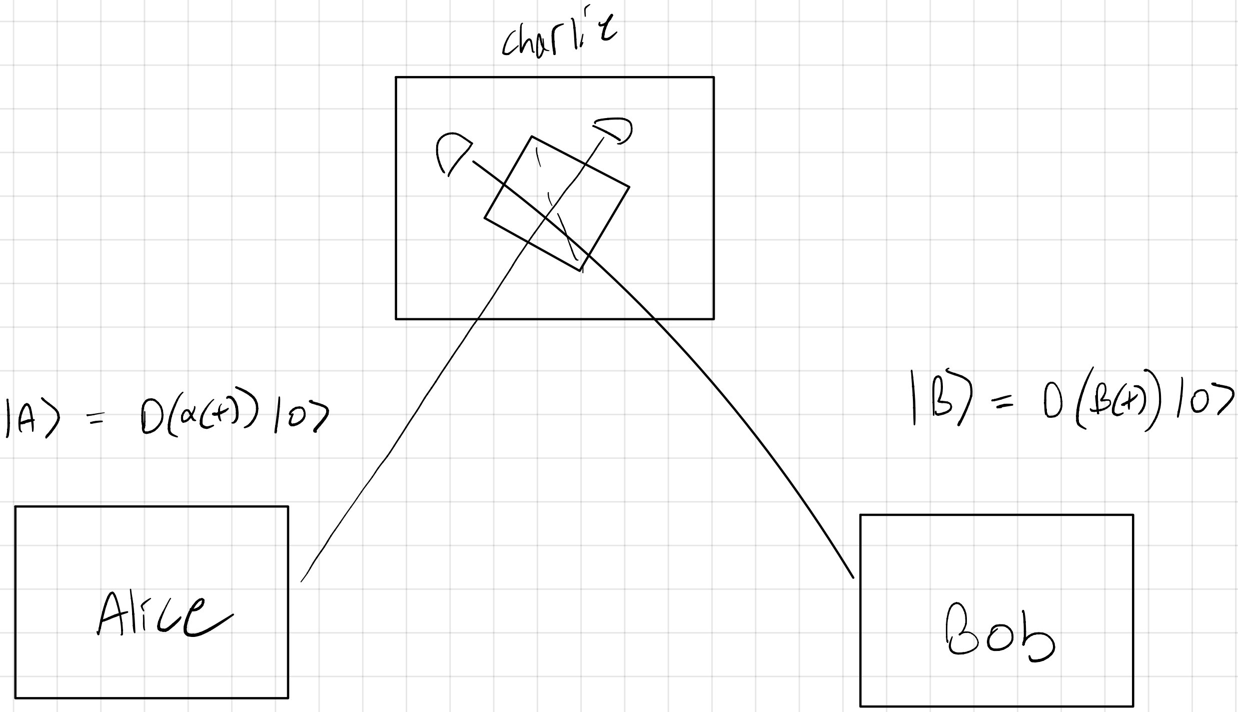
Optical ML with Quantum Networking



Encode qubits of duration Δt_s

Intersperse multi-symbol waveforms $\alpha(t)$ and $\beta(t)$
encoded on N symbols (samples)

↳ symbol duration $\Delta t_s / N$

Measurement Device Independent QKD

1) Preparation of entangled photon pairs. Charlie prepares a large number of entangled photon pairs and sends one photon from each pair to Alice / Bob over an insecure communication channel

2) Random Basis selection

   - Alice and Bob randomly choose one of 2 measurement bases, X or Z, in which to measure their photon

3) Measurement

   - Alice and Bob each measure their photon and record the results

4) Communication of measurement Basis

   - Alice and Bob publicly communicate their choice of measurement basis for each photon

5) Joint measurement

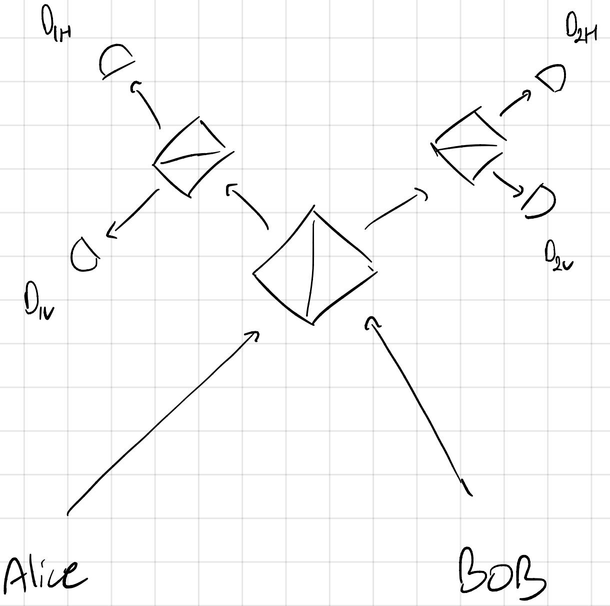
   - Charlie performs a joint measurement on the two photons using a Bell state analyzer. This generates a random bit which is announced

6) Key Generation

   - Alice and Bob use the publicly-announced bit to determine a subset of their measurement results that correspond to the same measurement basis, and use those results to generate a secret key

7) Privacy Amplification

   - Alice and Bob perform privacy amplification on their secret key to eliminate leaked information



1) Alice generates BB84 state : $|H\rangle\ |V\rangle\ \ |D\rangle\ |A\rangle$

   Bob generates BB84 state : $|H\rangle\ |V\rangle\ \ |D\rangle\ |A\rangle$

   Both send to charlie at the same time

2) Charlie announces resuts : $D_{1H}D_{2H}$, $D_{1H}D_{2V}$, $D_{1V}D_{2H}$, $D_{1V}D_{2V}$

3) Alice and Bob share basis choices securely : Rectilinear, Diagonal
   - Discard basis choice mismatches

4) $D_{1H}D_{2V}$ or $D_{1V}D_{2H} \mapsto |\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle - |VH\rangle\right)$

   $D_{1H}D_{2H}$ or $D_{1V}D_{2V} \mapsto |\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle + |VH\rangle\right)$

5) Either Alice or Bob perform bit flip based on Bell state

	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$
Rectilinear	Bit flip	Bit flip
Diagonal	Bit flip	—

6) Alice and Bob perform Error correction

7) Alice and Bob perform Privacy Amplification

Bell state analyzer by untrusted charlie

Alice/Bob frequency stabilized but not phase stabilized

Send to charlie a phase/amp modulated field and charlie reports results

↳ check Bell's inequality

New

connection of security to ML protocol

- Assured security of channel by sending qubits at random times

$t_s = 10$ ns

Gaussian envelope pulse that fits within 10 ns gap (channel security)

Amp modulated field with sample duration 1ns (10 samples in t_s)

$a_1, a_2, a_3, \ldots, a_{10}$

$b_1, b_2, b_3, \ldots, b_{10}$

detector 1 $\frac{a_1 + b_1}{\sqrt{2}}$ detector 2 $\frac{a_1 - b_1}{\sqrt{2}}$

Probability any of charlie's detector fire is $a \cdot b$

Look at photocurrent in homodyne receiver

MDI-QKD: Set Alice/Bob modulator in a slow way

↳ set qubit choice randomly

1 million pulses with laser - 10 ms total

100 million pulses with laser - 1 s total

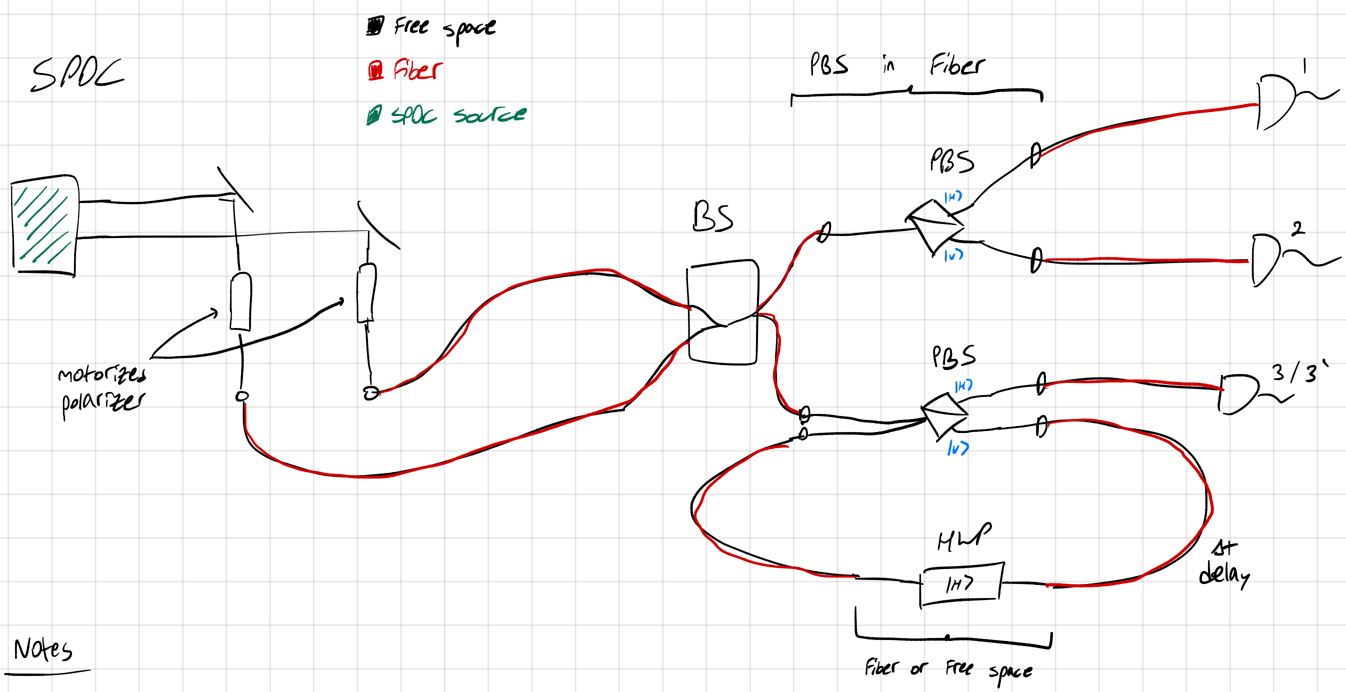
Apply hashing function to re-order

MDI-QKD

- can be done with <4 detectors

Entangled Bit Swapping

QuEd Thor Labs + Breadboard Quantenkoffer



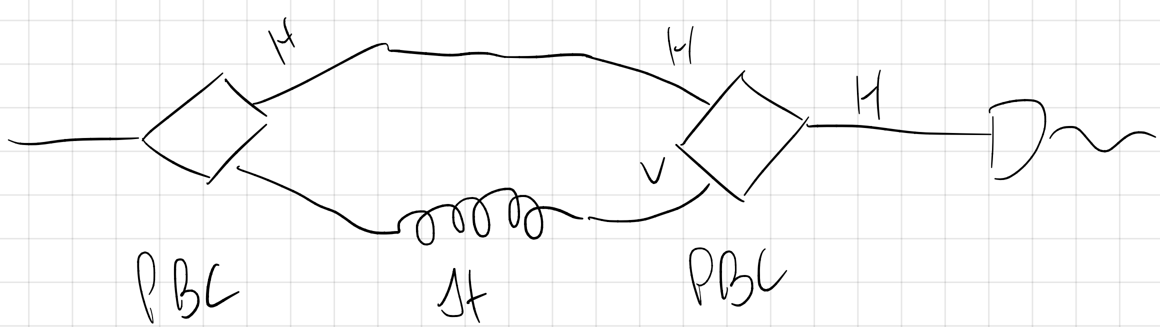
- Time delay setup
- only need a few time bins
- coincidence counts in time bins 0 and n

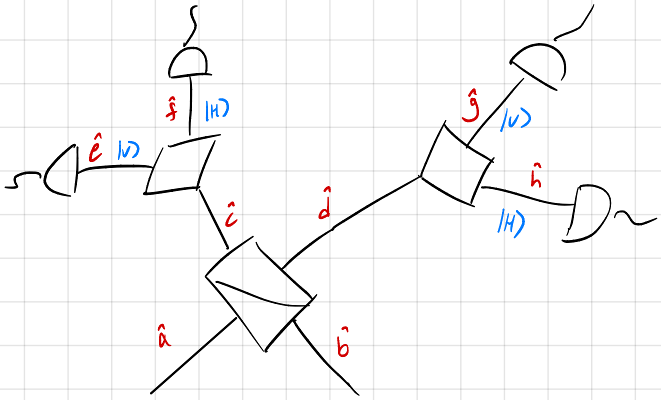
Pull counts/coincidences off Quantenkoffer

Time delay into detector so we need fine grained coincidence window

Notes

- Does not have to be SPDC source
  ↳ can be laser field split into two laser fields
- measurement here tells you the parody





$$n_e = \hat{e}^\dagger \hat{e} = \frac{(a_V - b_V)^2}{2}$$

$$n_f = \hat{f}^\dagger \hat{f} = \frac{(a_H - b_H)^2}{2}$$

$$n_g = \hat{g}^\dagger \hat{g} = \frac{(a_V + b_V)^2}{2}$$

$$n_h = \hat{h}^\dagger \hat{h} = \frac{(a_H + b_H)^2}{2}$$

$$\hat{c} = \frac{1}{\sqrt{2}}(\hat{a} - \hat{b}) \qquad \hat{e} = |V\rangle\langle V|\, \hat{c} \qquad \hat{g} = |V\rangle\langle V|\, \hat{d}$$

$$\hat{d} = \frac{1}{\sqrt{2}}(\hat{a} + \hat{b}) \qquad \hat{f} = |H\rangle\langle H|\, \hat{c} \qquad \hat{h} = |H\rangle\langle H|\, \hat{d}$$

$$\hat{a} = a_H|H\rangle + a_V|V\rangle$$

$$\hat{b} = b_H|H\rangle + b_V|V\rangle$$

$$\hat{c} = \frac{1}{\sqrt{2}}\left[(a_H - b_H)|H\rangle + (a_V - b_V)|V\rangle\right]$$

$$\hat{d} = \frac{1}{\sqrt{2}}\left[(a_H + b_H)|H\rangle + (a_V + b_V)|V\rangle\right]$$

$$\hat{e} = \frac{a_V - b_V}{\sqrt{2}}|V\rangle \qquad \hat{g} = \frac{a_V + b_V}{\sqrt{2}}|V\rangle$$

$$\hat{f} = \frac{a_H - b_H}{\sqrt{2}}|H\rangle \qquad \hat{h} = \frac{a_H + b_H}{\sqrt{2}}|H\rangle$$

$$\hat{e}^\dagger \hat{e} = \langle V|\left(\frac{a_V - b_V}{\sqrt{2}}\right)\left(\frac{a_V - b_V}{\sqrt{2}}\right)|V\rangle = \frac{(a_V - b_V)^2}{2}$$

$$\hat{f}^\dagger \hat{f} = \langle H|\left(\frac{a_H - b_H}{\sqrt{2}}\right)\left(\frac{a_H - b_H}{\sqrt{2}}\right)|H\rangle = \frac{(a_H - b_H)^2}{2}$$

$$\hat{g}^\dagger \hat{g} = \langle V|\left(\frac{a_V + b_V}{\sqrt{2}}\right)\left(\frac{a_V + b_V}{\sqrt{2}}\right)|V\rangle = \frac{(a_V + b_V)^2}{2}$$

$$\hat{h}^\dagger \hat{h} = \langle H|\left(\frac{a_H + b_H}{\sqrt{2}}\right)\left(\frac{a_H + b_H}{\sqrt{2}}\right)|H\rangle = \frac{(a_H + b_H)^2}{2}$$

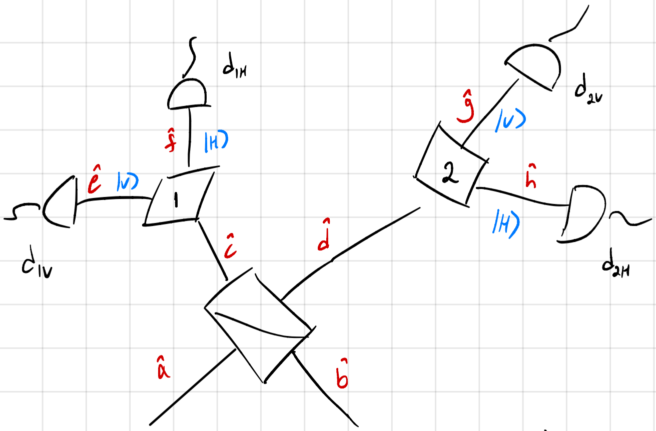
D_{1H}/D_{2V} or D_{1V}/D_{2H}

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

D_{1H}/D_{1V} or D_{2H}/D_{2V}

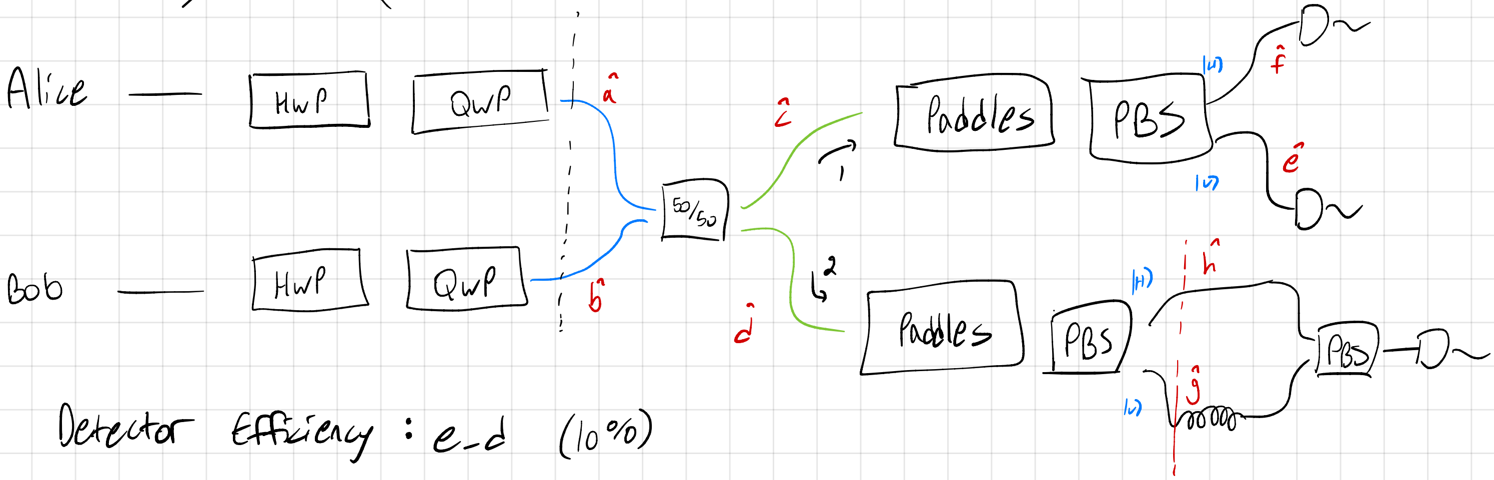
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Alice & Bob	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$
Rectilinear	Bit flip	Bit flip
Diagonal	Bit flip	—



ToDo

- Privacy Amplification – 94% (only sacrifice 6% of bits)
- Error correction



Detector Efficiency : e_d (10%)

PBS 1 : e_p1

PBS 2 : e_p2

50/50 BS : e_b

HWP A : e_ha

QWP A : e_qa

HWP B : e_hb

QWP B : e_qb

Fiber → Free space → Fiber : e_f 90% transmission

$|\psi_a\rangle = |H\rangle$

$|\psi_b\rangle = |H\rangle$

$$\hat{a} = \left[(e\_f)(e\_ha)(e\_qa)\right]\left[a_h|H\rangle + a_v|V\rangle\right]$$

$$\hat{b} = \left[(e\_f)(e\_h_b)(e\_q_b)\right]\left[b_H|H\rangle + b_v|V\rangle\right]$$

$$\hat{c} = (e\_b)\left[\frac{\hat{a} - \hat{b}}{\sqrt{2}}\right]$$

$$\hat{d} = (e\_b)\left[\frac{\hat{a} + \hat{b}}{\sqrt{2}}\right]$$

$$\hat{f} = (e\_p1)\ \hat{c}_h$$

$$\hat{e} = (e\_p1)\ \hat{c}_v$$

$$\hat{h} = (e\_p2)\ \hat{d}_h$$

$$\hat{f} = (e\_p2)\ \hat{d}_v$$

$$|\psi_a\rangle = |H\rangle$$

$$|\psi_b\rangle = |H\rangle$$

$$\hat{a}' = \left[(e_f)(e_{ha})(e_{ga})\right]\left[a_h|H\rangle + a_v|V\rangle\right]$$

$$\hat{b}' = \left[(e_f)(e_{h_b})(e_{g_b})\right]\left[b_H|H\rangle + b_v|V\rangle\right]$$

$$\hat{c}' = (e_b)\left[\frac{\hat{a} - \hat{b}}{\sqrt{2}}\right]$$

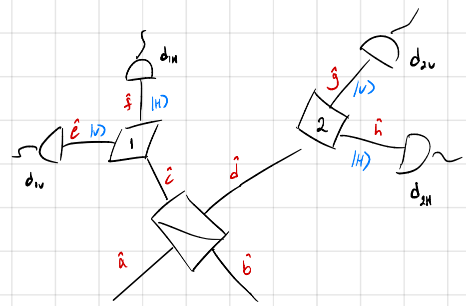
$$\hat{d}' = (e_b)\left[\frac{\hat{a} + \hat{b}}{\sqrt{2}}\right]$$

$$\hat{f}' = (e_{p1})\,\hat{c}_h \qquad \hat{h}' = (e_{p2})\,\hat{d}_h$$

$$\hat{e}' = (e_{p1})\,\hat{c}_v \qquad \hat{f}' = (e_{p2})\,\hat{d}_v$$

$$\hat{a}' = \left[\overbrace{(e_f)(e_{ha})(e_{ga})}^{a_e}\right]\hat{a}$$

$$\hat{b}' = \left[\underbrace{(e_f)(e_{hb})(e_{gb})}_{b_e}\right]\hat{b}$$



$$\hat{e} = \frac{a_v - b_v}{\sqrt{2}}|V\rangle \qquad \hat{g} = \frac{a_v + b_v}{\sqrt{2}}|V\rangle$$

$$\hat{f} = \frac{a_H - b_H}{\sqrt{2}}|H\rangle \qquad \hat{h} = \frac{a_H + b_H}{\sqrt{2}}|H\rangle$$

$$\hat{e}^+\hat{e} = \langle V|\left(\frac{a_v-b_v}{\sqrt{2}}\right)\left(\frac{a_v-b_v}{\sqrt{2}}\right)|V\rangle = \frac{(a_v-b_v)^2}{2}$$

$$\hat{f}^+\hat{f} = \langle H|\left(\frac{a_H-b_H}{\sqrt{2}}\right)\left(\frac{a_H-b_H}{\sqrt{2}}\right)|H\rangle = \frac{(a_H-b_H)^2}{2}$$

$$\hat{g}^+\hat{g} = \langle V|\left(\frac{a_v+b_v}{\sqrt{2}}\right)\left(\frac{a_v+b_v}{\sqrt{2}}\right)|V\rangle = \frac{(a_v+b_v)^2}{2}$$

$$\hat{h}^+\hat{h} = \langle H|\left(\frac{a_H+b_H}{\sqrt{2}}\right)\left(\frac{a_H+b_H}{\sqrt{2}}\right)|H\rangle = \frac{(a_H+b_H)^2}{2}$$

$$\hat{c} = \frac{(e_b)}{\sqrt{2}}\left[(a_e a_h - b_e b_h)|H\rangle + (a_e a_v - b_e b_v)|V\rangle\right]$$

$$\hat{d} = \frac{(e_b)}{\sqrt{2}}\left[(a_e a_h + b_e b_H)|H\rangle + (a_e a_v + b_e b_v)|V\rangle\right]$$

$$\hat{f} = \frac{\overbrace{(e_b)(e_{p1})}^{e_f}}{\sqrt{2}}\left(\overbrace{a_e a_h}^{a_h'} - \overbrace{b_e b_h}^{b_h'}\right)|H\rangle$$

$$\hat{e} = \frac{(e_b)(e_{p1})}{\sqrt{2}}(a_e a_v - b_e b_v)|V\rangle$$

$$\hat{h} = \frac{(e_b)(e_{p2})}{\sqrt{2}}(a_e a_h + b_e b_h)|H\rangle$$

$$\hat{g} = \frac{(e_b)(e_{p2})}{\sqrt{2}}(a_e a_v + b_e b_v)|V\rangle$$

$$N_f = \frac{(e_f)^2(a_h' - b_h')^2}{2} \qquad d_{1v} = (e_d)N_f$$

$$N_e = \frac{(e_e)^2(a_v' - b_v')^2}{2} \qquad d_{1H} = (e_d)N_e$$

$$N_h = \frac{(e_h)^2(a_h' + b_h')^2}{2} \qquad d_{2v} = (e_d)N_h$$

$$N_g = \frac{(e_g)^2(a_v' + b_v')^2}{2} \qquad d_{2H} = (e_d)N_g$$