Lecture 19, 5 Nov 2020

Can Eve do anything more?

$$|\varphi_\mu\rangle = \overset{0}{|0\rangle},\ \overset{1}{|1\rangle},\ \overset{2}{H|0\rangle},\ \overset{3}{H|1\rangle}$$

$$U|\varphi_\mu\rangle_1|\varphi\rangle_n = |\varphi_\mu\rangle_1|\psi_\mu\rangle_n$$

U preserves inner product

$$\langle\varphi_\nu|\varphi_\mu\rangle\underbrace{\langle\varphi|\varphi\rangle}_{=1} = \langle\varphi_\nu|\varphi_\mu\rangle\langle\psi_\nu|\psi_\mu\rangle$$

$\underline{\langle\varphi_\nu|\varphi_\mu\rangle \neq 0}$ for $\nu,\mu = \begin{matrix} 0 & 2 \\ 0 & 3 \\ 1 & 2 \\ 1 & 3 \end{matrix}$ $\quad |\psi_0\rangle = |\psi_2\rangle = |\psi_1\rangle = |\psi_3\rangle$

so can't obtain distinguishing info and leave state $|\varphi_\mu\rangle$ uncorrupted

What if Alice, Bob share an entangled $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?

still need random choice of H

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

---

doesn't buy an advantage:

once measured, equivalent to earlier protocol.

Only difference: QM makes choice of $|0\rangle, |1\rangle$ (or $H|0\rangle, H|1\rangle$)

(BB84) see also E91

Quantum Physics

[Submitted on 4 Nov 2020]

From Practice to Theory: The "Bright Illumination" Attack on Quantum Key Distribution Systems

Rotem Liss, Tal Mor

The "Bright Illumination" attack [Lydersen et al., Nat. Photon. 4, 686-689 (2010)] is a practical attack, fully implementable against quantum key distribution systems. In contrast to almost all developments in quantum information processing (for example, Shor's factorization algorithm, quantum teleportation, Bennett-Brassard (BB84) quantum key distribution, the "Photon-Number Splitting" attack, and many other examples), for which theory has been proposed decades before a proper implementation, the "Bright Illumination" attack preceded any sign or hint of a theoretical prediction. Here we explain how the "Reversed-Space" methodology of attacks, complementary to the notion of "quantum side-channel attacks" (which is analogous to a similar term in "classical" - namely, non-quantum - computer security), has missed the opportunity of predicting the "Bright Illumination" attack.

Comments:	17 pages
Subjects:	**Quantum Physics (quant-ph)**; Cryptography and Security (cs.CR)
Cite as:	arXiv:2011.02152 **[quant-ph]**
	(or arXiv:2011.02152v1 **[quant-ph]** for this version)

Submission history

From: Rotem Liss [view email]

[v1] Wed, 4 Nov 2020 06:50:26 UTC (16 KB)

Quantum Error Correction

Coupled to environment.

Classically: bit flips

Qubits can have infinitesimal changes

But if measured, lose the state.

How can state be

corrected without measuring it?

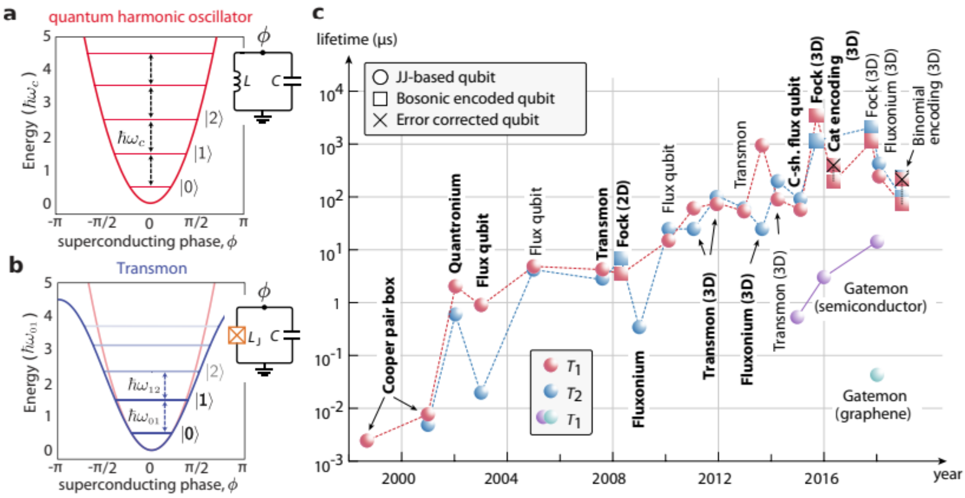


Figure 2

(a) The energy spectrum of a quantum harmonic oscillator (QHO). (b) The energy spectrum of the transmon qubit, showing how the introduction of the non-linear Josephson junction produces non-equidistant energy levels. (c) Evolution of lifetimes and coherence times in superconducting qubits. Bold font indicates the first demonstration of a given modality. ‘JJ-based qubits’ are qubits where the quantum information is encoded in the excitations of a superconducting circuit containing one or more Josephson junctions (see Sec. 2.1). ‘Bosonic encoded qubits’ are qubits where the quantum information is encoded in superpositions of multi-photon states in a QHO, and a Josephson junction circuit mediates qubit operation and readout (see Sec. 2.4). ‘Error corrected qubits’ represent qubit encodings in which a layer of active error-correction has been implemented to increase the encoded qubit lifetime. The charge qubit and transmon modalities are described in Sec. 2.1.1, flux qubit and the capacitively shunted flux qubit (‘C-sh. flux qubit’) are described in Sec. 2.1.2, and fluxonium and gatemon modalities are described in Sec. 5. The codes underlying the ‘cat encoding’ and ‘binomial encoding’ are discussed in Sec. 4.3. ‘(3D)’ indicates a qubit embedded in a three-dimensional cavity. For encoded qubits, the non-error-corrected T_1 and T_2 times used in this figure are for the encoded, but not error-corrected, version of the logical qubit (see Refs. (11) and (12) for details). The references for the JJ-based qubits are (in chronological order) (34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48); the semiconductor-JJ-based transmons (gatemons) are Refs. (49, 50, 51); and the graphene-JJ-based transmon is Ref. (52). The bosonic encoded qubits in chronological order are Refs. (53, 54, 11, 55, 12).

(from arXiv:1905.13641)

single qubit coherence

Table 1 State of the art high-fidelity two-qubit gates in superconducting qubits

Acronym[a]	Layout[b]	First demonstration [Year]	Highest fidelity [Year]	Gate time
CZ (ad.)	T–T	DiCarlo et al. (72) [2009]	99.4%† Barends et al. (3) [2014]	40 ns
			99.7%† Kjaergaard et al. (73) [2020]	60 ns
$\sqrt{\text{iSWAP}}$	T–T	Neeley et al. (81)$^\circ$ [2010]	90%* Dewes et al. (74) [2014]	31 ns
CR	F–F	Chow et al. (75) [2011]	99.1%† Sheldon et al. (5) [2016]	160 ns
$\sqrt{\text{bSWAP}}$	F–F	Poletto et al. (76) [2012]	86%* ibid.	800 ns
MAP	F–F	Chow et al. (77) [2013]	87.2%* ibid.	510 ns
CZ (ad.)	T–(T)–T	Chen et al. (56) [2014]	99.0%† ibid.	30 ns
RIP	3D F	Paik et al. (78) [2016]	98.5%† ibid.	413 ns
$\sqrt{\text{iSWAP}}$	F–(T)–F	McKay et al. (79) [2016]	98.2%† ibid.	183 ns
CZ (ad.)	T–F	Caldwell et al. (80) [2018]	99.2%† Hong et al. (6) [2019]	176 ns
CNOT_L	BEQ-BEQ	Rosenblum et al. (13) [2018]	~99%$^\square$ ibid.	190 ns
CNOT_{T-L}	BEQ-BEQ	Chou et al. (82) [2018]	79%* ibid.	4.6 µs

Gates ordered by year of first demonstration. Gate time is for the highest fidelity gate.

[a]Full names: CZ (ad.): Adiabatic controlled phase, $\sqrt{\text{iSWAP}}$: square-root of the iSWAP, CR: Cross-resonance, $\sqrt{\text{bSWAP}}$: Square-root of the Bell-Rabi SWAP, MAP: Microwave activated phase, RIP: Resonator induced phase gate, CNOT_L: Logical CNOT, CNOT_{T-L}: Teleported logical CNOT.

[b]F is short 'fixed frequency', T is short for 'tunable'. For all non-bosonic encoded qubit gates, the qubits were of the transmon variety (except for the first demonstration of $\sqrt{\text{iSWAP}}$, using phase qubits, and first demonstration of CR which used capacitively shunted flux qubits). Terms in parenthesis is a coupling element. '3D F' is short for a fixed frequency transmon qubit in a three-dimensional cavity. 'BEQ' is short for bosonic encoded qubit (see Sec. 2.4).

$^\circ$Implemented with phase qubits.

†Determined by interleaved randomized Clifford benchmarking (70).

$^\square$Determined by repeated application of the gate to various input states and observing state fidelity decay as function of applied gates. See (13) for details.

*Determined by quantum process tomography.

Gates implemented on flux-tunable qubits.

All-microwave gates.

Combination of tunable and fixed frequency components.

Gates on bosonic encoded qubits.

(from arXiv:1905.13641)

gate times

and fidelities

Classical

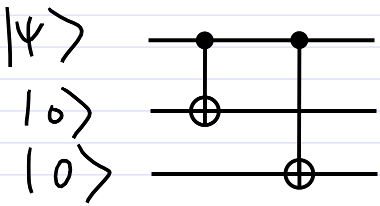
$$|\bar{0}\rangle = |0\rangle|0\rangle|0\rangle = |000\rangle$$

$$|\bar{1}\rangle = |1\rangle|1\rangle|1\rangle = |111\rangle$$

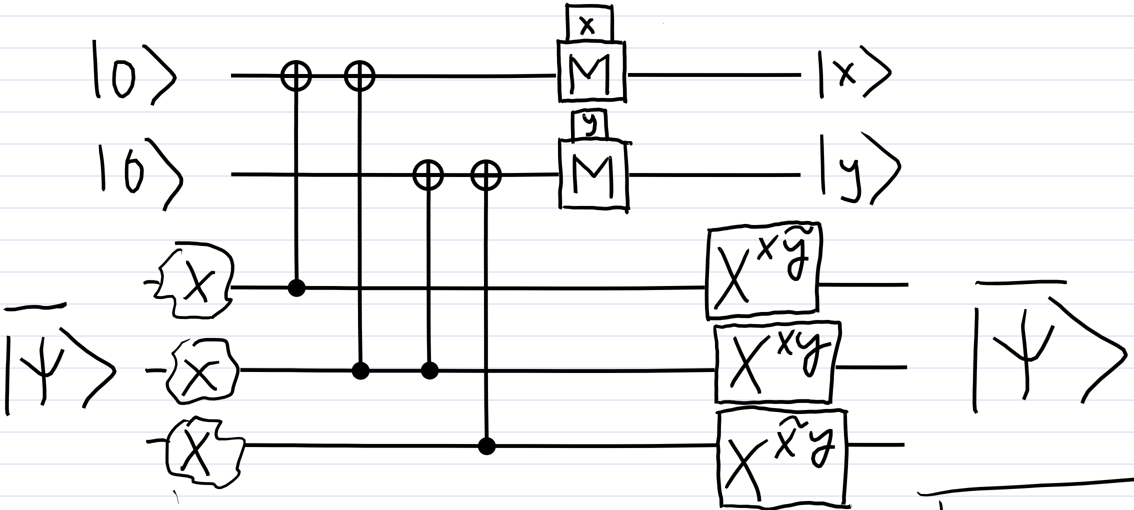
$|0\rangle|1\rangle|0\rangle$ $\quad \begin{matrix} |\bar{0}\rangle \\ |\bar{1}\rangle \end{matrix}$? majority rule

Quantum mechanical:

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



$$\alpha|000\rangle + \beta|111\rangle = |\bar{\psi}\rangle$$



restores state $|\bar{\psi}\rangle$

Learn nothing about α, β,

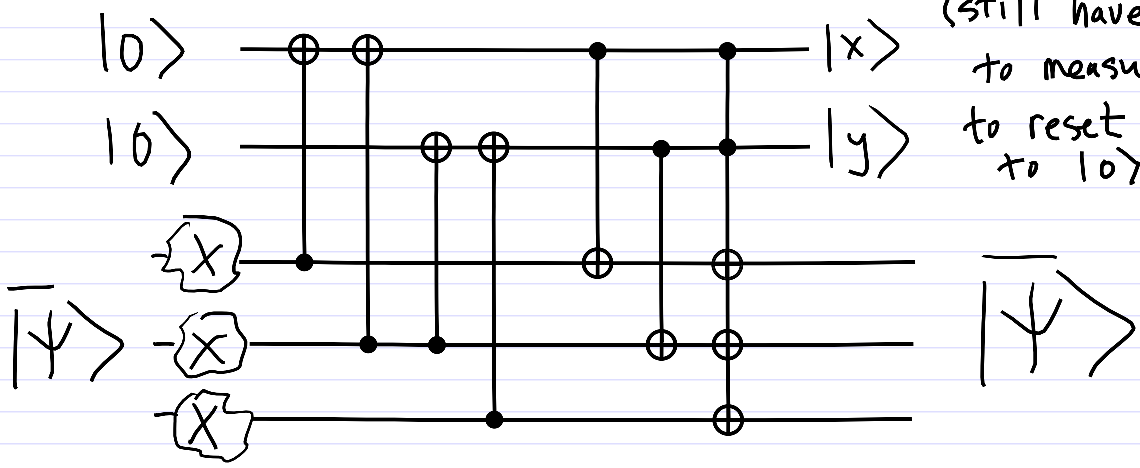
only relations within codewords

xy	
00	$\mathbb{1}$
10	X_2
01	X_0
11	X_1

$$2(3+1) = 2^3$$

$$2(n+1) \leq 2^n \quad n \geq 3$$

3 qubit codeword is minimum for correcting single bitflip error



(still have to measure to reset to $|0\rangle$)

For generalization, consider eigenvalues of $Z_1 Z_2$, $Z_0 Z_1$

Error	$Z_1 Z_2$	$Z_0 Z_1$
$\mathbb{1}$	1	1
X_2	-1	1
X_1	-1	-1
X_0	1	-1
	$(-1)^x$	$(-1)^y$

e.g. $(Z_0 Z_1) X_0 |\overline{\psi}\rangle = -X_0 (Z_0 Z_1) |\overline{\psi}\rangle = -X_0 |\overline{\psi}\rangle$

Model decohering effect of coupling to "environment" $|e\rangle$

$$|e\rangle|0\rangle \to \underline{|e_0\rangle|0\rangle} + |e_1\rangle|1\rangle$$

$$|e\rangle|1\rangle \to |e_2\rangle|0\rangle + \underline{|e_3\rangle|1\rangle}$$

$$\langle e_0|e_0\rangle \approx \underline{1} \approx \langle e_3|e_3\rangle$$

$$\langle e_1|e_1\rangle, \langle e_2|e_2\rangle \ll 1$$

$$|\psi\rangle \to e^{i\hat{n}\vec{\sigma}\frac{\theta}{2}}|\psi\rangle$$ (most general 1-qubit transformation)

$\left[\begin{matrix}\text{Small}\\ \theta\end{matrix}\right]$ $$e^{i\hat{n}\cdot\vec{\sigma}\frac{\theta}{2}} \approx (1-\theta^2/2)\underline{1} + i\hat{n}\cdot\vec{\sigma}\frac{\theta}{2}$$

$$\left[i n_j \frac{\theta}{2} = \varepsilon_j \quad j = x, y, z\right]$$

X = bit flip error
Z = phase-shift "
Y = combined "

$$\approx \underline{1} + \varepsilon_x \underline{X} + \varepsilon_y \underline{Y} + \varepsilon_z \underline{Z}$$

n qubit error-correcting code

$$|\psi\rangle \to \left(1 + \sum_j \left(\varepsilon_x^j X_j + \varepsilon_y^j Y_j + \varepsilon_z^j Z_j\right)\right)|\psi\rangle$$

(Any of single X, Y, Z error on any of n-qubits in codeword)

To have orthogonal subspaces to correct any of $3n+1$ errors, need

$$2(3\underset{\substack{\uparrow \\ X_i,\, Y_i,\, Z_i}}{n} + 1) \leq 2^n$$

i.e., $n \geq 5$

and there will be a minimal $n=5$ code that corrects all three types of error.