Quantum Error Correction

SOURCES:

Michele Mosca

Richard Spillman

Quantum Errors

- **PROBLEM**: When computing with a quantum computer, you can't look at what the computer is doing
  - You are only allowed to look at the end
- **RESULT**: What happens if an error is introduced during calculation?
- **SOLUTION**: We need some sort of quantum error detection/correction procedure

Classical Error Codes

- In standard digital systems bits are added to a data word in order to detect/correct errors
- A code is ***e-error detecting*** if any fault which causes at most **e bits** to be erroneous can be detected
- A code is ***e-error correcting*** if for any fault which causes at most e erroneous bits, the set of all correct bits can be automatically determined
- The ***Hamming Distance***, d, of a code is the minimum number of bits in which any two code words differ
  - the *error detecting/correcting capability* of a code depends on the value of d

Parity Checking

- PROCESS: Add an extra bit to a word before transmitting to make the total number of bits even or odd (even or odd parity)
  - at the receiving end, check the number of bits for even or odd parity
  - It will detect a single bit error
  - Cost: extra bit

- Example: Transmit the 8-bit data word 1 0 1 1 0 0 0 1
  - Even parity version: 1 0 1 1 0 0 0 1 0
  - Odd parity version: 1 0 1 1 0 0 0 1 1

Quantum Error Correcting by Peter Shor

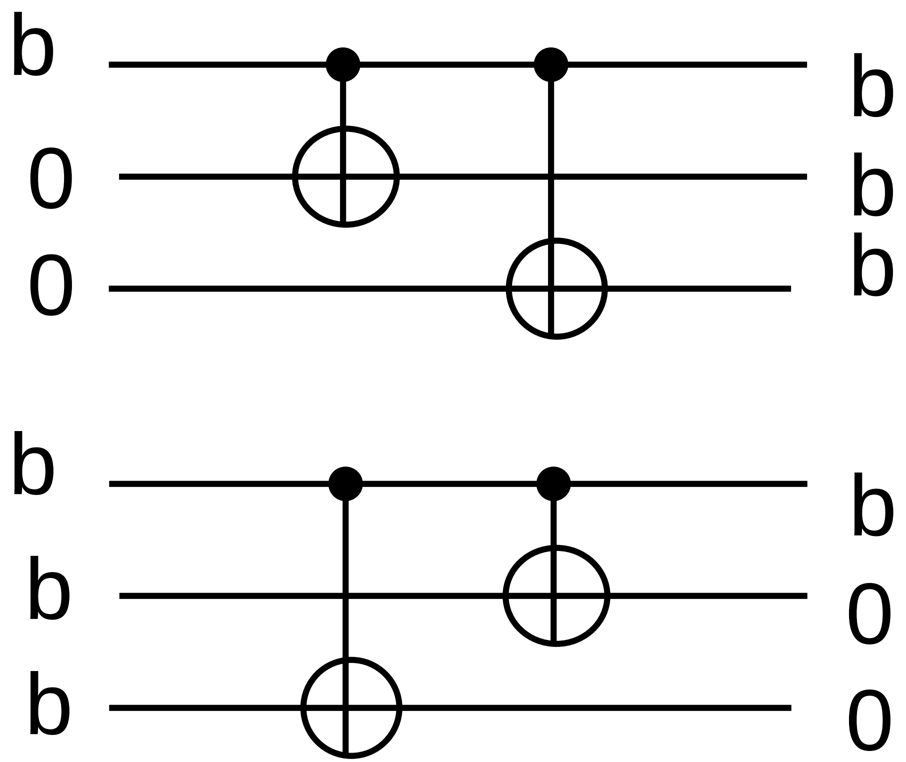
- In 1995, Peter Shor developed an improved procedure using 9 qubits to encode a single qubit of information

- His algorithm was a **majority vote type** of system that allowed **all single qubit errors to be *detected and corrected***

Classical Error Correcting Codes

- Suppose errors in our physical system for storing 0 and 1 cause each physical bit to be toggled independently with probability p
- We can reduce the probability of error to be in $O(p^2)$ by using a “repetition code”
- e.g. : encode a logical 0 with the state 000 and a logical 1 with the state 111

Reversible networks for encoding and decoding



Classical Error Correcting Codes

- After the errors occur, decode the logical bits by taking the majority answer of the three bits and correct the encoded bits
- So

$$000 \to 000 \qquad 111 \to 111$$

$$001 \to 000 \qquad 011 \to 111$$

$$010 \to 000 \qquad 101 \to 111$$

$$100 \to 000 \qquad 110 \to 111$$

Classical Error Correcting Codes

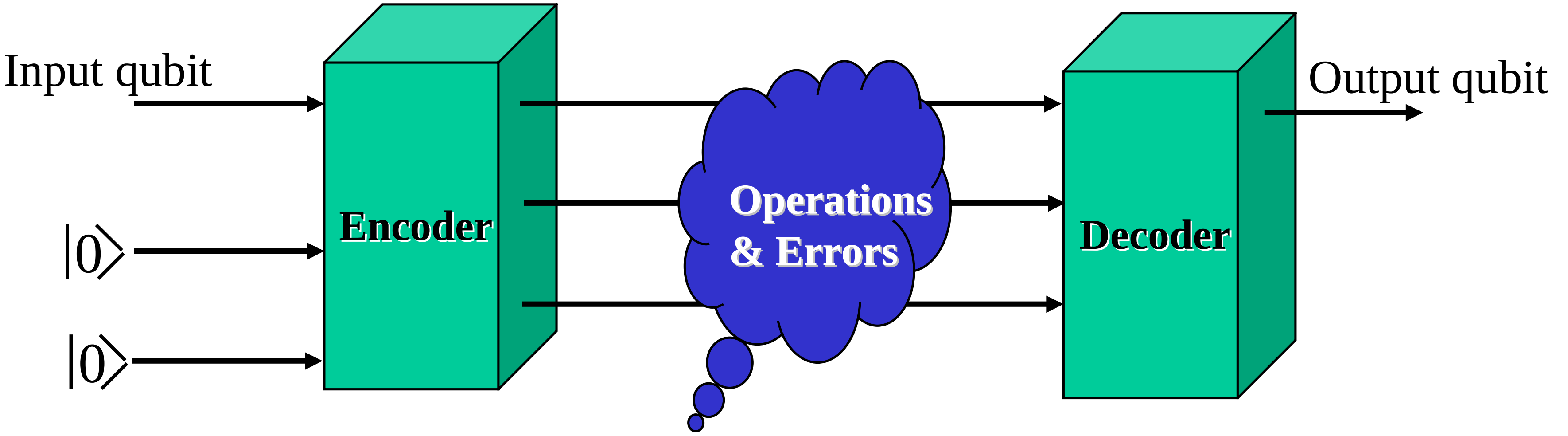
- As long as less than 2 errors occurred, we will keep the correct value of the logical bit
- The probability of 2 or more errors is

$$3p^2(1-p)+p^3 = 3p^2 - 2p^3 \in O(p^2)$$

(which is less than p if $p < \frac{1}{2}$)

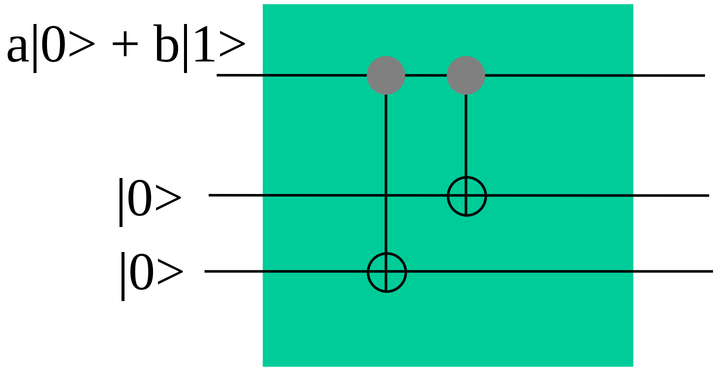
Example of 3-qubit error correction

- A **3-bit** quantum error correction scheme uses an encoder and a decoder circuit as shown below:



Encoder

❖ The **encoder** will <u>entangle the two redundant qubits</u> with the input qubit:



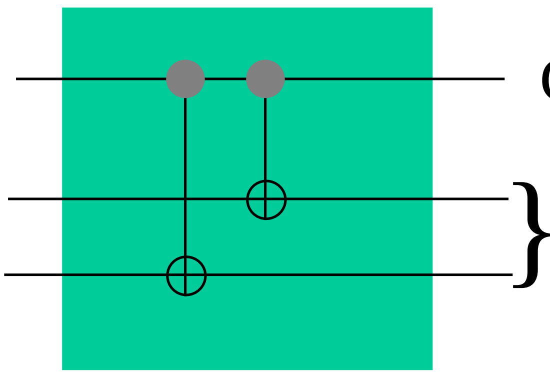
1. If the input state is |0> then the encoder does nothing so the output state is |000>

2. If the input state is |1> then the encoder flips the lower states so the output state is |111>

3. If the input is an superposition state, then the output is the entangled state a|000> + b|111>

Decoder

- Problem: Any correction must be done <u>without looking at the output</u>
  - The decoder looks just like the encoder:



Corrected output

Measure: if 11 <u>flip</u> the top qubit

If the input to the decoder is |000> or |111> there was no error so the output of the decoder is:

Input	Output	
|000>	|000>	
|111>	|100>	(the top 1 causes the bottom bits to flip)

Error free flag

Example continued:

Consider all the possible error conditions:

No Errors:

a|000> + b|111> decoded to a|000> + b|100> = (a|0> + b|1>)|00>

Top qubit flipped:

a|100> + b|011> decoded to a|111> + b|011> = (a|1> + b|0>)|11>

So, flip the top qubit = (a|0> + b|1>)|11>

Middle qubit flipped:

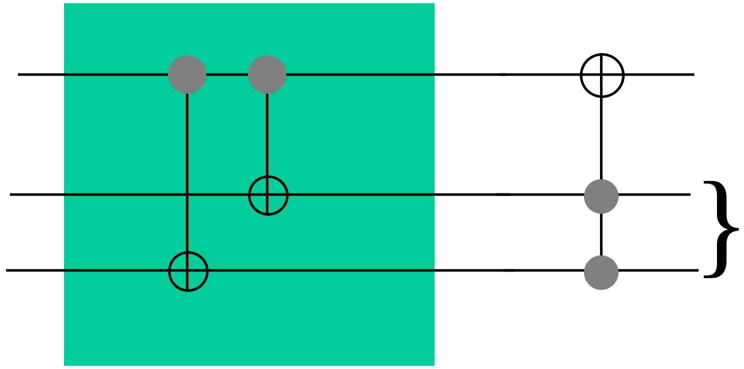
a|010> + b|101> decoded to a|010> + b|110> = (a|0> + b|1>)|10>

Bottom qubit flipped:

a|001> + b|110> decoded to a|001> + b|101> = (a|0> + b|1>)|01>

Decoder without Measurement

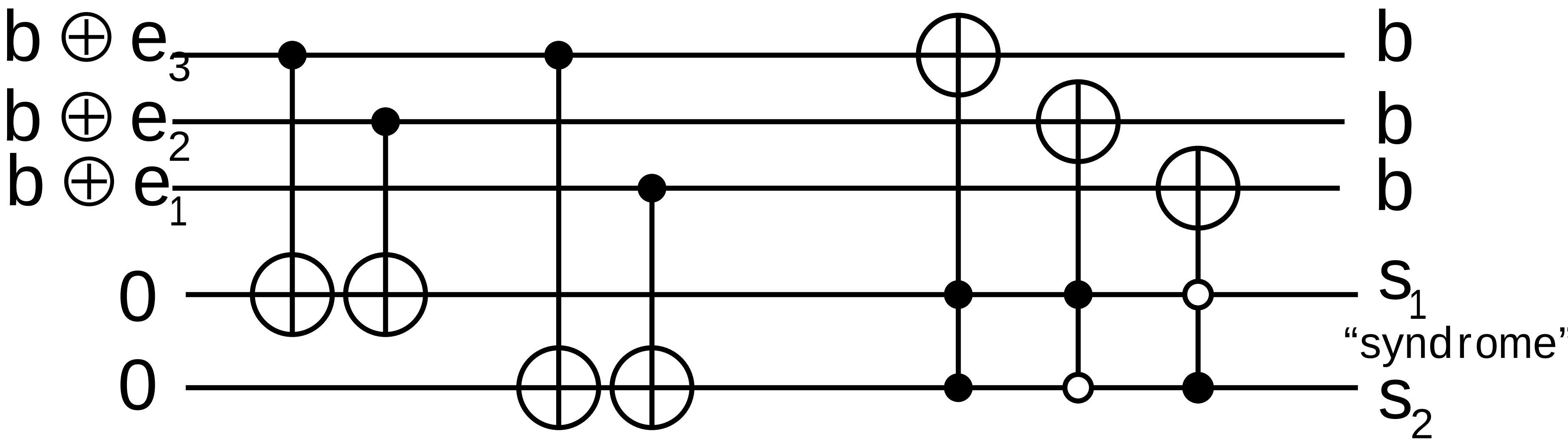
- The prior decoder circuit requires the measurement of the two extra bits and a possible flip of the top bit
  - Both these operations can be implemented automatically using a Toffoli gate



If these are both 1 then flip the top bit

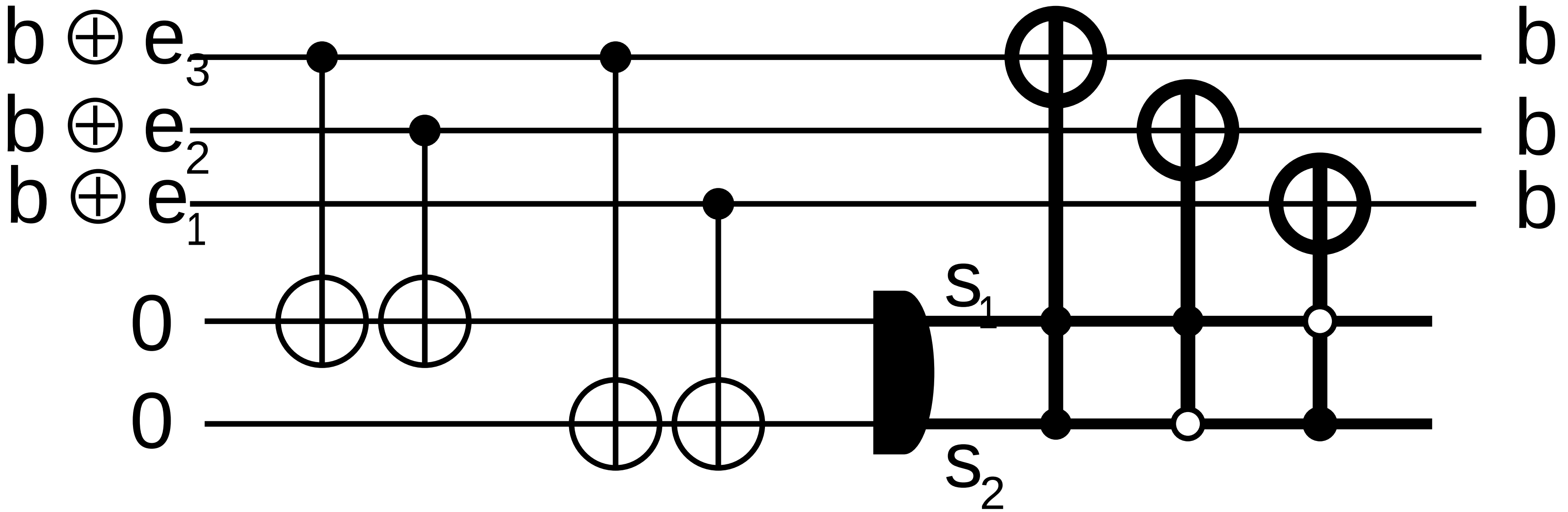
Reversible 5-qubit network for error correction

❖ Assume that $e_3 + e_2 + e_1 \leq 1$ $e_i \in \{0,1\}$

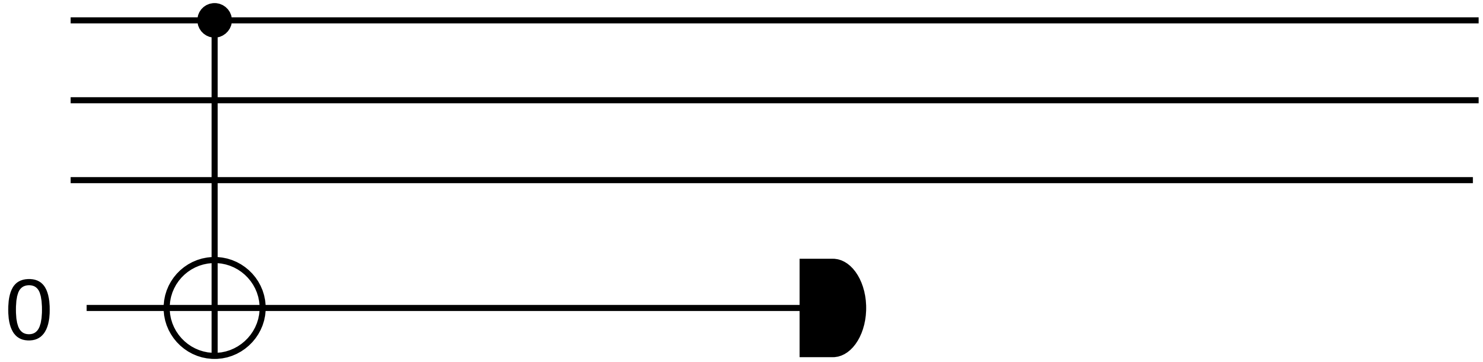


- If $s_1 s_2 = 00$ then no error occurred
- Otherwise, the error occurred in bit j where $j = 2s_1 + s_2$

Equivalently using measurements

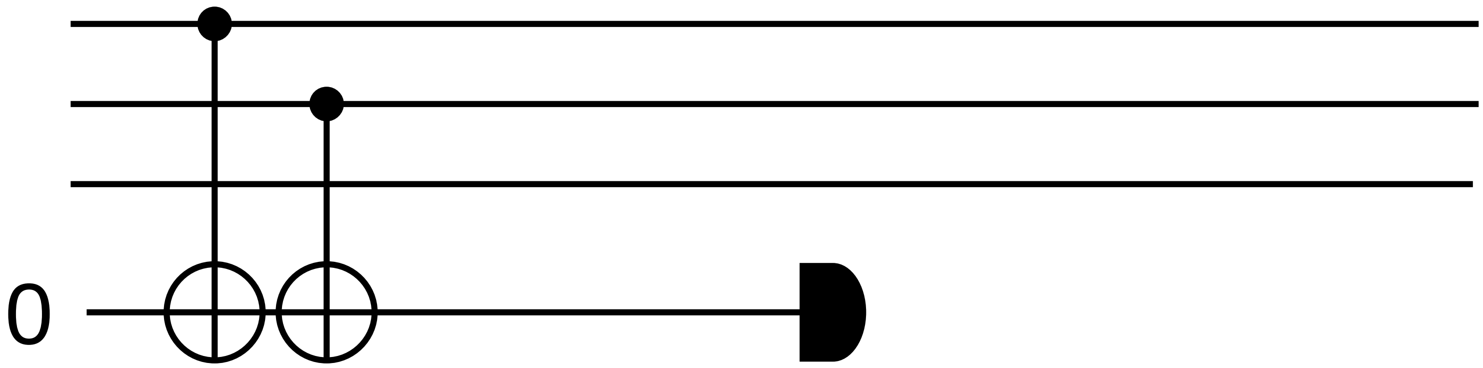


Stabilizer measurement??



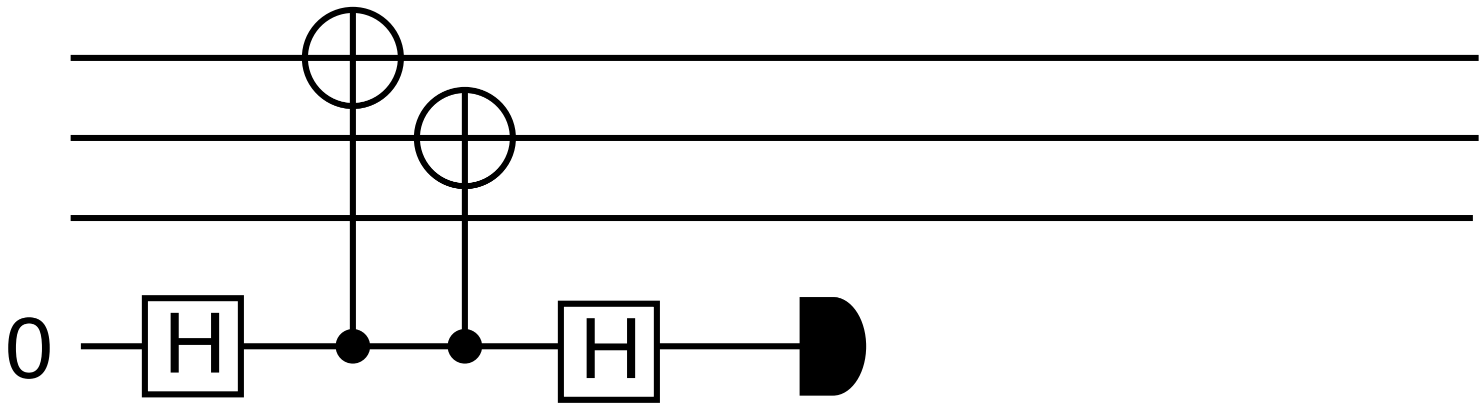
- This is implementing a Z_1 measurement (interpreting 0 as +1, and 1 as –1)

Stabilizer measurement??



- This is implementing a $Z_1 Z_2$ measurement

Stabilizer measurement??



- This is implementing a $X_1 X_2$ measurement

Notation clarification

- For an n-qubit system Z_j denotes

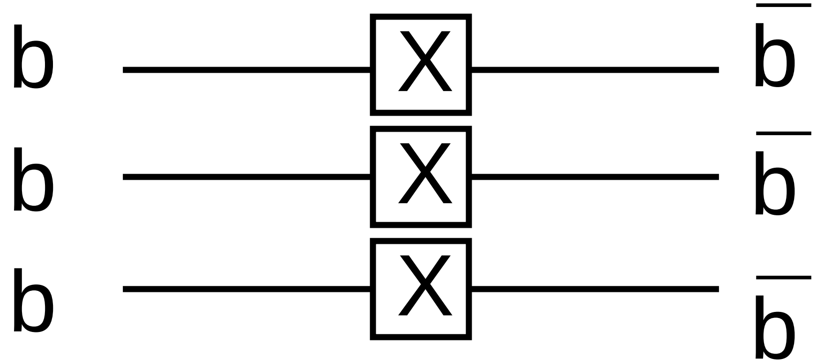
$$\underbrace{I \otimes I \otimes \cdots \otimes I}_{j-1} \otimes Z \otimes \underbrace{I \otimes \cdots \otimes I}_{n-j}$$

- E.g. n=3, then

$$Z_1 Z_2 = (Z \otimes I \otimes I)(I \otimes Z \otimes I) = (Z \otimes Z \otimes I)$$

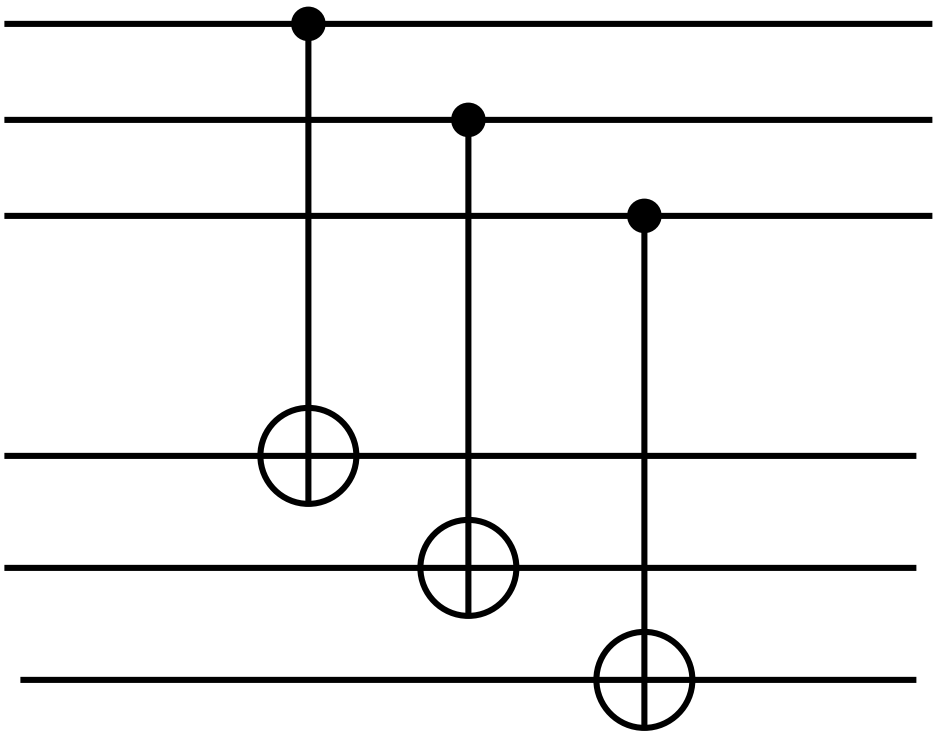
Perform operations on logical bits

- e.g. NOT gate



Perform operations on logical bits

- e.g. c-NOT gate

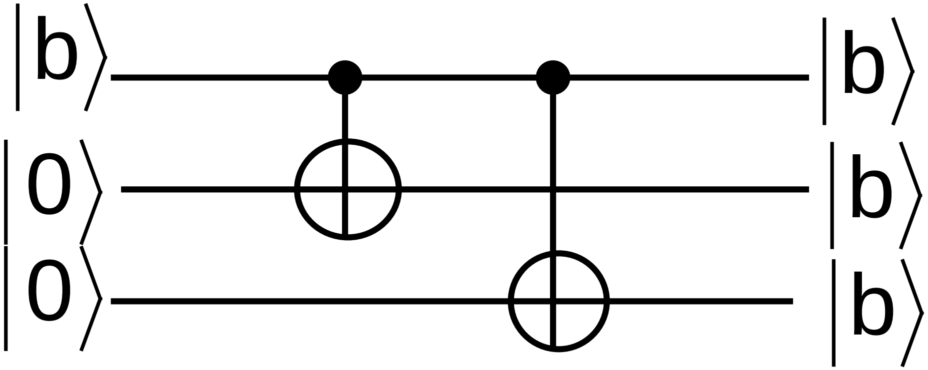


Quantum Error Correcting Codes

- e.g. : encode a logical $|0\rangle$ with the state $|000\rangle$

and a logical $|1\rangle$ with the state $|111\rangle$

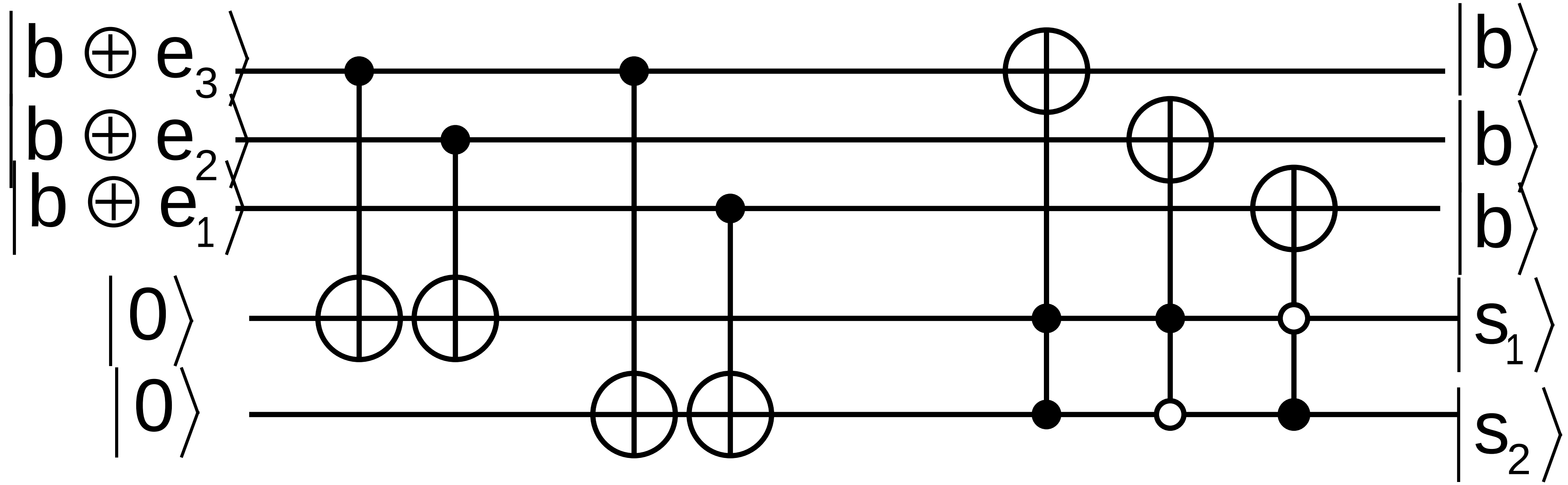
Quantum network for encoding



$$\left(\alpha|0\rangle + \beta|1\rangle\right)|0\rangle|0\rangle \rightarrow \alpha|0\rangle|0\rangle|0\rangle + \beta|1\rangle|1\rangle|1\rangle$$

Quantum network for correcting errors

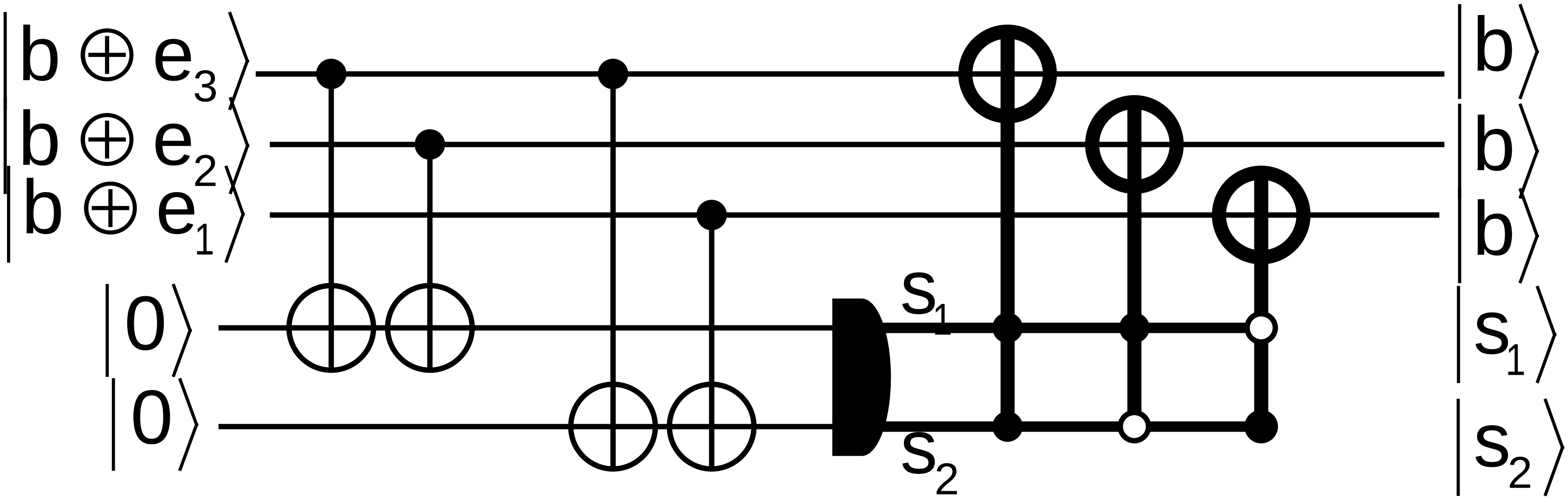
- Assume that $e_3 + e_2 + e_1 \leq 1$ $e_i \in \{0,1\}$



$$\alpha|e_3\rangle|e_2\rangle|e_1\rangle + \beta|1 \oplus e_3\rangle|1 \oplus e_2\rangle|1 \oplus e_1\rangle \rightarrow$$

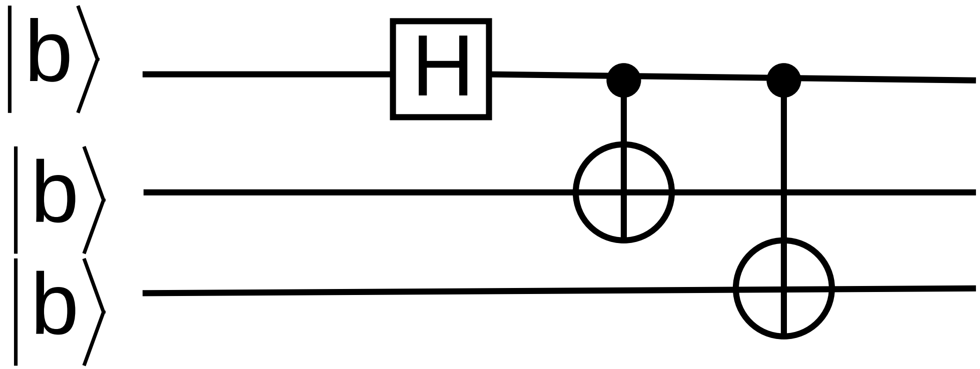
$$\alpha|0\rangle|0\rangle|0\rangle + \beta|1\rangle|1\rangle|1\rangle$$

Equivalently



Perform operations on logical bits

- e.g. Hadamard gate



$$\frac{1}{\sqrt{2}}|b\rangle|b\rangle|b\rangle + \frac{(-1)^b}{\sqrt{2}}|\overline{b}\rangle|\overline{b}\rangle|\overline{b}\rangle$$

What is the problem with classical cryptography?

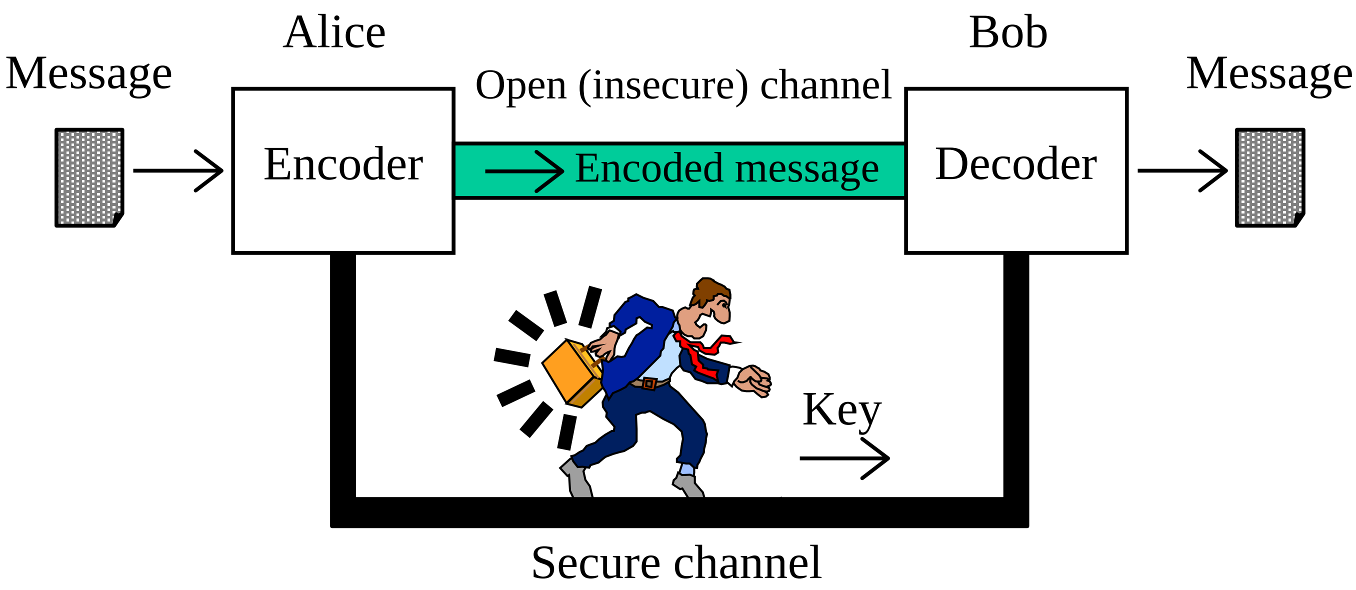
Secret key cryptography

- Requires secure channel for key distribution
- *In principle* every classical channel can be monitored passively
- Security is mostly based on complicated non-proven algorithms

Public key cryptography

- Security is based on non-proven mathematical assumptions (e.g. difficulty of factoring large numbers)
- We DO know how to factorize in polynomial time! Shor's algorithm for quantum computers. Just wait until one is built.
- Breakthrough renders messages insecure *retroactively*

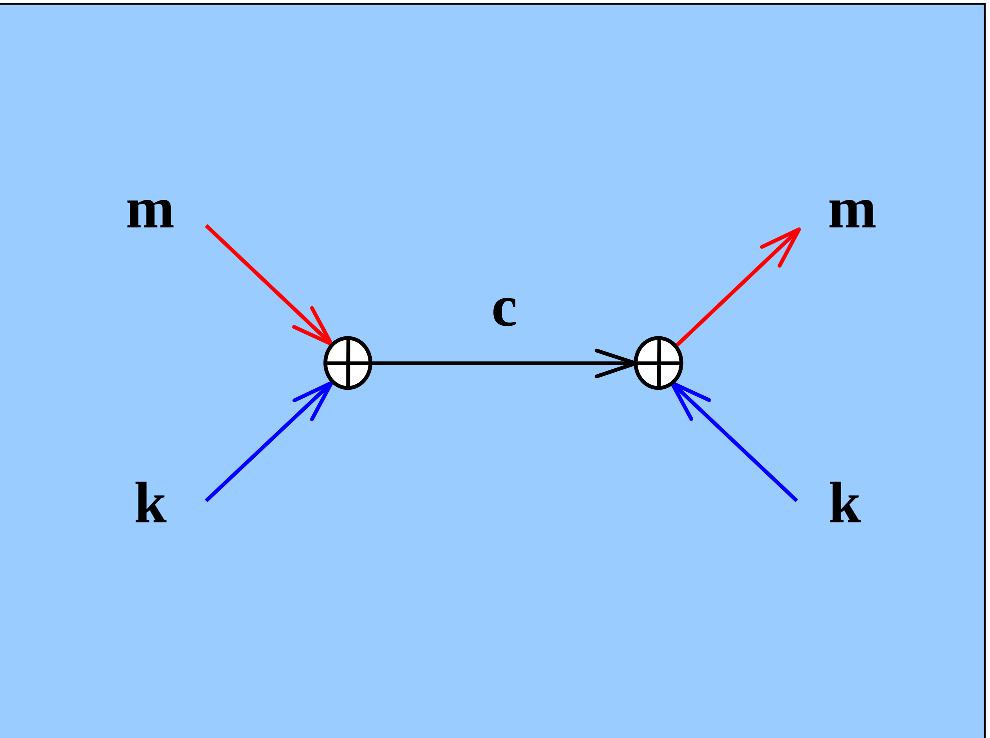
Key distribution

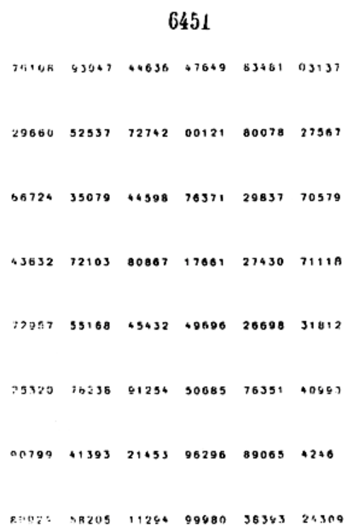


- **Secret key cryptography requires secure channel for key distribution.**
- **<u>Quantum cryptography</u> distributes the key by transmitting quantum states in *open channel.***

The holy grail: ***One-time pad***

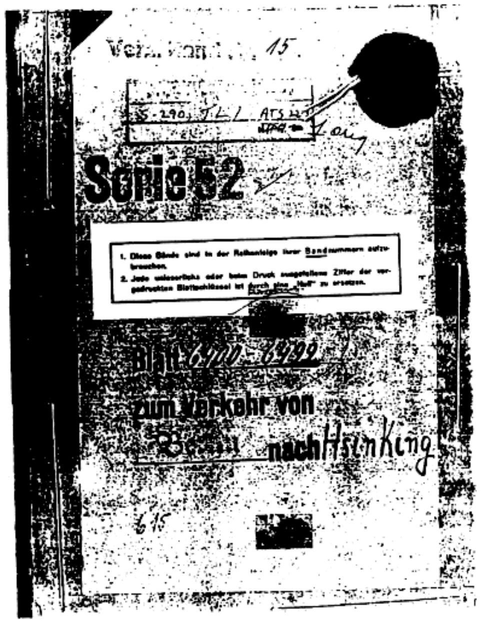
- The only cipher mathematically proven
- Requires massive amounts of key material





6451

76108	93047	44636	47649	83461	03137
29660	52537	72742	00121	80078	27567
66724	35079	44598	76371	29837	70579
43632	72103	80867	17661	27430	71118
72057	55168	45432	49696	26698	31812
75320	76236	91254	50685	76351	40993
00799	41393	21453	96296	89065	4246
89027	58205	11294	99980	36393	24309



Crypto Definitions: Alice, Bob and Eve

- It is a standard in cryptography to define the sender, receiver, and interceptor as:
  - Alice is the one who sends the ciphertext
  - Bob is the one who receives the ciphertext
  - Eve is the (evil) one who tries to steal the plaintext or key