq(j-1)}\right)\right\rangle$ (ideal world).

Trivialization of Norm

- **Action Analysis:** apply O_{f_i} on $|\psi_g\rangle$ & bound norm of $|\psi'\rangle = O_{f_i}|\psi_g\rangle$ turning *"bad"*.
- **Example:** bound *"bad"* norm of $O_{f_1}|\left(\psi_g^{\leq(j-1)}\right)\rangle$ (ideal world).
- **Simplification:** let $BAD = \{\beta : d^{\mathbf{I}} \cup (x_1, \beta)_1 \text{ is bad}\}$ then

$$||\mathrm{BN}||^2 \leq \frac{|BAD|}{2^n}.$$

Trivialization of Norm

- **Authors claim:**

$$||\mathrm{BN}||^2 \le \frac{|BAD|}{2^n} \le O(j/2^n) \Rightarrow |BAD| \le O(j).$$

Trivialization of Norm

- **Authors claim:**

$$||\mathrm{BN}||^2 \leq \frac{|BAD|}{2^n} \leq O(j/2^n) \Rightarrow |BAD| \leq O(j).$$

- **Bad equation:** $u_1 \oplus v_2 = u_1' \oplus v_2' = u_3 \rightarrow$ independent of $v_1 = \beta$

Trivialization of Norm

- **Authors claim:**

$$||\mathrm{BN}||^2 \leq \frac{|BAD|}{2^n} \leq O(j/2^n) \Rightarrow |BAD| \leq O(j).$$

- **Bad equation:** $u_1 \oplus v_2 = u_1' \oplus v_2' = u_3 \rightarrow$ independent of $v_1 = \beta$
- **Correct claim:** $||\mathrm{BN}||^2 = O(1)$.

Fixing Proof

- **Question:** Does increasing the number of rounds help?

Fixing Proof

- **Question:** Does increasing the number of rounds help?
- **Answer:** *No*. For any $r \geq 4$, creating a collision on $f_i \Rightarrow$ leads to trivialization of norm.

Fixing Proof

- **Question:** Does increasing the number of rounds help?
- **Answer:** *No*. For any $r \geq 4$, creating a collision on $f_i \Rightarrow$ leads to trivialization of norm.
- **Underlying Issue:** lack of oracle's knowledge of adversarial query pattern.

Non-Adaptive qCPA Setting

- **Setting:** adversary makes a single query $x^q = (x_1, \ldots, x_q)$ & oracle outputs $\hat{y}^q$.

Non-Adaptive qCPA Setting

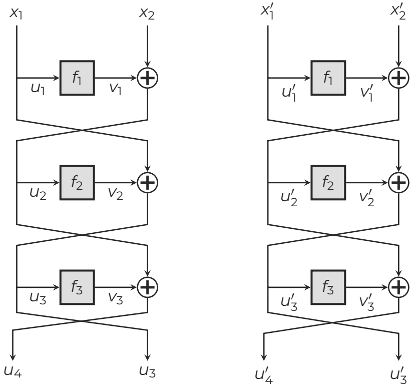
- **Setting:** adversary makes a single query $x^q = (x_1, ..., x_q)$ & oracle outputs $\hat{y}^q$.
- **Dummy Call Idea:** sandwich $x^q = (x_1, ..., x_q)$ between two compressed oracles (record & erase) $\Rightarrow$ oracle knows all query-response pairs for action analysis.

Non-Adaptive qCPA Setting

- **Setting:** adversary makes a single query $x^q = (x_1, \ldots, x_q)$ & oracle outputs $\hat{y}^q$.
- **Dummy Call Idea:** sandwich $x^q = (x_1, \ldots, x_q)$ between two compressed oracles (record & erase) $\Rightarrow$ oracle knows all query-response pairs for action analysis.
- **Non-Adaptive Setting:** includes Simon's non-adaptive version [BHNP$^+$19].

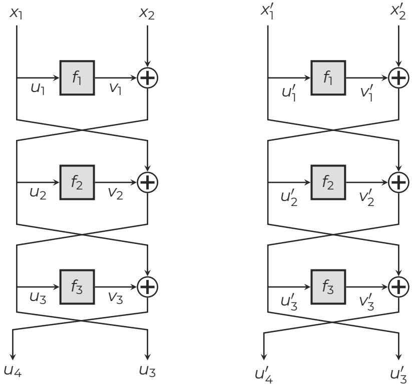
Non-Adaptive Proof for LR4

Bad Database Definition



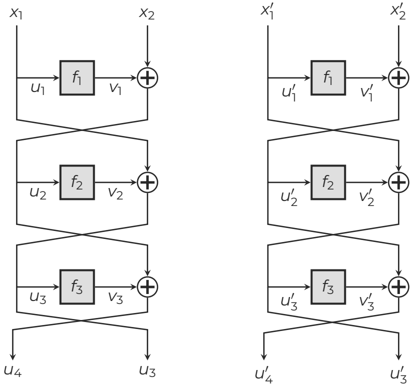
- **Dummy call:** oracle knows $(x_1, x_2) \mapsto (v_1, v_2, v_3)$ & $(x'_1, x'_2) \mapsto (v'_1, v'_2, v'_3)$

Bad Database Definition



- **Dummy call:** oracle knows $(x_1, x_2) \mapsto (v_1, v_2, v_3)$ & $(x'_1, x'_2) \mapsto (v'_1, v'_2, v'_3)$
- **Bad Events:** $\exists$ collision on input to f_3 $(u_3 = u'_3)$ or f_4 $(u_4 = u'_4)$.

Bad Database Definition



- **Dummy call:** oracle knows $(x_1, x_2) \mapsto (v_1, v_2, v_3)$ & $(x'_1, x'_2) \mapsto (v'_1, v'_2, v'_3)$
- **Bad Events:** $\exists$ collision on input to f_3 $(u_3 = u'_3)$ or f_4 $(u_4 = u'_4)$.
- Show a 1-to-1 mapping between good databases in both worlds.

Getting The Bound

- **Transition Capacity:** A measure of the probability of a database going bad after a single query.

Getting The Bound

- **Transition Capacity:** A measure of the probability of a database going bad after a single query.
- Analyze the action of f_1, f_2, f_3, f_4 and show an upper bound on transition capacities $\leq O\left(\sqrt{\frac{q^6}{2^n}}\right)$.

Getting The Bound

- **Transition Capacity:** A measure of the probability of a database going bad after a single query.
- Analyze the action of f_1, f_2, f_3, f_4 and show an upper bound on transition capacities $\leq O\left(\sqrt{\frac{q^6}{2^n}}\right)$.
- From the TDD Framework:

$$\mathbf{Adv}_{LR4}^{qNCPA}(A) \leq O\left(\sqrt{\frac{q^6}{2^n}}\right).$$

The Problem with the Adaptive Setting

- **Characterization of Bad Databases:** $\exists$ "colliding path" to input of f_3 or f_4 $\Rightarrow$ later queries (x_1, x_2) can make database go "bad" independently from v_1, v_2 or v_3.

The Problem with the Adaptive Setting

- **Characterization of Bad Databases:** $\exists$ "colliding path" to input of f_3 or $f_4 \Rightarrow$ later queries (x_1, x_2) can make database go "bad" independently from v_1, v_2 or v_3.
- **Global Issue:** In HI framework - trivialization of norm, TDD framework - database going "bad" between actions.

The Problem with the Adaptive Setting

- **Characterization of Bad Databases:** $\exists$ "colliding path" to input of f_3 or $f_4 \Rightarrow$ later queries (x_1, x_2) can make database go "bad" independently from v_1, v_2 or v_3.
- **Global Issue:** In HI framework - trivialization of norm, TDD framework - database going "bad" between actions.
- **Broken proofs:** LRWQ [HI21], a refined proof of TNT [MZH$^+$23] and LRQ [BCEJ23].

The Problem with the Adaptive Setting

- **Characterization of Bad Databases:** $\exists$ "colliding path" to input of f_3 or $f_4 \Rightarrow$ later queries (x_1, x_2) can make database go "bad" independently from v_1, v_2 or v_3.
- **Global Issue:** In HI framework - trivialization of norm, TDD framework - database going "bad" between actions.
- **Broken proofs:** LRWQ [HI21], a refined proof of TNT [MZH$^+$23] and LRQ [BCEJ23].
- TNT and LRWQ [BCEJ23] $\rightarrow$ bounds deteriorate to $O(2^{n/5})$.

The Misty Constructions

Misty-L vs Misty-R

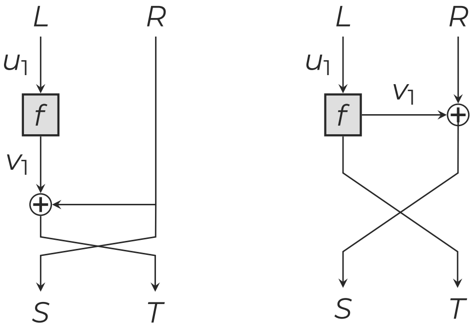


Figure 6: Misty-L (left) & Misty-R (right)

- Misty-L: $v_1 \oplus R = T$, Misty-R: $v_1 \oplus R = S$

Misty-L vs Misty-R

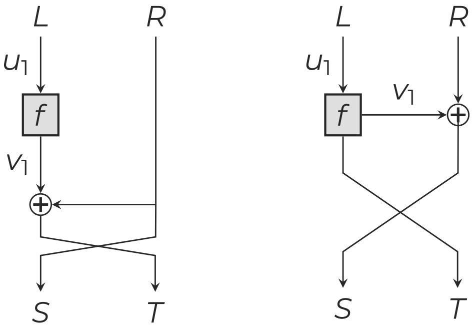


Figure 6: Misty-L (left) & Misty-R (right)

- Misty-L: $v_1 \oplus R = T$, Misty-R: $v_1 \oplus R = S$
- Efficient quantum attacks for 3 rounds Misty-R (resp. 4 rounds Misty-L).

Misty-L vs Misty-R

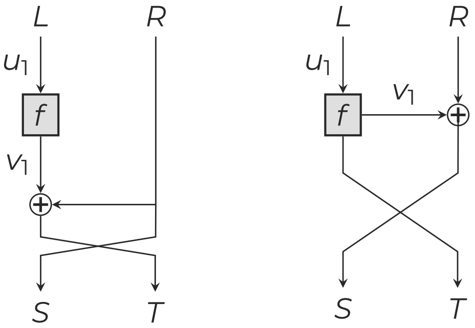
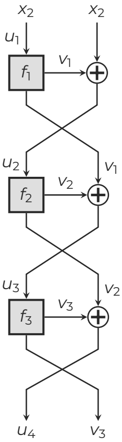
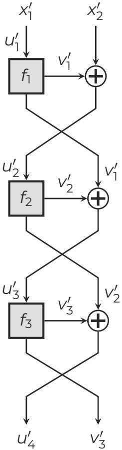


Figure 6: Misty-L (left) & Misty-R (right)

- Misty-L: $v_1 \oplus R = T$, Misty-R: $v_1 \oplus R = S$
- Efficient quantum attacks for 3 rounds Misty-R (resp. 4 rounds Misty-L).
- **In this work:** we show qCPA (adaptive) proofs in the TDD framework.

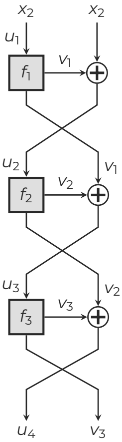
Bad Events for 4 Rounds Misty-R

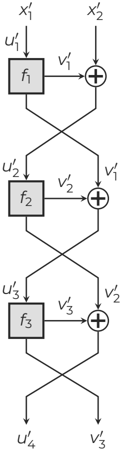




- **Bad Events:** $\exists$ collision on input to f_3 or f_4.

Bad Events for 4 Rounds Misty-R





- **Bad Events:** $\exists$ collision on input to f_3 or f_4.
- **Difference from LR4:** "bad" events are dependent on v_1, v_2, v_3.

Conclusions

TDD Framework Quantum (N)CPA Proofs

Scheme	Calls	Model	Bound
Luby-Rackoff	4	qNCPA	$O(2^{n/6})$ (Section 5)
Misty-R	4	qCPA	$O(2^{n/5})$
Misty-L	5	qCPA	$O(2^{n/7})$
LRWQ [HI21]	3	qCPA	$O(2^{n/5})$ [BCEJ23]
TNT [BGGS]	3	qCPA	$O(2^{n/5})$ [BCEJ23]

Quantum BB - $O(2^{n/3})$ queries [Zha13].

Conclusion

1. We revisit the qCPA security proof of LR4 [HI19]:

Conclusion

1. We revisit the qCPA security proof of LR4 [HI19]:
   - Trivialization of norms - flaw in the proof,

Conclusion

1. We revisit the qCPA security proof of LR4 [HI19]:
   - Trivialization of norms - flaw in the proof,
   - Non-adaptive qCPA proof for LR4 up to $O(2^{n/6})$ quantum queries - dummy call + TDD framework.

Conclusion

1. We revisit the qCPA security proof of LR4 [HI19]:
   - Trivialization of norms - flaw in the proof,
   - Non-adaptive qCPA proof for LR4 up to $O(2^{n/6})$ quantum queries - dummy call + TDD framework.
2. We provide qCPA proofs for the Misty constructions using TDD framework:

Conclusion

1. We revisit the qCPA security proof of LR4 [HI19]:
    - Trivialization of norms - flaw in the proof,
    - Non-adaptive qCPA proof for LR4 up to $O(2^{n/6})$ quantum queries - dummy call + TDD framework.
2. We provide qCPA proofs for the Misty constructions using TDD framework:
    - 4 rounds Misty-R up to $O(2^{n/5})$ quantum queries,

Conclusion

1. We revisit the qCPA security proof of LR4 [HI19]:
   - Trivialization of norms - flaw in the proof,
   - Non-adaptive qCPA proof for LR4 up to $O(2^{n/6})$ quantum queries - dummy call + TDD framework.
2. We provide qCPA proofs for the Misty constructions using TDD framework:
   - 4 rounds Misty-R up to $O(2^{n/5})$ quantum queries,
   - 5 rounds Misty-L up to $O(2^{n/7})$ quantum queries.

Future Work

- **Permutation Compressed Oracle:** permutation = product of transpositions [MMW24].

Future Work

- **Permutation Compressed Oracle:** permutation = product of transpositions [MMW24].
- **Proofs in TDD framework [BCEJ23]:** define a property which makes schemes provable in the framework?

Future Work

- **Permutation Compressed Oracle:** permutation = product of transpositions [MMW24].
- **Proofs in TDD framework [BCEJ23]:** define a property which makes schemes provable in the framework?
- **Tightening proofs:** new proof techniques? better bounds? seems hard!

Thank you!

References i

- Ritam Bhaumik, BenoIt Cogliati, Jordan Ethan, and Ashwin Jha.
  On quantum secure compressing pseudorandom functions.
  Cryptology ePrint Archive, Paper 2023/207, 2023.
- Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song.
  TNT: How to tweak a block cipher.
  pages 641–673.

References ii

- Xavier Bonnetain, Akinori Hosoyamada, Maria Naya-Plasencia, Yu Sasaki, and Andre Schrottenloher.
  ***Quantum Attacks Without Superposition Queries: The Offline Simon's Algorithm*, pages 552–583.**
  Springer International Publishing, 2019.
- Xavier Bonnetain and Maria Naya-Plasencia.
  Hidden shift quantum cryptanalysis and implications.
  Cryptology ePrint Archive, Paper 2018/432, 2018.

References iii

- Xavier Bonnetain, Maria Naya-Plasencia, and Andre Schrottenloher.
  On quantum slide attacks.
  Cryptology ePrint Archive, Paper 2018/1067, 2018.
- Xavier Bonnetain, Maria Naya-Plasencia, and Andre Schrottenloher.
  Quantum security analysis of aes.
  IACR Transactions on Symmetric Cryptology, pages 55–93, June 2019.
- Xavier Bonnetain, Andre Schrottenloher, and Ferdinand Sibleyras.
  ***Beyond Quadratic Speedups inÂ Quantum Attacks onÂ Symmetric Schemes*, pages 315–344.**
  Springer International Publishing, 2022.

References iv

- Andre Chailloux, Maria Naya-Plasencia, and Andre Schrottenloher. ***An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography*, pages 211–240.** Springer International Publishing, 2017.
- Lorenzo Grassi, Maria Naya-Plasencia, and Andre Schrottenloher. ***Quantum Algorithms for the k-xor Problem*, pages 527–559.** Springer International Publishing, 2018.

References v

Aline Gouget, Jacques Patarin, and Ambre Toulemonde.
(quantum) cryptanalysis of misty schemes.
In Deukjo Hong, editor, *Information Security and Cryptology - ICISC 2020, Proceedings*, volume 12593 of *Lecture Notes in Computer Science*, pages 43–57. Springer, 2020.

Akinori Hosoyamada and Tetsu Iwata.
***4-Round Luby-Rackoff Construction is a qPRP*, pages 145–174.**
Springer International Publishing, 2019.

Akinori Hosoyamada and Tetsu Iwata.
Provably quantum-secure tweakable block ciphers.
2021(1):337–377, 2021.

Akinori Hosoyamada, Yu Sasaki, and Keita Xagawa.
***Quantum Multicollision-Finding Algorithm*, pages 179–210.**
Springer International Publishing, 2017.

References vii

- Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata.
  ***Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers*, pages 391–411.**
  Springer International Publishing, 2019.
- Marc Kaplan, Gaetan Leurent, Anthony Leverrier, and Maria Naya-Plasencia.
  Quantum differential and linear cryptanalysis.
  IACR Transactions on Symmetric Cryptology, pages 71–94, December 2016.

- Marc Kaplan, Gaetan Leurent, Anthony Leverrier, and Maria Â Naya-Plasencia.
  ***Breaking Symmetric Cryptosystems UsingÂ QuantumÂ Period Finding*, pages 207–237.**
  Springer Berlin Heidelberg, 2016.
- Hidenori Kuwakado and Masakatu Morii.
  Quantum distinguisher between the 3-round feistel cipher and the random permutation.
  In *IEEE International Symposium on Information Theory, ISIT 2010, Proceedings*, pages 2682–2685. IEEE, 2010.

References ix

Hidenori Kuwakado and Masakatu Morii.
Security on the quantum-type even-mansour cipher.
In *2012 International Symposium on Information Theory and its Applications*, pages 312–316, 2012.

Michael Luby and Charles Rackoff.
How to construct pseudorandom permutations from pseudorandom functions.
17(2), 1988.

References x

- Christian Majenz, Giulio Malavolta, and Michael Walter.
  Permutation superposition oracles for quantum query lower bounds, 2024.
- Shuping Mao, Zhiyu Zhang, Lei Hu, Luying Li, and Peng Wang.
  Quantum security of TNT.
  Cryptology ePrint Archive, Report 2023/1280, 2023.
- Mark Zhandry.
  A note on the quantum collision and set equality problems, 2013.