

# Quantum computing & cryptography

Week 7

## Quantum algorithms: Introduction

- General features
- Deutsch's problem  $\rightarrow$  toy problem to illustrate techniques

Steve Vickers

## Computing a function $f$

$x$   $\xrightarrow{\quad}$   $f(x)$   
n-bit parameter  $0 \leq x < 2^n$       m-bit result  $0 \leq f(x) < 2^m$

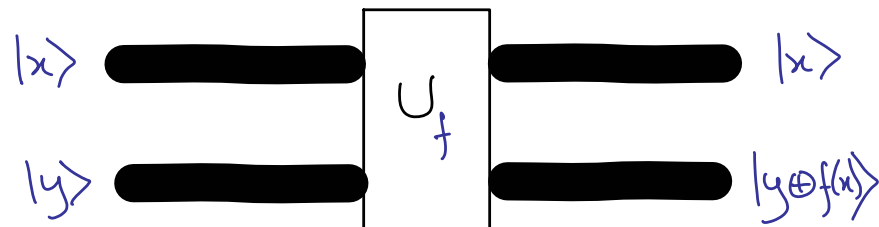
To ensure reversibility:  
separate input & output registers  
n bits      m bits

Before       $x$        $y$   
After       $x$        $y \oplus f(x)$

## For quantum computation

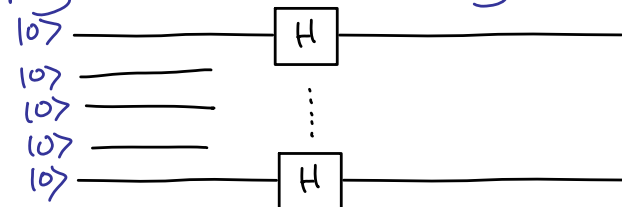
$U_f$  - unitary operator on  $n+m$  qubits

$$U_f |x\rangle_n |y\rangle_m = |x\rangle_n |y \oplus f(x)\rangle_m$$
$$U_f U_f = 1$$



## Hadamards on input

Apply H to  $|0\rangle$  on every input line



$$\text{Written } H^{\otimes n} |0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{0 \leq x < 2^n} |x\rangle_n$$

e.g.  $n=2$ :

$$(H \otimes H) |0\rangle_2 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Now apply  $U_f$

$$\begin{aligned}
 U_f (H^{\otimes n} \otimes I_m) |0\rangle_n |0\rangle_m \\
 = \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} U_f (|x\rangle_n |0\rangle_m) \\
 = \frac{1}{2^{n/2}} \sum_{0 \leq x < 2^n} |x\rangle_n |f(x)\rangle_m
 \end{aligned}$$

One application of  $U_f \Rightarrow$

State with information about  $f(x)$  for every  $x$   
 - but you can't extract it  
 Measurement  $\Rightarrow$  random  $x$  and its  $f(x)$

### Wishful Thinking

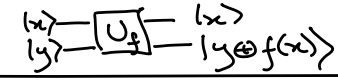




- apply  $H^{\otimes n}$  to input
- apply  $U_f$  just once
- make copies of state
- measure them all to get lots of random pairs  $(x, f(x))$

Can't!  
 No-cloning theorem

### Deutsch's problem

$f$  a function 1 bit argument  
 1 bit result

4 possibilities

	$f(0)$	$f(1)$		
constant 0	0	0		1
identity	0	1		$C_{10}$
flip	1	0		$C_{10} X_0$
constant 1	1	1		$X_0$

Is  $f$  constant? 1 bit of information about  $f$

2 out of 4 possible  $f$ 's are constant.

Apply  $f$  once - get one bit of info.  
 e.g. given  $x$ ,  $f(x)$  is one bit

Classically to find whether constant:

apply  $f$  twice -  $f(0), f(1)$

Quantum can do better

- use Hadamards
- apply  $f$  once

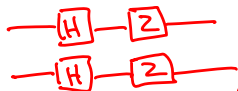
No free lunch!  
 Still just get one bit of info.

## Clever tricks

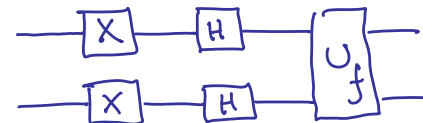
- Apply Hadamards to input and output
- Use other gates too

$$\begin{aligned}
 & \begin{array}{c} \text{---} \boxed{X} \text{---} \boxed{H} \text{---} \\ \text{---} \boxed{X} \text{---} \boxed{H} \text{---} \end{array} \quad (H \otimes H) (X \otimes X) |00\rangle \\
 & = (H \otimes H) |11\rangle \\
 & = \frac{1}{2} (|10\rangle - |11\rangle) \otimes (|10\rangle - |11\rangle) \\
 & = \frac{1}{2} (|00\rangle - |10\rangle - |01\rangle + |11\rangle)
 \end{aligned}$$

could use



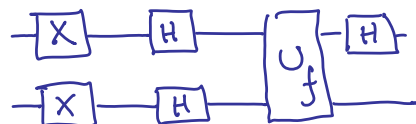
## Apply $U_f$



$$\begin{aligned}
 & U_f (H \otimes H) (X \otimes X) |00\rangle \\
 & = \frac{1}{2} (U_f |00\rangle - U_f |10\rangle - U_f |01\rangle + U_f |11\rangle) \\
 & = \frac{1}{2} (|0\rangle |f(0)\rangle - |1\rangle |f(1)\rangle - |0\rangle |\tilde{f}(0)\rangle + |1\rangle |\tilde{f}(1)\rangle) \\
 & = \begin{cases} \frac{1}{2} (|0\rangle - |1\rangle) (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) = f(1) \\ \frac{1}{2} (|0\rangle + |1\rangle) (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) \neq f(1) \end{cases}
 \end{aligned}$$

## Apply Hadamard to input

$$\begin{cases} \frac{1}{2} (|0\rangle - |1\rangle) (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) = f(1) \\ \frac{1}{2} (|0\rangle + |1\rangle) (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) \neq f(1) \end{cases}$$



$$\begin{aligned}
 & H, U_f (H \otimes H) (X \otimes X) |00\rangle \\
 & = \begin{cases} \frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) = f(1) \\ \frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) \neq f(1) \end{cases}
 \end{aligned}$$

## Measurements

$$\begin{cases} \frac{1}{\sqrt{2}} |1\rangle (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) = f(1) \\ \frac{1}{\sqrt{2}} |0\rangle (|f(0)\rangle - |\tilde{f}(0)\rangle) & \text{if } f(0) \neq f(1) \end{cases}$$

Measure input

result  $\begin{cases} 1 & f \text{ constant} \\ 0 & f \text{ not constant} \end{cases}$

Resulting output state =  $\frac{1}{\sqrt{2}} (|f(0)\rangle - |\tilde{f}(0)\rangle)$

Measure output

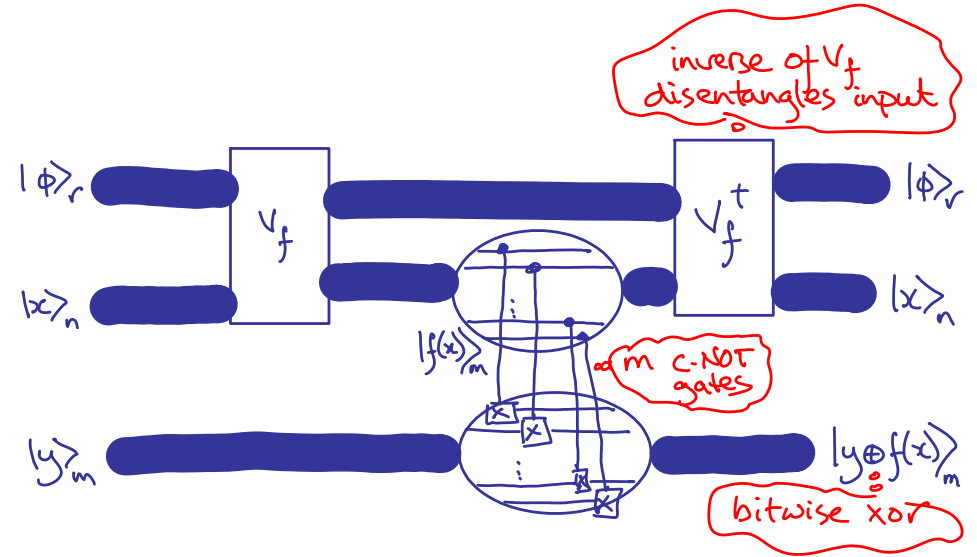
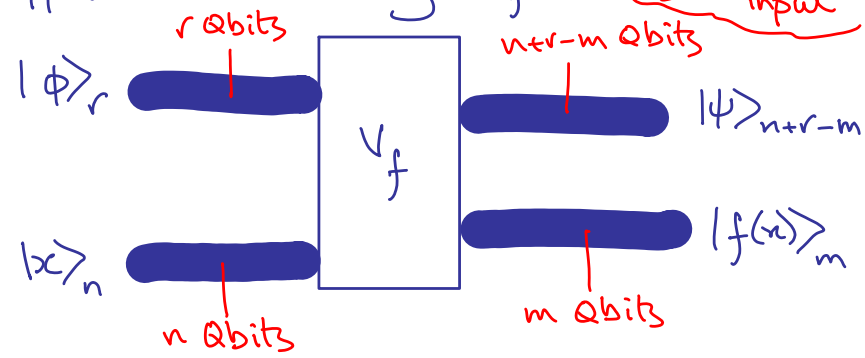
result 0 or 1 at random

Learn nothing about  $f(0)$  or  $f(1)$

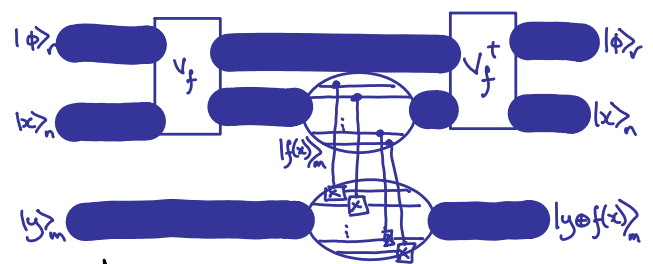


General argument (Works for multibit input & output)

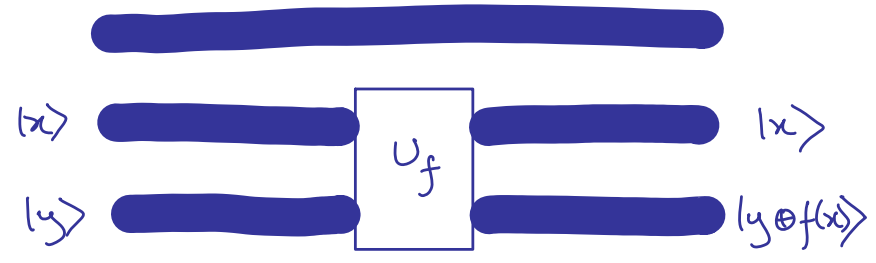
function  $f$  -  $n$  input bits  
 -  $m$  output bits  
 Suppose have unitary  $V_f$  (calculates  $f$  but may entangle input)



Attend



Acts as required:



To summarize

- When circuit involves other qubits - must be careful not to entangle them
- Applying  $V_f$  and  $V_f^\dagger$  is like having to apply  $V_f$  twice
- Lose benefit of quantum computation in Deutsch problem
- In other problems the benefit can be more clear-cut (which was only a toy problem anyway)