Why Quantum Cryptography Can't Work

Steve Meyer - Pragmatic C Software Corp.

(Assistance from Minnesota Center for Philosophy of Science. Also John Bell and Arthur Fine)

I. **Important because if Quantum Computers (QMC) built, current public key algorithms broken. Also many proposals for cryptographic protocols tied to QM.**

II. **QMCs Pseudo Science Like 90's Cold Fusion.**
Every step uncorroborated but accepted for psychological reasons:
   a. **Aging Feynman desire for place in history.**
   b. **CS theoreticians lack of P=NP progress.**
   c. **"Neatness" of QM.**
   d. **Authoritative Von Neuman's 1931 QM must be probabilistic proof.**
   e. **Failure to distinguish mathematical assumptions from scientific experiments.**
   f. **Opportunistic experimental physicists claims of imminent success.**
   g. **Science backward - modern discrete computation methods should be used to improve QM.**
   h. **Story of result of CS research establishment eliminating skeptics.**

III. Other Types of Molecular/Membrane Computers do not Compute Anything

a. **Computer: input chemicals, reaction runs, read out results.**

b. **Only three possibilities all analog computers:**
   1. **Human pre-computation - answer is assigned binary property of reaction.**
   2. **Answer read out time exponential (hard)**
   3. **Analog computer - compute minimum surface of bubble solution.**

IV. Definition of Quantum Computer (QMC)

a. **QMC is normal turning machine with time P (1) bounded oracle subroutine**
b. **Oracle input vector of Qbits - probably +1/-1 particle spin**
c. **Qbit vector in 2ˆn states simultaneously - superposition is all bases of linear vector space stored in "atom"**
d. **Operation is transform function f: {0, 1}ˆn -> {0, 1} for all points simultaneously such as Fourier transform**
e. **Read out involves QM measure usually after amplitude increasing transforms.**

V. Even Mathematical Foundation of QMCs Physically Uncorroborated

a. **Based on Von Neuman's problematic proof of necessary probabilistic nature of QM.**
b. **Assumes results from HEP - different dimensions - phenomenological problem of bubble chamber track interpretation.**
c. **Assumes Quantum states only linear combinations.**
d. **QM only corroborated inside atom.**
e. **Leap of faith from atomic physics to QM information theory.**

f. Bohm 50s other worlds domain of measurement criticism of QM applies to QMC.

g. Sociological pattern of monster barring - ignoring anomalies in QM.

h. Circularity of mathematic logic and QM logic.

i. Ignore quasi-experimental nature of mathematical assumptions.

j. Pickering's criticism of physics as "phenomenology". Need to belief physical theory to see bubble chamber tracks applies.

VI. Physical Realizability of QMC Unrelated to CS QMC Algorithms.

a. **Builders of Qbits make leap of faith back to atomic chemistry.**
b. **QMC developers seem to be looking for new type of conventional computer logic gate such as one electron switch.**
c. **Need simplifying assumptions: only one Qbit switches at a time. no averaging of states, need wave cancellation on average, etc.**
d. **Cryptography would say the averaging removes any computation.**
e. **What is needed is to apply "code breaking" mathematical analysis to calculations predicting feasibility of physical QMC.**
f. **QMC experimental approximations remove "oracle" properties of Qbit vector - ability to store 2**n "bits" in n bit Qbit vector.**

VII. Quantum Cryptography

a. **Additional ability to physically send single Qbits needed for QM bit commitment protocols.**
b. **Quantum teleportation.**
c. **Consequence of QMC is that 2*n "bit" capacity communication channel only need n Qbit capacity.**
d. **Conjecture: even for QMCs, CO-NP problems exist that can not be solved in polynomial time.**
e. **Complexity Theory empty because not tied to physical world view.**