

Re: *Quantum Computing* expert Bill Munro

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-04/0443.html>

From: Bill Unruh (unruh@string.physics.ubc.ca)

Date: 04/06/03

From: unruh@string.physics.ubc.ca (Bill Unruh)

Date: 6 Apr 2003 15:37:46 GMT

jsavard@ecn.ab.ca () writes:

]... and his colleague Keith Harrison were billed as encryption experts in
]a recent New Scientist item which I just saw today.

]In any event, these researchers called on scientists around the world to
]develop ciphers resistant to attack by quantum computers.

I did not read the article, but it sounds a bit weird.

a) Quantum computers are not here any time soon.

b) Quantum algorithms are still rather rare (fourier transform seems
still to be the only one that has been found to be useful and offers
an exponential speedup).

...

]Essentially, of course, as readers of my posts and website will no doubt
]realize, I would have expressed _extreme_ pessimism concerning the
]possibility of developing *public-key ciphers* that would be resistant to
]the advent of powerful quantum computers, since I am even untrusting of
]their security absent that development, since advances in mathematics
]could very easily vitiate pretty well all public-key ciphers.

Advances in mathematics can always destroy cyphers— public or private
key. Quantum computers will not help in destroying them Unless
mathematical advances are found which make them susceptible to the very
peculiar strengths of Q Computers. Q Computers are NOT "very powerful"
except on a very limited class of problems. They will always be far less
powerful than classical computers on an operation cycle basis (error
correction is horrendously expensive for one thing), and it is only on a
small set of problems where the peculiarities of the Q Comp would be
useful.

....