POST QUANTUM CRYPTOGRAPHY –

WIDENING THE SEARCH

Michael Collins

University of Oxford

CAVEAT

I am not a cryptographer!

But I have been involved in the creation and adminstration of programmes at the interface of mathematics and computer science for over thirty years –

Joint undergraduate degree

M.Sc. in Mathematics and the Foundations of Computer Science

Centre for Quantum Mathematics and Computation (QMAC)

Now PQC

This programme will comprise two distinct but interwoven strands –

Research

Inspiring and training the next generation of cryptographers

RESEARCH

I will start by talking about a major project in my own field – finite group theory – to illustrate both time lines and how "theory", "practice" and unexpected connections may interact

1893 "Despite the major progress of recent years, on the one hand in our knowledge of particular examples, and on the other the development of a general theory, a large gulf remains between the two" – Frank Cole ("ICM" 1893)

Classification of Finite Simple Groups

1911 Burnside 2nd edition Prime 2 seems different

Classification of Finite Simple Groups

1911	Burnside 2^{nd} edition	Prime 2 seems different
1961	Feit-Thompson theorem	Odd order implies solvable

Classification of Finite Simple Groups

1911	Burnside 2^{nd} edition	Prime 2 seems different
1961	Feit-Thompson theorem	Odd order implies solvable
2011	Final links published	Aschbacher, Lyons, Smith, Solomon

Classification of Finite Simple Groups

1911	Burnside 2nd edition	Prime 2 seems different
1954	Brauer proposed a systematic programme (ICM)	
1961	Feit-Thompson theorem	Odd order implies solvable
2011	Final links published	Aschbacher, Lyons, Smith, Solomon

Classification of Finite Simple Groups

1911	Burnside 2nd edition	Prime 2 seems different
1954	Brauer proposed a systematic programme (ICM)	
1961	Feit-Thompson theorem	Odd order implies solvable
1972-73	Gorenstein programme	16-, reduced to 4-, point programme
2011	Final links published	Aschbacher, Lyons, Smith, Solomon

Classification of Finite Simple Groups

1911	Burnside 2nd edition	Prime 2 seems different
1954	Brauer proposed a systematic programme (ICM)	
1961	Feit-Thompson theorem	Odd order implies solvable
1972-73	Gorenstein programme	16-, reduced to 4-, point programme
1978	Durham LMS Symposium	Final road map drawn up
2011	Final links published	Aschbacher, Lyons, Smith, Solomon

Classification of Finite Simple Groups

1911	Burnside 2nd edition	Prime 2 seems different
1954	Brauer proposed a systematic programme (ICM)	
1961	Feit-Thompson theorem	Odd order implies solvable
1972-73	Gorenstein programme	16-, reduced to 4-, point programme
1978	Durham LMS Symposium	Final road map drawn up
1980	Classification claimed	"Gaps" in proof
2011	Final links published	Aschbacher, Lyons, Smith, Solomon

Finding the Finite Simple Groups

1900	Dickson's "Linear Groups" published. Alternating groups and finite analogues of classical groups known – also five Mathieu groups
1901,5	Dickson found (what later proved to be) finite analogues of E_6 and G_2
1955	Chevalley's $\mathbb{Z}$-form leads to finite analogues of complex Lie groups
~1960	Steinberg *et al* "Twisted" variations
1965	Janko found a group of order 176560
1966-75	20 more groups "found" – all but Monster and J_4 constructed
Early '80s	Monster and J_4 constructed; Ree group issue settled

IMPORTANT LESSONS

- Different facets of a programme may require quite different talents

- When you look for something randomly, still keep careful track of what you find so that others can replicate!

The Oxford Project

Three phases

The Oxford Project

Phase I. Ask obvious questions!

The Oxford Project

Phase I. Ask obvious questions!

(a) What can a quantum computer do?

The Oxford Project

Phase I. Ask obvious questions!

(a) What can a quantum computer do?

(b) What can a quantum computer **NOT** do?

The Oxford Project

Phase I. Ask obvious questions!

(a) What can a quantum computer do?

(b) What can a quantum computer **NOT** do?

Phase II. Look for areas of mathematics and theoretical computer science that offer the possibility of protecting information from a quantum attack.

Phase III. Search for specific structures!

Phase I

Tools at our disposal:

- Classically, study of quantum computing via unitary operators
- Newer – algebraic methods (Temperley-Lieb algebras etc)
- Algebraic topology (esp cobordism theory)
- Analysis (e.g., operator algebras, C*-algebras)
- Even newer – higher category theory

Amongst questions to be asked –

- Why do Shor's algorithm and Grover's algorithm work?
- Would a deeper understanding of these throw light on the limitations of a quantum computer?
- What are the appropriate measures of complexity when discussing a quantum computer?

Amongst questions to be asked –

- Why do Shor's algorithm and Grover's algorithm work?
- Would a deeper understanding of these throw light on the limitations of a quantum computer?
- What are the appropriate measures of complexity when discussing a quantum computer?

Hardest part –

What can we prove, as opposed to what do we merely believe?

Phase II

Aim to involve wide a spread of interests in mathematics and theoretical computer science –

- Number theory
- Combinatorics
- Algebraic Topology
- Algebra
- Quantum Computer Science and Algorithms Groups in DCS
- Broader resource of QMAC

Example

Group Theory has many undecidable problems – for example, the word problem.

Word Problem in a ***given*** finite group clearly decidable, but possibly "hard enough" – for finitely presented infinite groups, may or may not be decidable. There are decision problems that are provably hard – can any be exploited?

Also look for unexpected connections

Phase III

Find exploitable examples amongst areas identified for further study in Phase II.

Phase III

Find exploitable examples amongst areas identified for further study in Phase II.

Don't have an answer, otherwise project would already be complete!

"Trivial" example

$\mathrm{SL}(2,\mathbb{Z})$ is generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

Given a matrix X in $\mathrm{SL}(2,\mathbb{Z})$,

- Can we express X as a word in these generators?
- Can we express X as the shortest possible word in these generators?
- What is the length of the shortest expression?

In fact, it is possible to make these particular questions look hard, but they are in fact quite easy because of an inherent geometric structure. However, there are questions of this nature that most certainly are/might be hard.

One observation

If a quantum resistant algorithm should turn out necessarily to be "messy", we may not need to apply it throughout a system, but only as an initial "buffer".

Building Capacity - Teaching and Training

- Attract students through offering courses on cryptography, PQC for MFoCS
- These students take course work and write a dissertation
- Then prepared to go straight into Ph.D. work
- Extend basic cryptography course to undergraduate programme

Organisation of the Project

PI: Roger Heath-Brown
Assoc PI: Tom Sanders
Leading from CS side: Samson Abramsky

Two Postdoctoral Fellows to be appointed

Will use resources of the groups identified in Phase II, together with interested parties from other departments, institutes in Oxford –

e.g., Physics, Cyber Security Institute

Have allocated funds for workshops and senior visitors who will inspire and contribute – intend this to be part of a national effort where we will seek input as widely as possible. No area of study off the agenda, but seek to collaborate, not compete.

May be others – e.g., if Oxford's bid for a Quantum Technologies Hub should be successful, Samson Abramsky will lead a Work Package entitled "Unified Classical and Quantum Computing", and DCS will establish a post in quantum algorithms.

Goals

- We will create two posts within the Mathematical Institute to be held during the grant period by young researchers dedicated to work in the area of post quantum cryptography (PQC) and who can benefit from working with the large groups of both mathematicians and computer scientists already holding established or postdoctoral posts in Oxford.

- We will promote a broad interest in PQC and its interaction with current research amongst those already working in Mathematics or Computer Science in Oxford.

- We will inspire and train a cadre of students to work in cryptography and specifically PQC through the enhancement both of the existing taught M.Sc. course in Mathematics and the Foundation of Computer Science (MFoCS) and of the undergraduate courses in Mathematics and in Mathematics and Computer Science.

Gilles Pisier – Course currently being given at Texas A & M

Title: Tensor products of C*-algebras and Operator space theory

The course will revolve around the famous Connes-Kirchberg open problem. The various equivalent forms of the problem will be described and the necessary accompanying background will be presented. In addition the general theory of tensor products of C* algebras will be described. The notion of exact C* algebra and operator space will play an important role there, with an emphasis on C* algebras associated to discrete groups. Various forms of the non-commutative Grothendieck theorem will be presented in view of its recent connection with Bell's inequality. An introduction to quantum information theory will be given. Gaussian and unitary random matrices will be used repeatedly to illustrate the estimates by more "concrete" examples.

References: G. Pisier, An introduction to operator space theory, Cambridge Univ. Press, 2003

N. Brown and N. Ozawa, C*-algebras and finite-dimensional approximations, Graduate Studies in Mathematics, 88, American Mathematical Society, Providence, RI, 2008.

N. Ozawa, About the QWEP conjecture, Internat. J. Math. 15 (2004), 501–530.