Cryptography, CS, and Quantum Computing Research Programme Testing

1. Introduction

Here are the transparencies from my Eurocrypt 2003 rump session talk. I offered to post these transparencies because due to lack of time, I was not able to show the last few slides containing quotations sceptical of quantum computation (QC) from founders of quantum physics (QP - name quantum physics is used here instead of quantum mechanics). After end of slides, abstract of talk and annotated bibliography that provides citation references have been added.

The idea behind the talk is that QC and cryptography are closely related, each can be used to scientifically test the other. Since non existence proofs are impossible in science because in the future some new theory may be discovered, instead of using arguments, talk uses statements made by the founders of QP to advocate the sceptical view toward quantum computation research programme.

It happened that there was a conference also held in Warsaw back in 1938 on "New Theories in Physics" that discussed computational aspects of QP - specifically the "Bohr Interpretation". Therefore, whenever possible, quotations from that conference were used.

I believe study of quantum computation will lead to significant scientific progress in computer science (CS), physics, and cryptography.

2. Background Explanation

Here are explanations of the background knowledge assumed for this talk:

1. **Lakatos concepts of research programme and mathematical formalism**
   The term "research programme" refers to a theory by philosopher Irme Lakatos who taught at LSE after leaving Hungary in the mid 1950s for Britain (See Lakatos entries in bibliography section at end). I used the language and hypotheses of that theory because it allows discussing QC as a scientific theory rather than as an engineering race. Implicit in this talk is idea that one can provisionally judge a theory as degenerating or low probability and make decisions based on that judgment.

   In addition, Lakatos' thesis was on formal versus informal mathematics (see *Proofs and Refutations* reference at end) in which he showed that historically "proof" meant "thought experiment". His theory is particularly relevant to QC because QC involves mathematics of vector fields and Lakatos thesis examples came from analysis area rather than foundations or logic.

2. **Idea behind definition of CS and cryptography as vectors on page 6**
   Transparency on page 6 formulates the question of the nature of CS and cryptography (Crypto) in terms of conceptual vectors, i.e. are CS and Crypto mathematics as Knuth claims, Physics as Bohr claimed or something in between. Professor Stern's excellent invited lecture presented at Eurocrypt 2003 (proceedings p. 449-461) addresses this problem in area of Crypto protocols and

definitions of security Another aspect of conceptual framework of my talk is belief that Crypto and CS must in some way be tied to physical reality.

3. **Explanation of Verilog UDP transparency as irregular vector field example**
Transparency on page 13 shows a modern example of an irregular vector field like mathematical object that only makes sense for our modern age in which computers extend our computational ability. It is intended to show a modern example of the Detouches/Fervier idea and development of alternatives to formalization of quantum physics in terms of Hilbert vector spaces. I did not have time to discuss this during talk, but the example is a tabular description (called a user defined primitive or UDP) describing a D style flip flop (timed electronic device) from the Verilog Hardware Description Language. It is interesting for number of reasons:

    1. UDP table describes a finite vector field (or field like object) that is so irregular that it requires a computer to calculate various operations. The previous state column and the edge column dimensions require different vector component evaluation rules.
    2. New field values are computed by vector (like?) operations and make use of linear superposition property of object just as QC operations depend on linear superposition.
    3. One traditional aspect of QC is retention of concept of gates that are implemented as quantum gates operating on Qbits, but this example shows that there may be other alternatives to QC that do not require gates such as QC as composition operations on finite fields of switching devices.

4. **Terman versus Polya/Bloch CS research organization item at end of abstract**
There was a change at Stanford University that occurred just after end of careers of founders of QP such as George Polya (Von Neumann's professor), Felix Bloch, Linus Pauling, and William Shockley that is relevant to current wide spread belief in high probability of engineering success of QC. In spite of anti-formalist conviction of founders of QP at Stanford, the current formalist view was adopted without any scientific debate.

    Visible manifestation of this conceptual change can be seen by contrasting the Stanford AI Lab in the 1970s at which public key Crypto was developed versus Stanford Linear Accelerator (SLAC) at which much of the entanglement theory and early CS were developed.

    Conceptual change to CS/Crypto/QC as engineering instead of science also manifested itself back in the 1970s again without any debate in take over by EECS department of UC Berkeley CS department at which NP completeness and Merkle part of public key Crypto were discovered. L&S CS department had been closely related to math and physics departments.

    I believe as long as CS, Crypto, and QC are studied as engineering problems rather than as scientific theories, scientific progress will be severely impaired.

Talk does not explicitly address this issue but I believe there is no other way to interpret the quotations.

5. **Citation for Bohr Quotation in original talk was wrong.**
   Source for the Bohr quotation on formalism (page 5) given during talk was incorrect. Actual source is lecture given on same visit to New York in 1954 but at New York University not Columbia. Lecture title is "Mathematics and Natural Philosophy" not "Unity of Knowledge".

Here are the transparencies ...

Cryptography, CS, and Quantum Computing Research Program Testing

Steve Meyer - Pragmatic C Software Corp.
(Assistance from Minnesota Center for Philosophy of Science)
(Also Bohr Institute Archive and AHQP Collection)

I. **Imagine viewing quantum computation (QC) as an on going scientific research programme instead of just an engineering race to build a computer so fast limitations of NP completeness do not apply.**

II. **I am suggesting trying to use the multi-dimensional thinking that Niels Bohr used in discovering the Bohr interpretation of QP.**

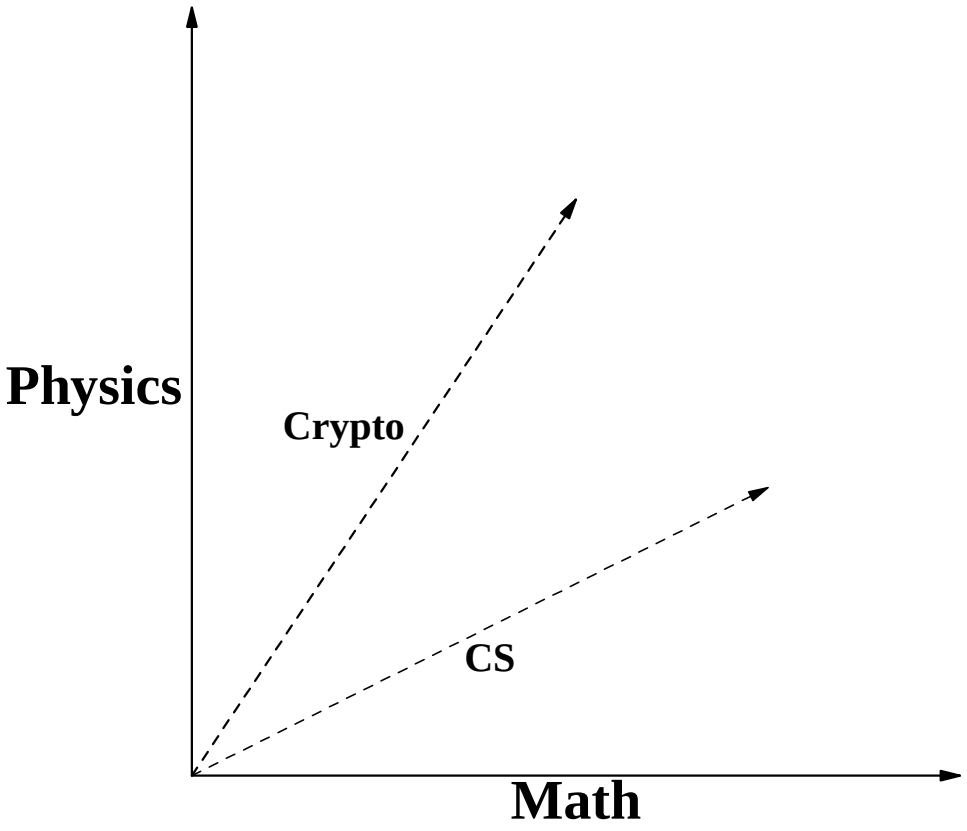
III. **Therefore, there are methodological opportunities presented by quantum computing research programme for better understanding the conceptual nature of cryptography and Computer Science (CS).**

IV. **If the possibility of physical realization of quantum computation is viewed in wider context as a research programme, studying QC can help determine the nature of CS and Crypto.**

V. Amazingly, discussions at the 1938 Warsaw conference on "New Theories in Physics" sponsored by the International Institute of Intellectual Co-operation reach forward through time to address QC question. Announced topic of conference was discussion of Bohr atom versus mathematical formalization of QP.

VI. I am taking the sceptics side of the QC debate and believe the discussions at that 1938 conference can be used for scientific and/or mathematical testing of the QC research programme.

VII. In addition, I am suggesting widening our thinking to see cryptography and theoretical CS as both testing and being tested by QC research programme.


Physics
Crypto
CS
Math

Bohr Anti-Formalist View

The general lesson of the role that mathematics has played through the ages in natural philosophy is the recognition that no relationship can be defined without a logical frame and that any apparent disharmony in the description of experience can be eliminated only by an appropriate widening of the conceptual framework. This lesson, familiar to mathematicians, and conspicuous in studies in the foundations of their science, has been enforced by the development of physics in a way that a bearing on many other fields of human knowledge and interest in which we met with similar situations in the analysis and synthesis of experience.

Source 1954 New York University Lecture "Mathematics and Natural Philosophy".

Knuth Formalist View

Like mathematics, computer science will be somewhat different from the other sciences, in that it deals with artificial laws that can be proved, instead of natural laws that are never known with certainty.

Quoted in book "Quantum Computation and Quantum Information", by M. Nielsen and I. Chang, p. 171.

Need for Observer

The Polish president of the Union Prof. C. Bialobrzeski brought up the approximation problem (p. 7). Namely, that first approximations and simplified systems give generally satisfying results but "if we wish to make more exact calculations everything is spoilt and the theory is unusable."

Problem is relevant to mathematical consequences of entangling large number of Qbits. Analysis of this problem is very much like the code breaking part of cryptography.

Another relevant issue raised by Bialobrzeksi at conference is that behavior which shows clearly

when particles are free is almost entirely lost when particles are part of chemical atoms.

From "New Theories in Physics" discussion.

Need for Observer and Problem with Statistical Analysis

Von Neumann himself (p. 44) brought up the problem that the mathematics of QP always requires an observer in the system.

If we wish to analyse the meaning of the statistical statements of quantum physics, we must necessarily deal with "ensembles" of a great number of identical systems, and not with individual systems. Even by discussing such ensembles only, it must be possible to decide, whether a given statistical theory - in this case quantum physics - can be based on a causal one or not.

From "New Theories in Physics" discussion.

A QC that requires say a human optical system as part of the "computer" will not be useful no matter how fast. For second quote, ensembles imply problem with isolated QC system.

Alternative Logic of QP

A student of French attendee M. Detouches named Mlle. Fervier had devised a different logic of QP for which inner products and therefore quantum entanglement does not exist.

From "New Theories in Physics" discussion.

Cryptography uses many alternative and finite (or rational) fields. Computers allow irregular and fine grained fields to be computed. Seen from another viewpoint, mathematics of physics can, perhaps, be used as source of cryptographic methods such as one way functions.

Verilog UDP: Irregular Computer Operation Finite Field

```
primitive udp_dff (out, in, clk, clr_, set_);
   output out;
   input in, clk, clr_, set_;
   reg out;

   table
//in clk clr_ set_ : Qt : Qt+1
  0   r   ?    1   : ?  :  0; // clock in 0
  1   r   1    ?   : ?  :  1; // clock in 1
  1   *   1    ?   : 1  :  1; // reduce pessimism
  0   *   ?    1   : 0  :  0; // reduce pessimism
  ? (10)  ?    ?   : ?  :  -; // no chg on negedge
  *   b   ?    ?   : ?  :  -; // no chg on in switch
  ?   ?   ?    0   : ?  :  1; // set output
  ?   b   1    *   : 1  :  1; // cover all set_ chg
  1   x   1    *   : 1  :  1; // cover all set_ chg
  ?   ?   0    1   : ?  :  0; // reset output
  ?   b   *    1   : 0  :  0; // all clr_
  0   x   *    1   : 0  :  0; // cover all clr_ chg
   endtable
endprimitive
```

Vector Fields Mapping:

clk=0; (in, clk, clr_, set_, Qt) => (new clk, Qt, Qt+1)
clk=1: (in, clk, clr_, set_, Qt) => (new clk, Qt, Qt+1)
clk=x: (in, clk, clr_, set_, Qt) => (new clk, Qt, Qt+1)

Professor Kramer's Criticism of Formalism

Professor Kramers thought that there was a difference between essentially mathematical and an essentially physical attitude. The mathematical attitude tried to scheme out, to simplify and to abstract in order to find out which were the logical elements in the processes of calculation. That was what the President had done. But professor Bohr still thought like an obstinate physicist.

From New Theories in Physics, p. 98.

Felix Bloch's "Proof" QCs can not be Built - Relating What Bohr Said:

The dilemma in quantum mechanics is this: that all observations in quantum mechanics are essentially classical. That is to say, he said that the only way we can make contact with reality is through classical experiments.

From Kuhn's AHQP interview of Felix Bloch, p. 35.

Next page is abstract submitted to Rump Session committee ...

Cryptography, CS, and Quantum Computing Research Programme Testing

Steve Meyer
Pragmatic C Software Corp.
520 Marquette Ave., Suite 900
Minneapolis, MN 55402
Email: sjmeyer@pragmatic-c.com

Abstract:

Talk discusses methodological opportunities presented by quantum computing (QC) research programme for better understanding the conceptual nature of cryptography and computer science (CS). A graph showing mathematics along one axis and physics along another perpendicular axis will be shown. Both CS and Crypto can be view as vectors between the two orthogonal axes. If the possibility of physical realization of quantum computation (QC) is viewed in wider context as a research programme, studying QC can help determine the nature of CS and Crypto. This will be explained by discussing quotations from the 1938 Warsaw conference on **New Theories in Physics.**

The two sides of the question can be best seen by representative quotations. Niels Bohr stated the anti-formalist view in his 1954 Columbia University lecture "The Unity of Knowledge" last paragraph: *(sic. title was wrong - "Mathematics and Natural Philosophy" is correct title)*

> *The general lesson of the role that mathematics has played through the ages in natural philosophy is the recognition that no relationship can be defined without a logical frame and that any apparent disharmony in the description of experience can be eliminated only by an appropriate widening of the conceptual framework. This lesson, familiar to mathematicians, and conspicuous in studies in the foundations of their science, has been enforced by the development of physics in a way that a bearing on many other fields of human knowledge and interest in which we met with similar situations in the analysis and synthesis of experience.*

In book by M. Nielsen and I. Chang "Quantum Computation and Quantum Information", p. 171, Donald Knuth states the formalist view:

> *Like mathematics, computer science will be somewhat different from the other sciences, in that it deals with artificial laws that can be proved, instead of natural laws that are never known with certainty.*

Topic is appropriate for conference in Warsaw because during development of quantum physics (QP) in 1938, a conference also in Warsaw sponsored by the International Institute of Intellectual Co-operation on **New Theories in Physics** met to discuss the Bohr interpretation in context of Von Neumann's 1931 book that axiomatized QP using Hilbert vector spaces. I am taking the sceptics side of the QC debate and believe the discussions at that 1938 conference can be used for scientific and/or mathematical testing of the QC research programme.

The conference discussion ended up defending the Bohr interpretation and criticizing the axiomatization of physics. During the conference, the following areas were discussed relevant to QC research program and cryptography. More relevant quotations from the conference will be shown time permitting.

1. A student of French attendee M. Detouches named Mlle. Fervier had devised a different logic of QP for which inner products and therefore quantum entanglement does not exist. Cryptography uses many alternative and finite (or rational) fields. Computers allow irregular and fine grained fields to be computed. Seen from another viewpoint, mathematics of physics can, perhaps, be used as source of cryptographic methods such as one way functions.
2. Von Neumann himself (proceedings p. 44) brought up the problem that the mathematics of QP always requires an observer in the system. A QC that requires say a human optical system as part of the "computer" will not be useful no matter how fast.
3. The Polish president of the Union Prof. C. Bialobrzeski brought up the approximation problem (p. 7). Namely, that first approximations and simplified systems give generally satisfying results but "if we wish to make more exact calculations everything is spoilt and the theory is unusable." Problem is relevant to mathematical consequences of entangling large number of Qbits. Analysis of this problem is very much like the code breaking part of cryptography.
4. Another relevant issue raised at conference is that behavior which shows clearly when particles are free is almost entirely lost when particles are parts of chemical atoms.

The talk concludes with a discussion of competing scientific research programs on the nature of CS and Cryptography at Stanford in the 1970s when public key cryptography was discovered. The sceptical view of formalist CS and therefore of QC research programme was advocated at SLAC by Felix Bloch and George Polya and Wolfgang Panofsky among others while the formalist view was advocated by engineering dean Terman and the Stanford CS and AI Lab professors.

3. Annotated References from the QC Sceptical Side

3.1 Quantum Physics

1. Bohm, D., A Suggested Interpretation of the Quantum Theory in Terms of 'Hidden' Variables, I and II, *Physical Review 85: 166-193,* 1952.

   Bohm style hidden variables probably do not offer much help in testing QC because they are aimed at solving causality problems from 19th century physics relating to thermodynamics. It was thought in the 19th century that thermodynamics was inherently probabilistic, but thermodynamics was later re-formulated in purely causal terms using "new" variables. Bohm's hidden variables attempted to similarly re-formulate QP.

2. International Union of Physics and Polish Intellectual Co-operation Committee. *New Theories in Physics.* Proceeding of Conference held May 30 - June 3rd 1938 in Warsaw Poland. International Institute of Intellectual Co-operations, Paris, 1939.

   This is reference for source of quotations used in talk.

3. Wheeler, J., and Wojciech, H. (ed.). *Quantum Theory and Measurement.* Princeton University Press, 1983.

   This is by far best source for original QP papers because not only are the original EPR and Bell papers reprinted but discussions of the papers and replies are also reprinted.

3.2 Quantum Computation

1. Berman, L., et al., *Introduction to Quantum Computers.* World Scientific Publishing, Singapore, 1998.

   A good less technical introduction to QC.

2. Cristian, S. and Paun, G. *Computing with Cells and Atoms.* Taylor and Francis, London, 2001.

   Another good less technical introduction to QC.

3. DiVincenzo, D. Quantum Computation. *Science 270:255-261,* 1995.

   Interesting early paper on difficulties in solving the QC engineering problem. If QC is possible, it should be possible to construct an exponentially fast quantum

computer using the simple up/down spin inversion system using magnetic pulses discussed in this paper.

4. Grover, L. Rapid Sampling Through Quantum Computing. 32th Annual ACM Symposium on Theory of Computing (STOC), 618-626, 2000.

   This and Shor paper give basic exponential QC algorithms. Question from sceptical side is whether algorithm is just elaboration of mathematical axioms or if algorithm connects to physical reality.

5. Nielsen, M. and Chuang, I. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

   This is most comprehensive book on QC but it seems to have same problems as books that advocated logical positivism. Namely, it assumes the phenomenon. Book contains comprehensive bibliography through 2000.

6. Shor, P. Algorithms for Quantum Computation: Discrete Log and Factoring. *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science (FOCS),* Santa Fe, New Mexico, IEEE Computer Society Press, Los Alamitos, CA, 124-134, 1994.

   This and Grover paper give basic exponential QC algorithms. See Grover paper note.

3.3 Computer Science

1. DeMillo, R., Lipton, R., and Perlis, A. Social Processes and Proofs of Theorems and Programs, *Communications of the ACM 22:271-280,* 1970.

   This paper unfortunately had the effect of stopping debate on the nature of CS and also had the effect of ending publication of papers that were sceptical of formalist CS. It established the principle that truth in CS is what is determined by social interaction of whichever community is in power at a given time. Therefore, any disproof of QC research programme must address social beliefs and conventions of CS community in addition to providing objective disproof.

2. Kugel, P. Digital to Analog Conversion (a speculation). *SIGACT News April-June:27-33,* 1976.

   This early speculative paper addresses two possible problems with the assumptions underlying QC. First, what are the theoretical capabilities and limitations of analog computers, and second, are there alternatives to the Church-Turing thesis?

3. Stern, J. Why Provable Security Matters. *Advances in cryptology - EUROCRYPT'2003 Proceedings.* 449-461.

Interesting invited lecture given at this year's Eurocrypt that shows axiomatic mathematics will still be important in cryptography even if exponentially fast quantum computers are built.

3.4 Natural Philosophy and Methodology

1. Bohr, Niels. (Kalckar J. Ed.) *Niels Bohr Collected Works, Volume 7 Foundations of Quantum Physics II (1933-1958).* Elsevier, Amsterdam, 1996.

Book contains interesting discussion of Bohr's reaction to discussions during 1938 Warsaw conference (pp. 260-263).

2. Bohr, Niels. (Sanders J. Ed.) *Essays and Papers.* Volumes 1 and 2. Unpublished, 1987.

Book is a two volume collection of Bohr's philosophical writing (Bohr was part of European system in which physics was studied as natural philosophy). The 1954 New York University lecture "Mathematics and Natural Philosophy" in which Bohr gave his view of role of mathematics in physics appears on page 550 of Volume 2.

3. Feyerabend, P. *Problems of Empiricism: Philosophical Papers, Volume 2.* Cambridge, 1981.

Feyerabend and Lakatos both devoted their careers to establishing objective criteria for determining value of research programs. They also both studied and wrote extensively on the intellectual standing of QP.

4. Kuhn, T., et al. (ed.) *Sources for the History of Quantum Physics. (usually abbreviated AHQP),* Microfilm archive, 1967.

Archive contains comprehensive collection of original manuscripts and letters during development of QP on microfilm. It also contains transcripts of interviews with the founders of QP who were still alive in the early 1960s. The interview with Felix Bloch probably provides the most opportunities for developing the sceptical view of QC.

5. Kuhn, T. S. *The Structure of Scientific Revolutions.* Princeton University Press, 1962.

Theory of scientific theory testing from historian who was responsible for AHQP archive. Book was written after Kuhn interviewed founders of QP and compiled extensive microfilm archive so it may offer source of experiments for testing QC.

6. Lakatos, I. *Proofs and Refutations, The Logic of Mathematical Discovery.* Cambridge University Press, 1976.

   This is Lakatos' very popular thesis that is relevant to QC because it showed that mathematical proofs outside of logic area are "thought experiments". It was widely accepted and during the 1960s was thought to have disproved logical positivism. Also, examples in appendix from modern 19th century analysis may be useful in evaluating mathematical formalization of QP and QC.

7. Lakatos, I. *The Methodology of Scientific Research Programmes.* philosophical papers vol. 1 and 2, Cambridge University Press, 1978.

   Collected papers that develop the theory of scientific research programs assumed as background knowledge in talk.

8. Pickering, A. *Constructing Quarks: A Sociological History of Particle Physics.* University of Chicago Press, 1984.

   Book offers sceptical view of high energy physics (HEP) written by a trained physics who became a sociologist. It is possible phenomenological problems with HEP also apply to QC.