Quantum Software Development

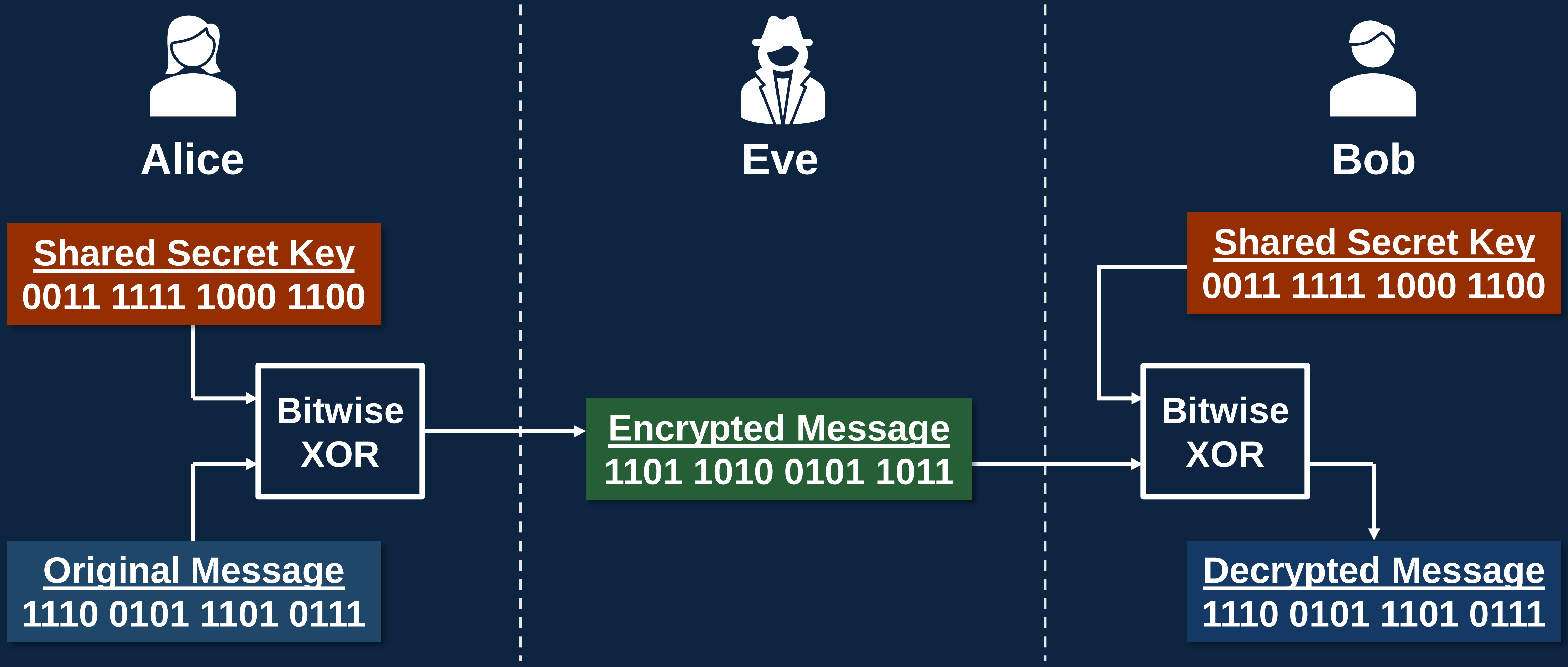
Lecture 5: Quantum Communication (cont.)
Quantum Error Correction

February 14, 2024

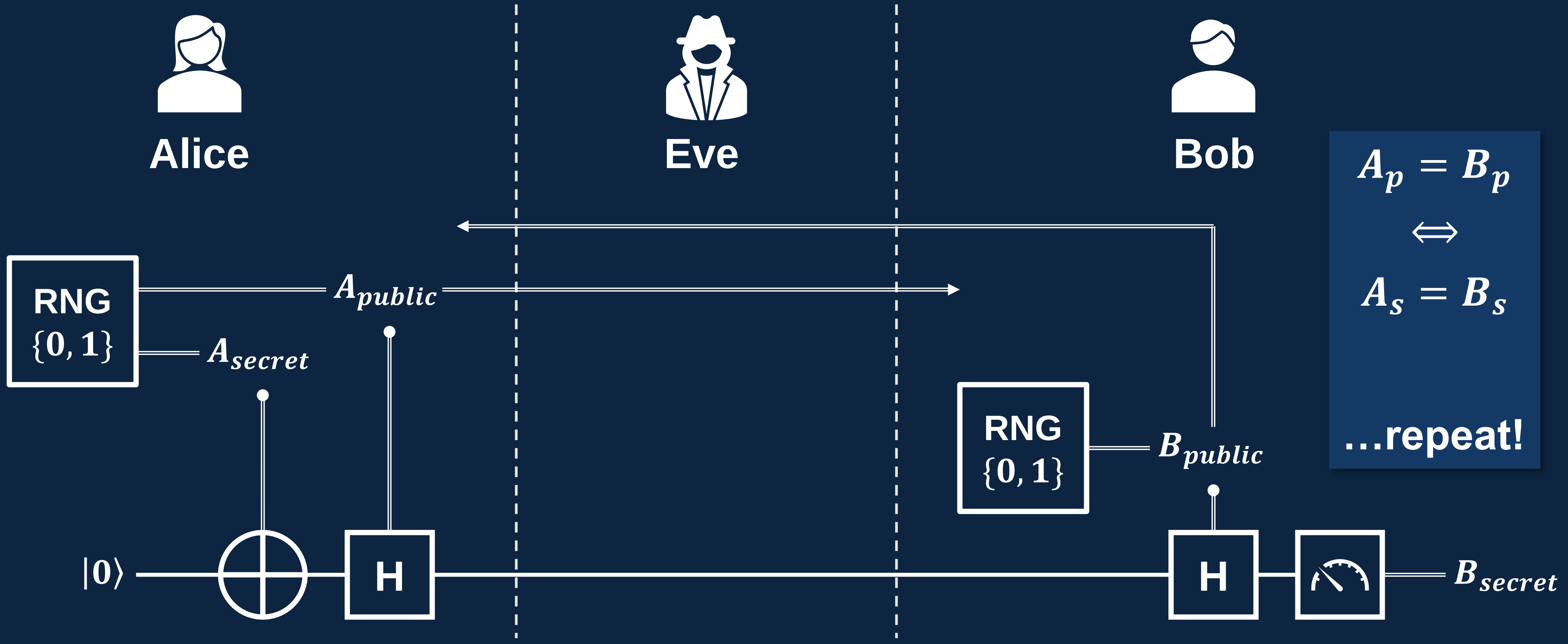
Tufts University | School of Engineering
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Quantum Communication (cont.)

Classical, symmetric-key encryption is sufficient for information security when parties share a secret key.



Quantum key distribution allows parties to generate a secret key without a shared entanglement source.



$$A_p = B_p$$
$$\Leftrightarrow$$
$$A_s = B_s$$

…repeat!

MITRE

Since QKD does not provide source authentication, it fails to improve on classical cryptosystems.

NSA’s criticism of QKD

1. **QKD is only a partial solution**…it does not provide a means to authenticate the transmission source.
2. **QKD requires special purpose equipment…**it also lacks flexibility for upgrades or security patches.
3. **QKD increases infrastructure costs and insider threat risks.**
4. **Securing and validating QKD is a significant challenge.** The actual security provided by a QKD system is not the theoretical unconditional security…but rather the more limited security that can be achieved by hardware and engineering designs.
5. **QKD increases the risk of denial of service.**

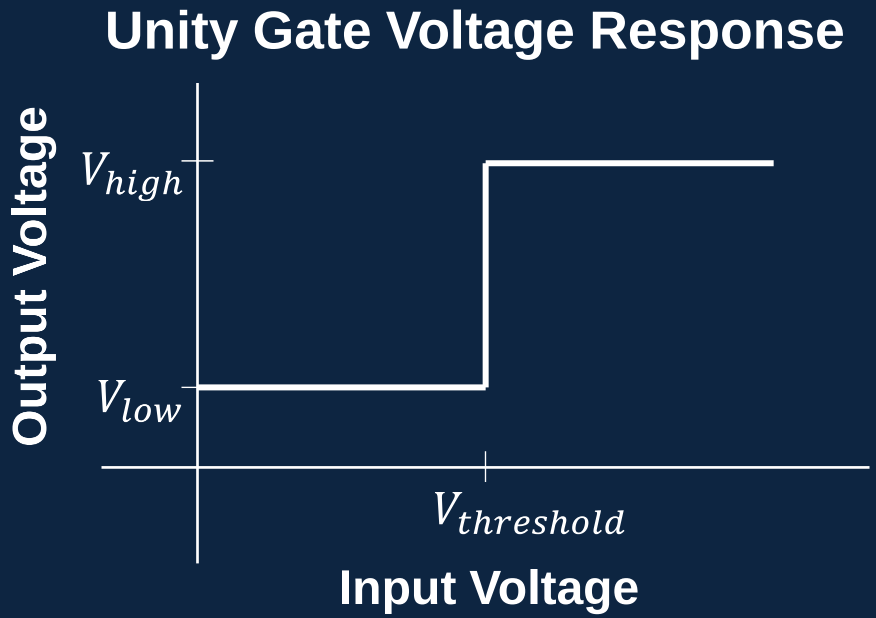
https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Quantum Error Correction

MITRE

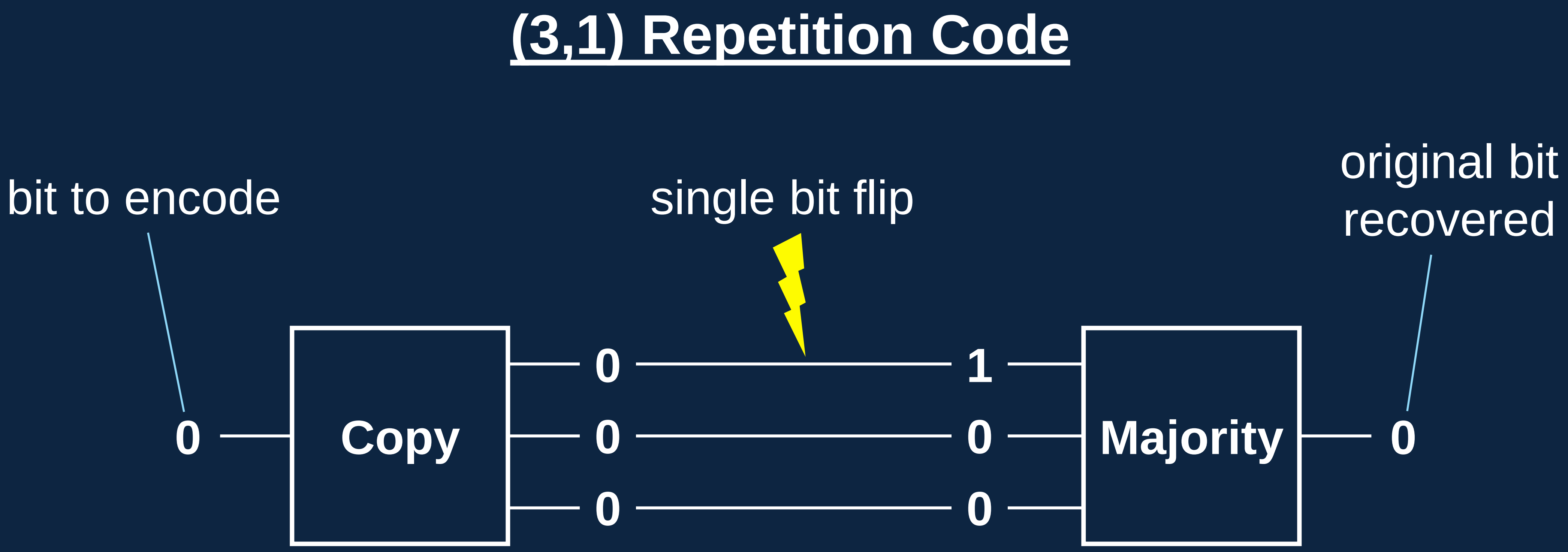
Error correction is necessary for universality.

Life (gene replication) could not occur without biological processes to correct errors in DNA sequences.

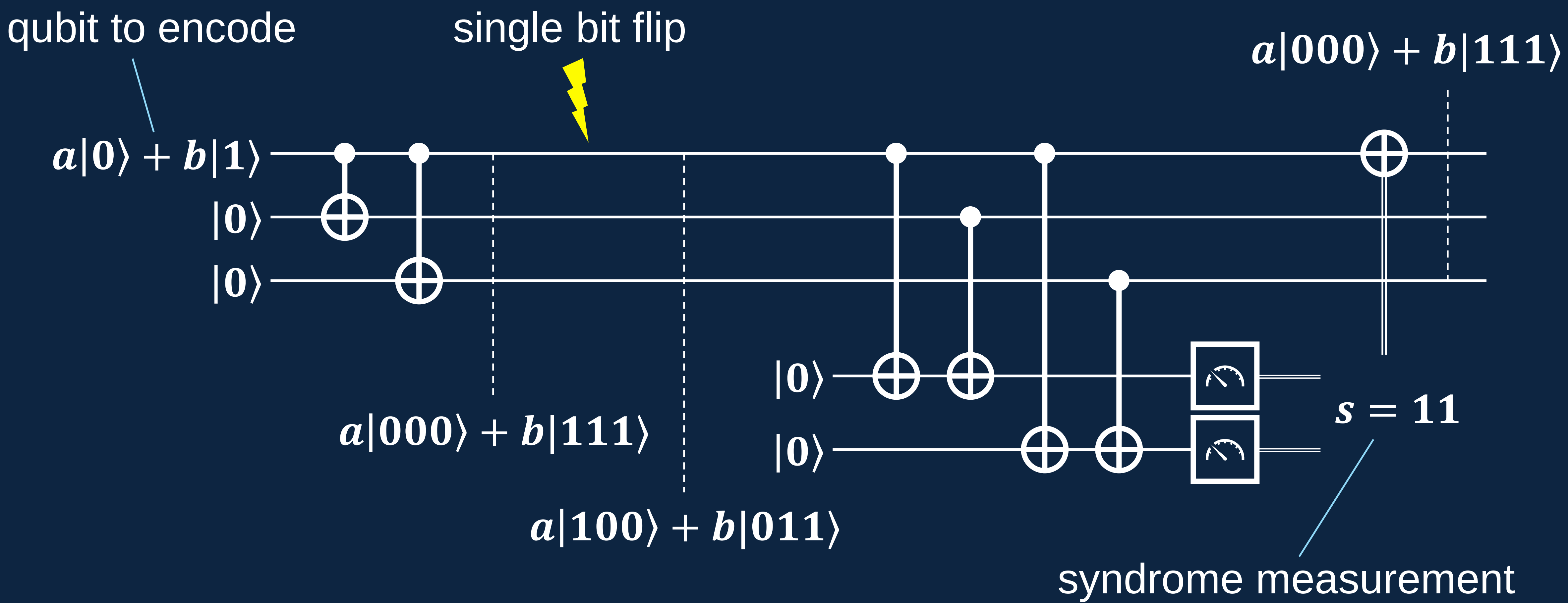


Digital gates correct errors in input voltage. (Analog gates cannot do this and are not universal.)

Error correction codes are used to add redundancy when processing or transmitting information.

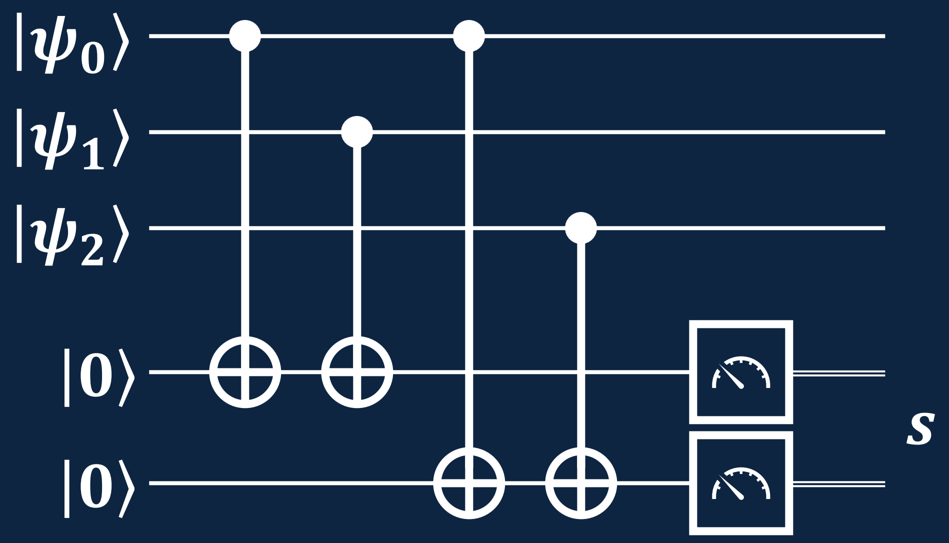


Quantum error correction schemes are designed to fix errors while preserving superposition.



The syndrome measurement itself is part of the error correction process.

Bit Flip Code



s	flipped
00	*None*
01	ψ_2
10	ψ_1
11	ψ_0

Suppose $|\psi\rangle = |000\rangle$ when a "partial" bit flip error occurs in ψ_0, resulting in:

$$|\psi\rangle = c|000\rangle + d|100\rangle$$

After the syndrome measurement, either:

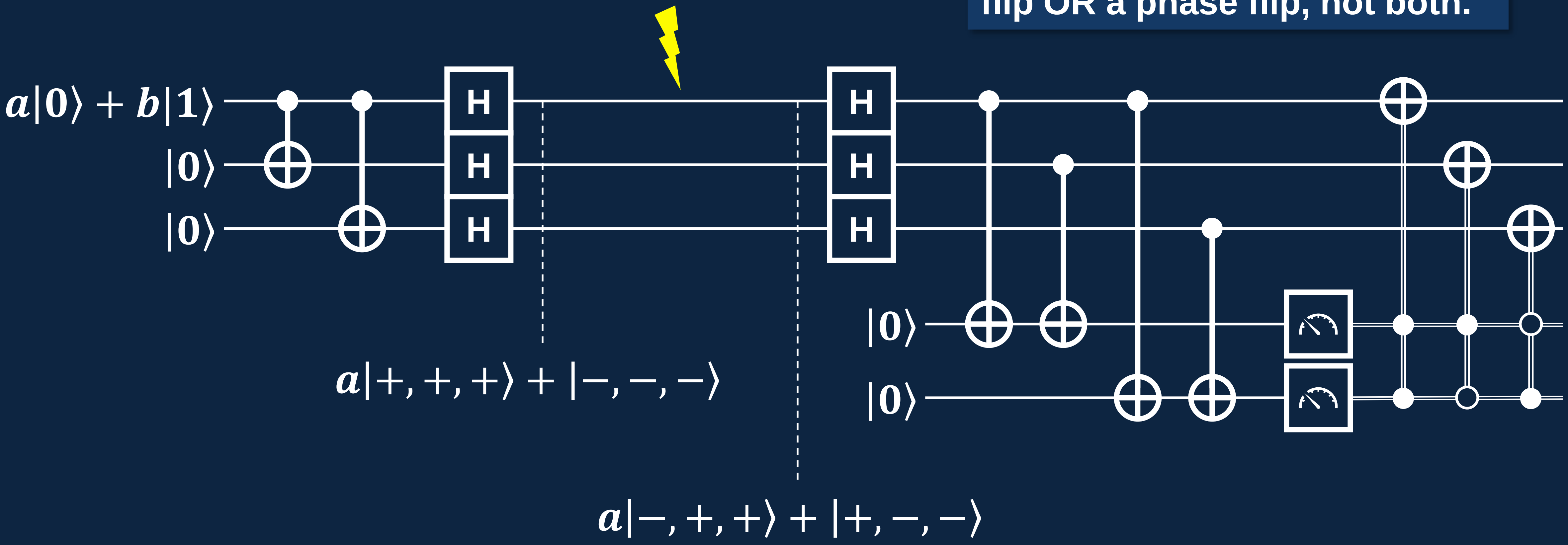
- $|\psi\rangle = |000\rangle$, OR
- $|\psi\rangle = |100\rangle$ and the error can be corrected

MITRE

How could the bit-flip error correction circuit be modified to correct phase flips?

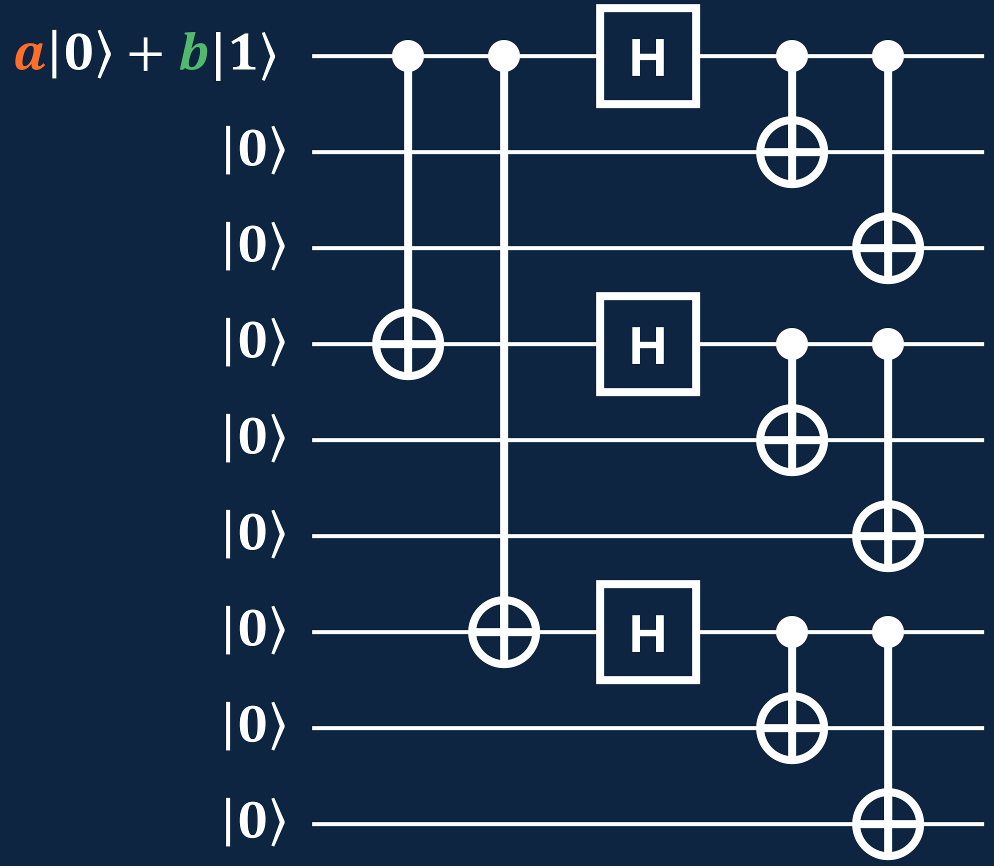
This approach can detect a bit flip OR a phase flip, not both.

single phase flip

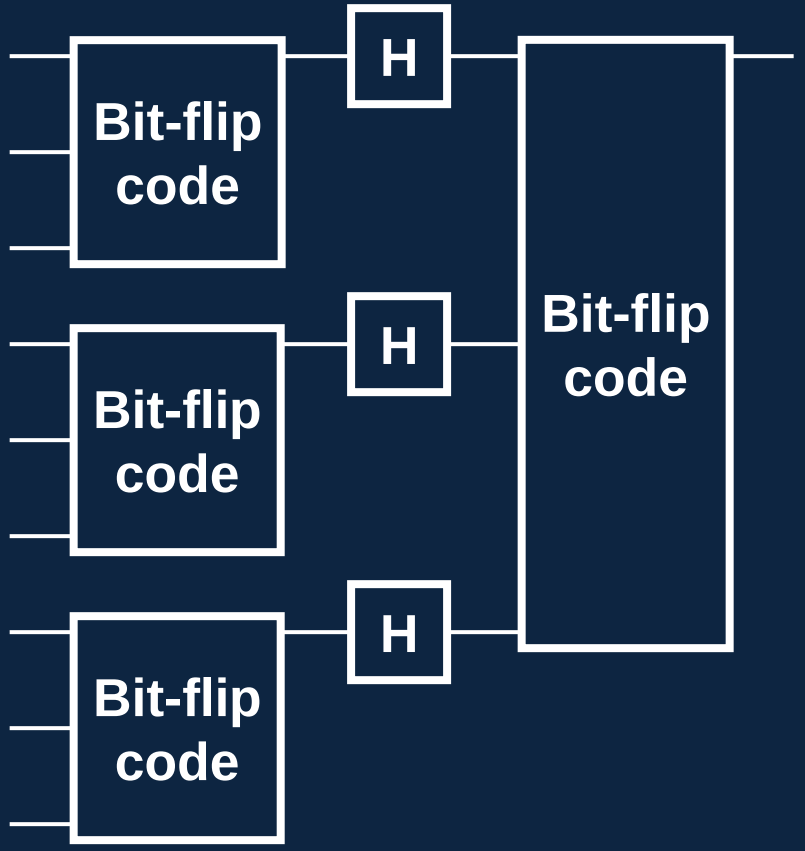


MITRE

The Shor code corrects both bit- and phase-flip errors.

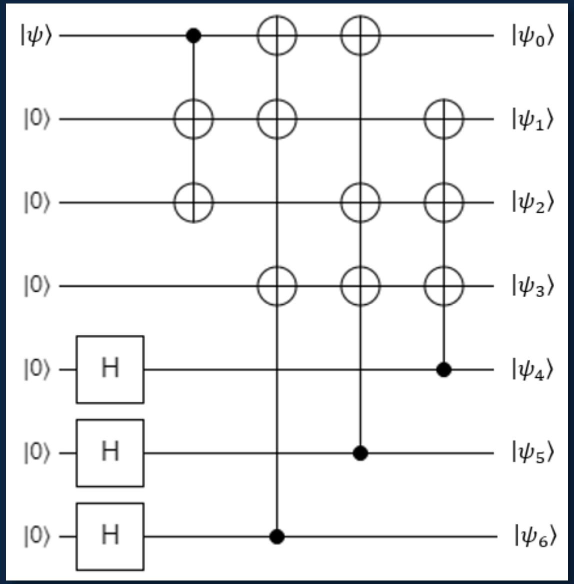


$$\frac{a}{\sqrt{8}}(|000\rangle + |111\rangle)^{\otimes 3}$$
$$+$$
$$\frac{b}{\sqrt{8}}(|000\rangle - |111\rangle)^{\otimes 3}$$

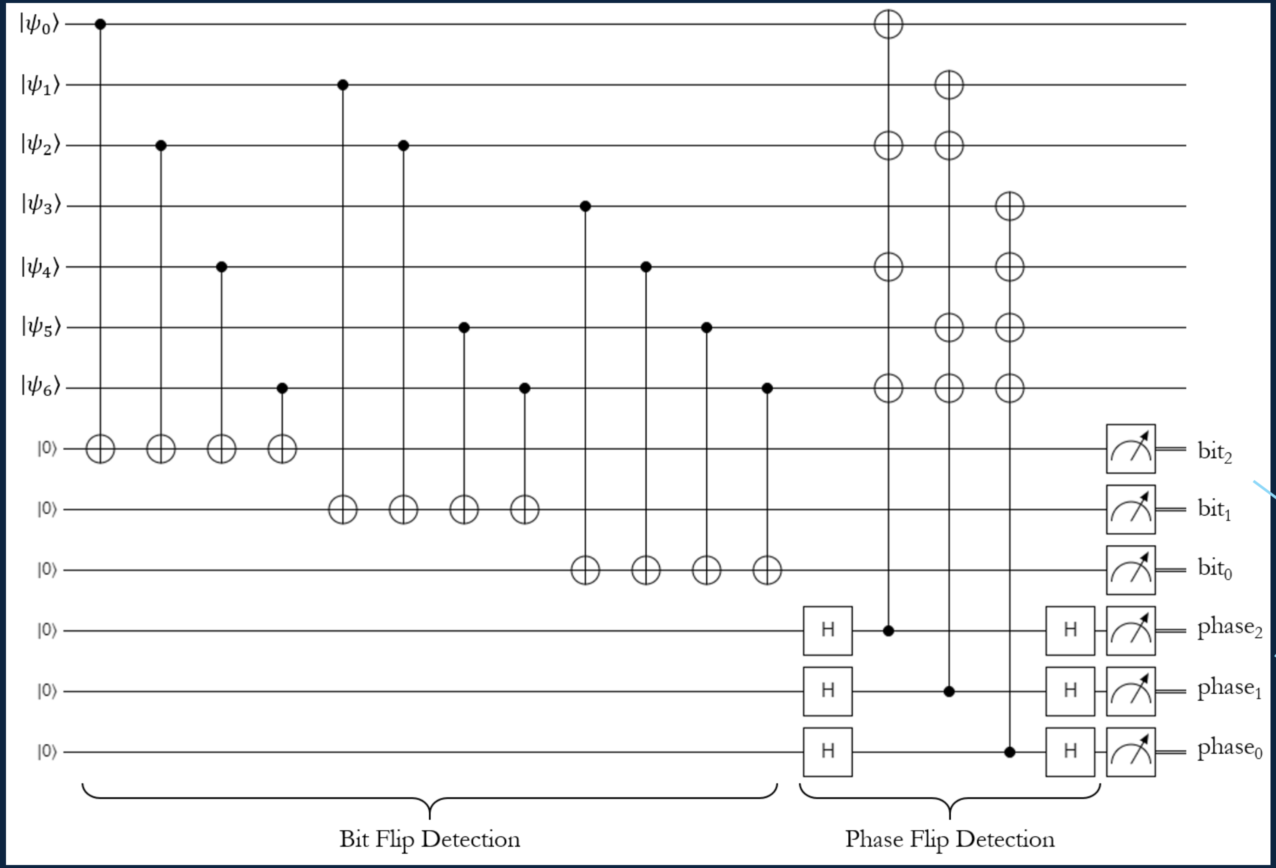


The Steane code uses 7 physical qubits to encode 1 logical qubit.

Encoding



Syndrome Measurement



little-endian

s	flipped
000	*None*
001	ψ_0
010	ψ_1
⋮	⋮
111	ψ_6

MITRE