High Fidelity to Low Weight

Daniel Gottesman

Perimeter Institute

A Word From Our Sponsor ...

Quant-ph/0212066, “Security of quantum key distribution with imperfect devices,”

D.G., H.-K. Lo, N. Lutkenhaus, J. Preskill

Revised

“v2 is even better than v1 ... longer, more general ... engrossing characters,” Q. Bitt, Quantum Daily News

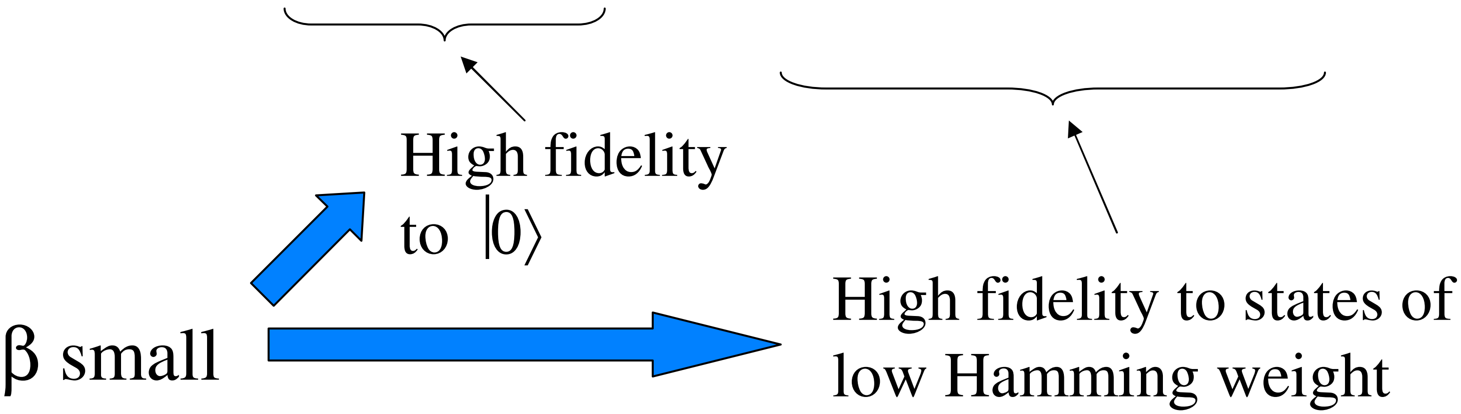
“If you only referee one paper this year, you should referee this one,” Anonymous

Different Kinds of Distance

Continuous: Fidelity, trace distance, L_p

Discrete: Hamming distance

When many repetitions, two types mix:



High fidelity to $|0\rangle$

β small

High fidelity to states of low Hamming weight

High Fidelity to Low Weight

This kind of state shows up often:

- Sampling test
- Incomplete test w/ only 1 passing state (e.g., quantum signatures, quant-ph/0105032, w/ I. Chuang)
- Small imperfections (e.g., QKD w/ imperfections, quant-ph/0212066)

Need to deal with superposition and entanglement, frequently involving basis change

A Useful Lemma

Definition: Let ρ be a state of N qubits, and let O be an operator acting on a qubit with two eigenvalues λ_0 and λ_1. Then $\mathrm{wt}_O\, \rho$ is a random variable produced by measuring O on each qubit of ρ and counting the number of λ_0 outcomes.

Lemma: Suppose we have a state ρ of N qubits, and $\mathrm{Prob}\ (\mathrm{wt}_X\, \rho > rN) = 0$. Then

$$\mathrm{Prob}\ (\,|N/2 - \mathrm{wt}_Z\, \rho| > sN) \leq 2^{-N[1-h(r)-h(1/2-s)] + o(N)}$$

$$h(x) = -\,x \log_2 x - (1-x) \log_2 (1-x)$$

Proof of Lemma

Counting argument:

X-basis

Z-basis

Purify ρ to

Quantum Key Distribution (BB84)

- Alice chooses random sequence of bits and bases
- Alice sends corresponding qubits to Bob
- Alice and Bob:
    - Compare bases
    - Discard bits where bases disagree
    - Compare bit values on a test subset (and discard)
    - Use an error-correcting code to fix remaining bits
    - Perform privacy amplification

Protocol aborts if error rate is too high on test bits (up to ~18% allowed)

Security of QKD

- Naturally occuring channel noise ⟶ error correction
- Eve can measure only a few bits but get lucky and remain undetected ⟶ privacy amplification (take parities of "raw" key bits)

Security proof idea:

Quantum error correction

⇕

Environment learns nothing about state

Classical EC ⟷ Bit flip error correction

Privacy amplification ⟷ Phase error correction

Security with Imperfections

- Alice and Bob only measure bit flip error rate

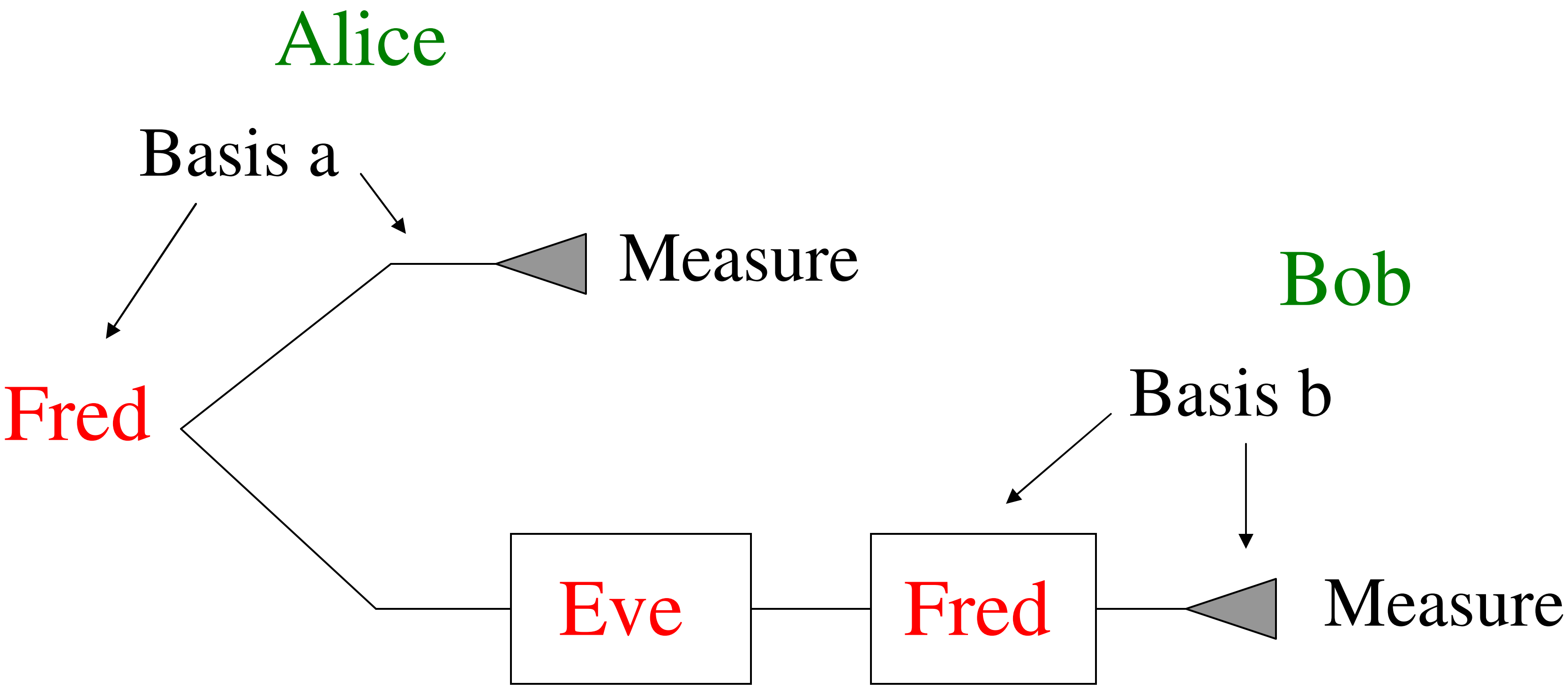
- In ideal protocol, complete symmetry between X and Z bases $\Rightarrow$ bit and phase error rates are the same

- If apparatus imperfect, symmetry between bases is broken $\Rightarrow$ bit and phase error rates can differ

- How much can they differ?

Treat by imagining Fred allied to Eve,
makes basis-dependent but weak attack

Alice, Bob, Eve, and Fred



Slight Basis Dependence

Alice and Bob flip coins to choose basis, and discard result if the coins differ.

Purify this:

$|0\rangle_{coin} \equiv$ Z basis for both Alice and Bob

$|1\rangle_{coin} \equiv$ X basis for both Alice and Bob

Ideal protocol: Coin state is $(|0\rangle_{coin} + |1\rangle_{coin})^N$.

Slight basis dependence: Coin is entangled with photons, but Prob $(\mathrm{wt}_X\ (\mathrm{coin}) < \Delta N)$ is very close to 1.

"Δ-balanced attack"

Examples of Δ-Balanced Attacks

- States with a small fraction of multiphoton states
- Misalignment of polarizers
- Small general individual imperfections in photon sources
- Small general individual imperfections in detectors

Note: Only Fred alters coin, not Eve

Applying the Lemma

“X_{lemma}” = X_{coin}

“Z_{lemma}” = $Z_{\text{coin}} \otimes (Z_A \otimes Z_B)$ or - $Z_{\text{coin}} \otimes (X_A \otimes X_B)$

When $Z_{\text{coin}} = 0$, $Z_A \otimes Z_B$ gives the bit flip error rate and when $Z_{\text{coin}} = 1$, $Z_A \otimes Z_B$ gives the phase error rate, and the reverse for $X_A \otimes X_B$.

Z_{lemma} tells us the balance between the bit flip and phase error rates (or, rather, the average of the 2 Z_{lemma}s):

- Eigenvalue -1 = only bit flip errors
- Eigenvalue +1 = only phase errors

By lemma, wt_Z is near N/2 $\Rightarrow$ # bit flips $\approx$ # phase errors

Summary

- Lemma shows a state which has small weight in X basis has weight near 1/2 in Z basis

- Useful applications for lemma in cryptography

- QKD remains secure with small imperfections of various types, with quantifiable allowed error rates

Open Questions

- Does following a Δ-balanced attack with another Δ-balanced attack produce an attack that is still (poly(Δ))-balanced?

- Tighten bounds in lemma (in particular, allow probability $\rightarrow 0$ with smaller s)

- Extend lemma to more general pairs of operators and higher-dimensional Hilbert spaces