Name: $\qquad$

Entry number: $\qquad$
There are 2 questions for a total of 20 points.

1. (10 points) Given a 4-to-1 function $f:\{0,1\}^{n} \rightarrow\{0,1\}^{n}$ such that $f(x)=f(x \oplus a)=f(x \oplus b)=$ $f(x \oplus a \oplus b)$ for some $a, b \neq 0^{n}$ and $a \neq b$. Give an efficient Quantum algorithm for finding $a$ and $b$. Discuss running time. You may use the following Quantum gate:

2. (10 points) Suppose you are given the following quantum gates:
3. $\mathrm{QFT}_{n}: n$-qubit QFT
4. InvQFT ${ }_{n}$ : $n$-qubit inverse QFT
5. $R_{k} \equiv\left[\begin{array}{cc}1 & 0 \\ 0 & e^{\frac{2 \pi i}{2^{k}}}\end{array}\right]$ for $k=1, \ldots, n$.

Given two $n$-qubit registers that are initialized to $|x\rangle$ and $|y\rangle$ respectively, describe how you would compute $\left|(x+y)\left(\bmod 2^{n}\right)\right\rangle$ using just the gates given above. You may also use the controlled operations.

