ASK 2018

Nov 14, 2018

FUJITSU

shaping tomorrow with you

Lower Bounds in Quantum Computing and Applications to Cryptography

Avradip Mandal

Fujitsu Laboratories of America, Inc.

Software Quality and Security Lab

Power of Quantum Computing

FUJITSU

Quantum Computing can provide exponential speed up against certain class of problems

- Example: Factoring, Discrete Log

On the other hard on the problems like unordered search quantum algorithms provide only quadratic speed up

- Known to be optimal
- Focus of this talk: how to prove optimality or lower bounds

Goal of this talk

FUJITSU

- Proving Lower bounds of the query complexity of Quantum Algorithms is a rich research area.
- However, in crypto settings we are generally interested in average case lower bound as opposed worst case lower bound.
- In this talk we will go over two well known proof techniques Polynomial method and Adversarial method and their extension to cryptographic setting

Topics covered in this talk

FUJITSU

- Recap of Quantum Computing Basics
- Quantum Query Model
- Polynomial Method
  - Lower bound of Grover Search
  - Lower bound of Average Case Grover Search
- Adversary Method
  - Lower bound of Grover Search
  - Lower bound of Average Case Grover Search
- Random Permutation vs Random Function

Qubits

FUJITSU

- Classical bit takes $0, 1$ values; Quantum Bit (qubit) is a unit vector in $\mathbb{C}^2$.
  - $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ is a state which is even super position of $|0\rangle$ and $|1\rangle$
- State of n qubits can be represented by a unit vector in $\mathbb{C}^{2^n}$
  - Different vectors with same global phase corresponds to exact same qubit state
  - i.e. $|\Psi\rangle$ and $c|\Psi\rangle$ represent the same qubit state for any $c \in \mathbb{C}$, with $|c| = 1$
- Quantum States allow (only) two kinds of operations: Measurement and Unitary transformation

Measurement

FUJITSU

- Measuring $a|0\rangle + b|1\rangle$ with respect to standard basis $\{|0\rangle, |1\rangle\}$
  - Collapses to state $|0\rangle$ with probability $|a|^2$
  - Collapses to state $|1\rangle$ with probability $|b|^2$
- Measuring $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ in standard basis results in states $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$
- Hadamard basis $\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ measurement results in $|+\rangle$ with probability 1.

Projective Measurement

FUJITSU

- Suppose a vector space $\mathcal{H}$ decomposes into k orthogonal subspaces S_i s.t. $\mathcal{H} = S_1 \oplus S_2 \oplus \cdots \oplus S_k$
- There are k projective operators $P_1, \cdots, P_k$ s.t. $P_i : \mathcal{H} \to S_i$
- Projective measurement on $|\psi\rangle \in \mathcal{H}$ with this operator set would result in state $\frac{P_i|\Psi\rangle}{|P_i|\Psi\rangle|}$ with probability $|P_i|\Psi\rangle|^2$
- A single measurement is always enough.

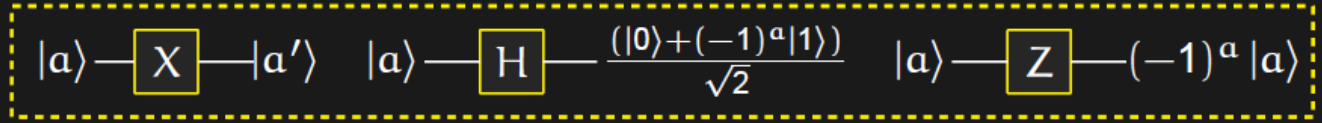
Unitary Transformation

FUJITSU

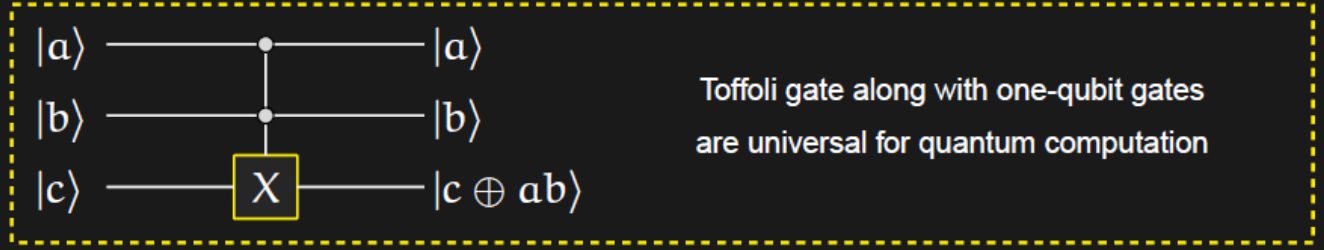
- $U: \mathcal{H} \rightarrow \mathcal{H}$ is unitary if $U^{+}U = I$
  - $U^{+} = (\overline{U})^{T} = \overline{U^{T}}$
- Transform then measurement, is same as measurement then transform
- In classical sense unitary transformations corresponds to reversible circuits.

Quantum operations: Few examples

Single qubit operations: NOT, Hadamard and Phase-flip gates

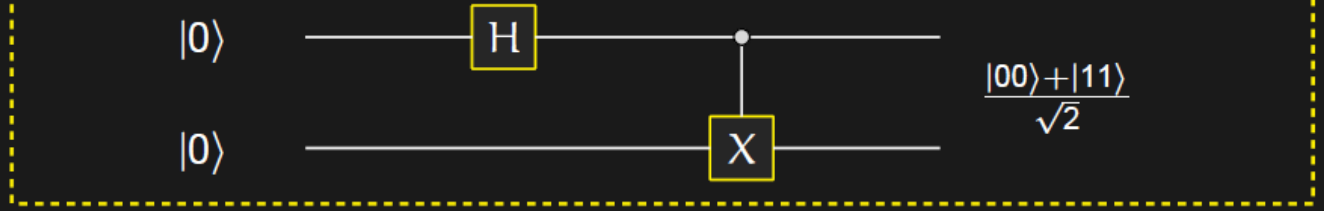


Simulating classical gates: Toffoli gate



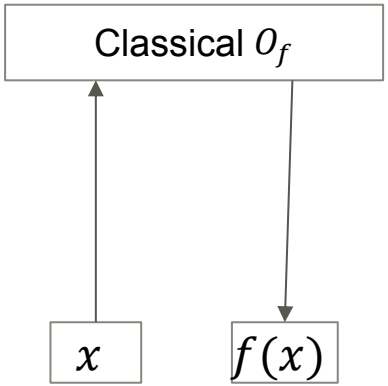
Toffoli gate along with one-qubit gates are universal for quantum computation

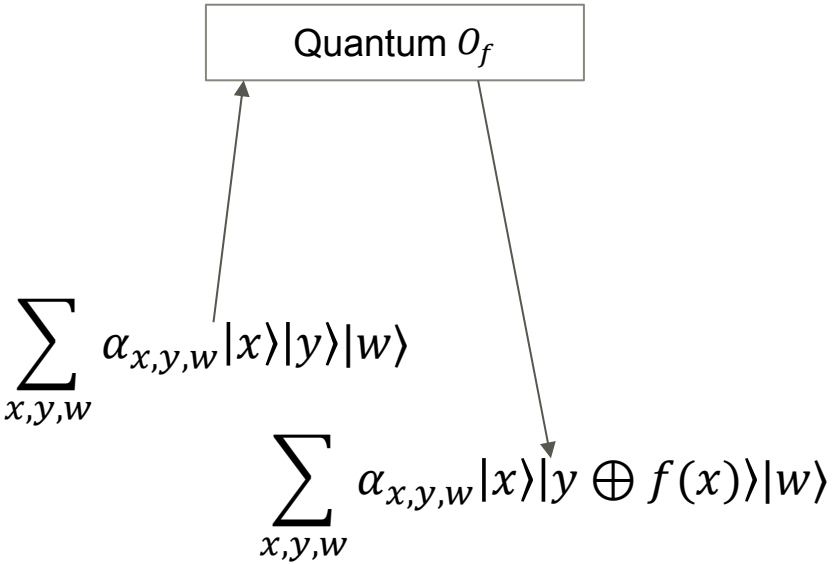
Creating entanglement: Using Hadamard and CNOT gate



Slide stolen from Sarvagya Upadhyay

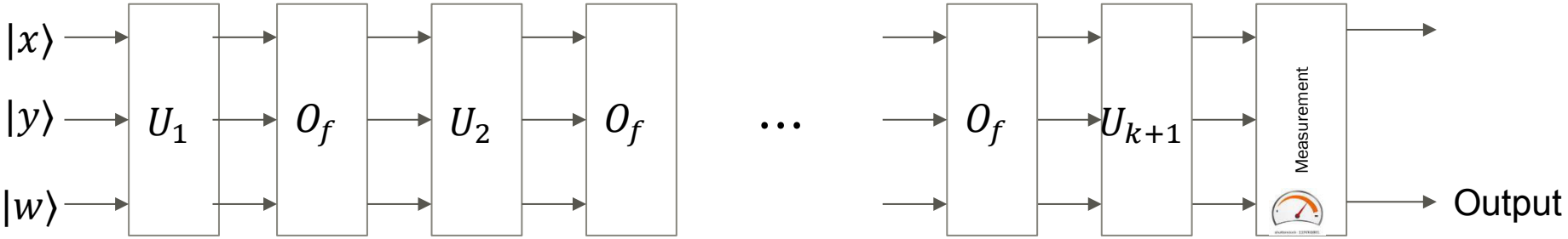
Classical vs Quantum Oracle



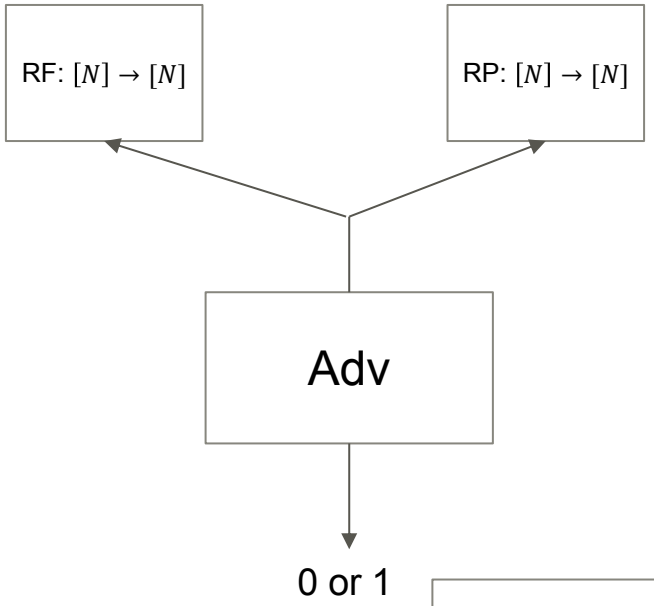


Generic Quantum Algorithm

FUJITSU



Classical Lower Bound: RP vs RF



Suppose the adversary makes q queries $x_1, \dots, x_q$

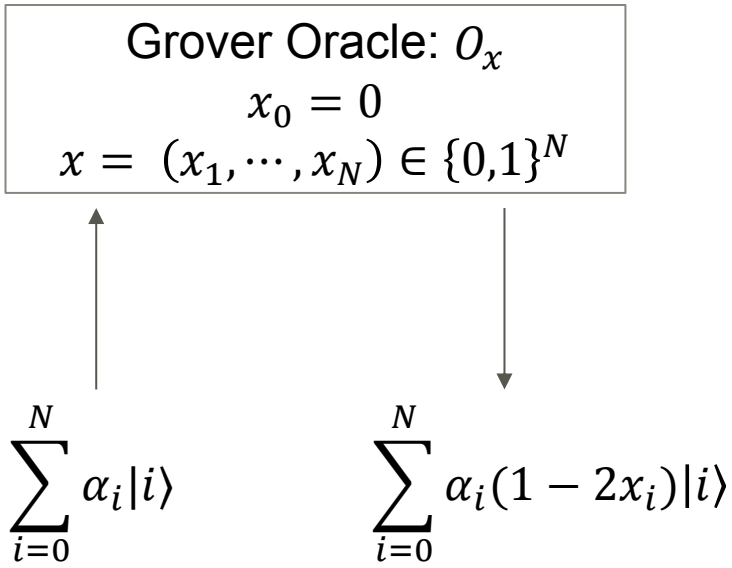
$$Adv = SD\left(\left(RF(x_1), \dots RF(x_q)\right), \dots \left(RP(x_1), \dots RP(x_q)\right)\right)$$

$$\leq 2 \sum_{i \in [0, q-1]} (N-i)\left(\frac{1}{N-i} - \frac{1}{N}\right) = \frac{2q(q-1)}{N}$$

This style of argument does not really work against quantum adversaries which make queries in superposition

Grover Search Polynomial Lower Bound[Beals et al. 01]

FUJITSU



Evaluate $F(x_1, .., x_N): \{0,1\}^N \to [N]$

Output i s.t. $x_i = 1$

Observation:

- If we make T queries to Grover Oracle, Coefficient of $|i\rangle$ is a degree T multinomial in $x_1, \cdots, x_n$
- Probability of accepting $|i\rangle$ is a degree $2T$ multinomial

Fact: if $p(x_1, \ldots, x_N)$ approximates $F(x_1, \ldots x_N)$,
then degree of p is $\Omega(\sqrt{N})$ [Nissan-Szegedy 94]

AvgSearch Lower bound (polynomial)

FUJITSU

- In crypto we are interested in average case lower bounds (not worst case)

Oracle D_λ: Initialize Grover Oracle with

$(x_1, \cdots, x_N) \leftarrow \{0,1\}^N$, where $\Pr[x_i = 1] = \lambda$

AvgSearch Lower bound (polynomial) [Hulsing, Rijneveld, Song PKC16, Zhandry12]

FUJITSU

- One can transform Avgsearch adversary to distinguishing adversary between D_λ and D_0
- For any q-query adversary Probability of outputting any state $|j\rangle$ is a linear combination of $\Pr[x_{i_1} = b_1, x_{i_2} = b_2, \dots, x_{i_{2q}} = b_{2q}]$ for all possible $\left((i_1, b_1), \dots, (i_{2q}, b_{2q})\right)$ tuples
  - $\Pr[x_{i_1} = b_1, x_{i_2} = b_2, \dots, x_{i_{2q}} = b_{2q}]$ is a degree $2q$ polynomial in λ
- $Adv(D_\lambda, D_0) = p(\lambda) - p\,(0)$, where p is a degree $2q$ polynomial and $0 \le \lambda \le 1 \Rightarrow 0 \le p(\lambda) \le 1$
- By markov inequality, for $\lambda \in [0,1]$ we have

$$\max_{\lambda \in [0,1]} |p'(\lambda)| \le \deg(p)^2 \max_{\lambda \in [0,1]} |p(\lambda)| \le 4q^2$$

  - Shadrin, Aleksei. "Twelve proofs of the Markov inequality." *Approximation theory: a volume dedicated to Borislav Bojanov* (2004): 233-298.

- For $\lambda \in [0,1]$ we have $Adv(D_\lambda, D_0) = p(\lambda) - p\,(0) \le \lambda \max_{\lambda \in [0,1]} |p'(\lambda)| \le 4\lambda q^2$

Density Matrix and Mixed states

FUJITSU

- Until now we have seen only pure states
- Mixed states are probabilistic ensemble of mixed states
- $|\psi_{mixed}\rangle = \{(p_1, |\Psi_1\rangle), \dots, (p_n, |\Psi\rangle), \text{where}$
  - p_i's are probabilities which sum to 1
  - $|\Psi_1\rangle, |\Psi_2\rangle, \dots, |\Psi_n\rangle$ are pure states
- Can be represented by density matrix
  - $\rho_{mixed} = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$

Density Matrices

FUJITSU

- Density matrices are used to describe quantum subsystems
- ρ is a density matrix, if
  - ρ is hermitian : $\rho^+ = \rho$
  - ρ is positive semi definite: for any $|\Psi\rangle$ we have $\langle\Psi|\rho|\Psi\rangle$
  - $Tr(\rho) = 1$: diagonal elements should sum to 1
- Unitary Transformation: $\rho \xrightarrow{U} U\rho U^+$

Adversary Method : basic idea [Ambainis02]

FUJITSU

$$\rho_{start} = \rho_0 \xrightarrow{U_1 O_x U_0} \rho_1 \xrightarrow{U_2 O_x} \dots \xrightarrow{U_q O_x} \rho_q = \rho_{end}$$

- Fix ρ_{start} and find some nice properties (depending on notion of successful adversary) of ρ_{end}
- Define a function $S: Density\ Matrix \to \mathbb{R}$, s.t.
  - $S(\rho_{start}) = s_0$
  - $S(\rho_{end}) \leq s_q$ (use the nice properties of ρ_{end})
  - $S(\rho_{i-1}) - S(\rho_i) \leq \Delta$
- We have lower bound $q \geq \frac{s_0 - s_q}{\Delta}$
- Why Density Matrices, not pure states?

Adversarial lower bound [Ambainis02]

- $|\Psi_{start}\rangle = \sum_x \alpha_x |0\rangle \otimes |x\rangle \xrightarrow{U_q O \ldots U_1 O U_0} \alpha_x |\Psi_x\rangle \otimes |x\rangle$
- $\mathcal{H}_A \otimes \mathcal{H}_I$ total workspace of the algorithm
- Initially $\mathcal{H}_I$ and $\mathcal{H}_A$ are not entangled. In the end they become highly entangled
- The goal is to have some bound on this entanglement propagation.

Grover Search Adversarial Lower Bound [Ambainis02]

FUJITSU

$$|\Psi_{start}\rangle = \frac{|0\rangle \otimes (\,|100\ldots0\rangle + |010\ldots0\rangle + \cdots + |000\ldots1\rangle)}{\sqrt{N}}$$

$$|\Psi_{end}\rangle = \frac{|1\rangle|100\ldots0\rangle + |2\rangle|010\ldots0\rangle + \cdots + |N\rangle|000\ldots1\rangle)}{\sqrt{N}}$$

- ρ_{start} and ρ_{end} be the density matrices corresponding to $\mathcal{H}_I$ part of the workspace

$$\rho_{start} = \begin{pmatrix} \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \\ \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{N} & \frac{1}{N} & \cdots & \frac{1}{N} \end{pmatrix} \qquad \rho_{end} = \begin{pmatrix} \frac{1}{N} & 0 & \cdots & 0 \\ 0 & \frac{1}{N} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{1}{N} \end{pmatrix}$$

Grover Search Adversarial Lower Bound

FUJITSU

- The function S: sum of absolute values of off diagonal entries.
- $S(\rho_{start}) = N - 1, S(\rho_{end}) = 0$
- Observation: if measurement of $\mathcal{H}_A$ results in $|i\rangle$, then only i^{th} column and i^{th} row gets affected by every Oracle call O
- With some linear algebra and Cauchy Schwartz:
  - $|S(\rho_{i+1}) - S(\rho_i)| \leq 2\sqrt{N-1}$
- Hence, $q \geq 0.5\sqrt{N-1}$

AvgSearch: Adversarial Bound [Ambainis14]

FUJITSU

- a, k, v be the state, input and output register of the adversary.
- $O_f|a\rangle|k\rangle|v\rangle = |a\rangle|k\rangle|v + f(k)\rangle$
- Adversary interacts either with O_f or O_N
  - $f \leftarrow D_\lambda : \Pr[f(k) = 1] = \lambda$
  - all zero function $N \leftarrow D_0 : N(k) = 0 \; \forall k$

Trace Distance TD

FUJITSU

- ρ and σ be any two density matrices
- $TD(\rho,\sigma) = \frac{1}{2}Tr(\sqrt{(\rho-\sigma)^{+}(\rho-\sigma)})$
  - $A^{+}A$ is hermitian for any A. Hence it has square root.
- $TD(\rho,\sigma) \leq TD(\rho,\tau) + TD(\tau,\sigma)$
- If U is unitary, then $TD(U\rho U^{+}, U\sigma U^{+}) = TD(\rho,\sigma)$
- $Adv(\rho,\sigma) \leq TD(\rho,\sigma)$

AvgSearch: Adversarial Bound

FUJITSU

$$|\Psi\rangle \xrightarrow{UO_f} |\Psi_f^1\rangle \xrightarrow{UO_f} \dots \xrightarrow{UO_f} |\Psi_f^q\rangle$$

$$|\Psi\rangle \xrightarrow{UO_N} |\Psi_N^1\rangle \xrightarrow{UO_N} \dots \xrightarrow{UO_N} |\Psi_N^q\rangle$$

$$|\Psi_f^i\rangle = (UO_f)^i |\Psi\rangle$$

$$|\Psi_N^i\rangle = U^i |\Psi\rangle$$

$$D_f^i = TD(|\Psi_f^i\rangle, |\Psi_N^i\rangle) = TD(O_f|\Psi_f^{i-1}\rangle, |\Psi_N^{i-1}\rangle)$$

$$\leq TD(O_f|\Psi_f^{i-1}\rangle, O_f|\Psi_N^{i-1}\rangle) + TD(O_f|\Psi_N^{i-1}\rangle, |\Psi_N^{i-1}\rangle)$$

$$\leq D_f^{i-1} + TD(O_f|\Psi_N^{i-1}\rangle, |\Psi_N^{i-1}\rangle)$$

$$D_f^0 = TD(|\Psi_f^i\rangle, |\Psi_N^i\rangle) = TD(|\Psi\rangle, |\Psi\rangle) = 0$$

Claim: $\mathrm{Exp}[TD(O_f|\Psi_N^i\rangle, |\Psi_N^i\rangle)] \leq 2\sqrt{\lambda}$

FUJITSU

- Q_f be the projector that projects input register to $|k\rangle$ to a subspace where $f(z) = 1$
  - $Q_f = \sum_{z,f(z)=1} Q_z$, where $Q_z = (I \otimes |\mathrm{z}\rangle \otimes \mathrm{I})(I \otimes \langle \mathrm{z}| \otimes \mathrm{I})$
- $Exp\left[\left\|Q_f|\Psi_N^i\rangle\right\|^2\right] = \lambda$
- $\mathrm{Exp}\left[TD(O_f|\Psi_N^i\rangle, |\Psi_N^i\rangle)\right] \leq 2Exp\left[\left\|Q_f|\Psi_N^i\rangle\right\|\right]$

$$\leq 2\sqrt{Exp\left[\left\|Q_f|\Psi_N^i\rangle\right\|^2\right]} = 2\sqrt{\lambda}$$

AvgSearch: Adversarial Bound

FUJITSU

$$\text{Adv} \leq Exp\left[D_f^q\right] = Exp\left[D_f^{q-1}\right] + \text{Exp}[TD\left(O_f\left|\Psi_N^i\right\rangle, \left|\Psi_N^i\right\rangle\right)]$$

$$\leq 2q\sqrt{\lambda}$$

Random Function vs Random Permutation

FUJITSU

Zhandry's theorem[Zha12]:

D_r is a distribution on $X \to Y$ indexed by $\mathrm{r} \in \mathbb{Z} \cup \{\infty\}$, s.t. for every k pairs $(x_i, y_i) \in X \times Y$ the function $p(r) = \Pr_{f \leftarrow D_r}[f(x_i) = y_i, \forall [1,k]]$ is a polynomial of degree at most k in $\frac{1}{r}$; then $Adv(D_r, D_\infty) \leq \frac{Cq^3}{r}$ for some universal constant C

Random Function vs Random Permutation[Zhandry15]

FUJITSU

Define D_r as follows:

$$[N] \xrightarrow{F \leftarrow RF} [r] \xrightarrow{\pi \leftarrow RI} [N]$$

RI is a partial Random Injective function defined over range of $F([N])$

Observation:

D_N is a $[N] \rightarrow [N]$ Random Function

D_∞ is a $[N] \rightarrow [N]$ Random Permutation

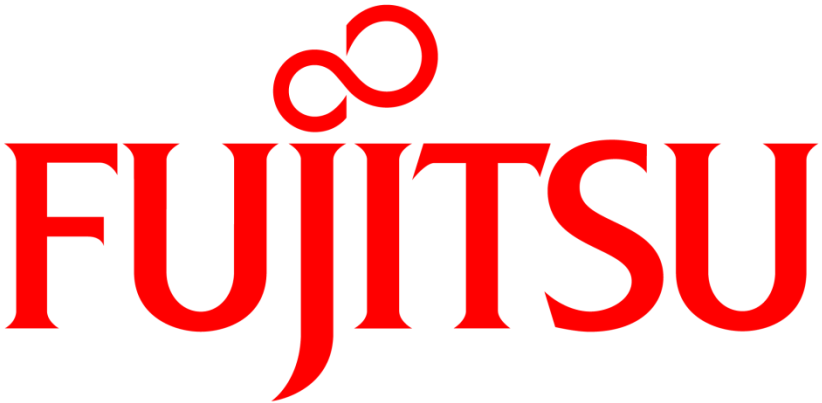
By Zhandry's theorem:

$$\text{Adv(RF,RP)} \leq \frac{Cq^3}{N}$$

Conclusion

FUJITSU

- Adversary Methods and Polynomial methods have a long line of research for proving lower bounds for Quantum Algorithms
- Polynomial method requires symmetry in the problem domain
- Depending on problem in worst case setting sometime
  - Adversary method gives better lower bound
  - Polynomial method gives better lower bound
  - They are equivalent
- However, the average case setting is still a relatively new line of research and not much is known on how these two methods compare against each other.
- Open Problem: Can we use adversary method to show RF , RP equivalence?



shaping tomorrow with you