From: Miller, Carl A. (Fed)
To: Moody, Dustin (Fed); Chen, Lily (Fed)
Cc: (b) (6) Liu, Yi-Kai (Fed)
Subject: Postquantum crypto project
Date: Tuesday, April 18, 2017 10:17:45 AM
Attachments: Microsoft Word - NIST Blog 2nd Draft.docx.pdf

Hi Lily & Dustin:

If you have a minute:

I'm writing an entry for the NIST "Taking Measure" blog (http://nist-takingmeasure.blogs.govdelivery.com) and making some comments about the Postquantum Cryptography Project. Here's what I have right now. What do you think?

"The game-changing effect of quantum physics on cryptography is a double-edged sword. In 1994 Peter Shor invented a quantum algorithm, which, if implemented in a large-scale quantum computer (and we're not close to having one yet) would make many of the ways that we protect information completely insecure. Today I work in the Cryptographic Technologies group at NIST. Here, we create services and standards for the public to help them stay ahead of the game in the ongoing effort to protect information. We lead the postquantum cryptography project, the goal of which is to design next generation cryptography standards that are resistant to quantum computers."

[The full draft is attached, although it's long and I wouldn't expect you to read the whole thing. Comments on that are welcome too.]

The editors and I have been working to write something that is not too alarming, but also accurately calls public attention to PQC. Your input is welcome.

Yi-Kai and Stephen: Your input is also welcome! (You may know more about the background than I do.) And I'm also trying to fill in a figure in the following sentence:

"The investments in the field of quantum computing are now at $XXX per year."

-Carl

—————
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

Quantum Information: Changing the Rules of the Game

I was a math researcher at the University of Michigan back in 2008 when I had the crazy—one could even say random—notion to shift from pure math to quantum information. This was a major departure from what I was used to. Most of my career up to that point had been devoted to researching mathematics that had no immediate practical applications. I was a "Math Olympian" in high school, I had studied math in graduate school, and I was on course to get a tenure-track job in math after my time at Michigan.

But math is both an art and a tool, and at this point in my career I was interested in doing applied science. I had read about quantum information in popular science articles, and (not knowing much about it) thought it was mysterious and quite interesting.

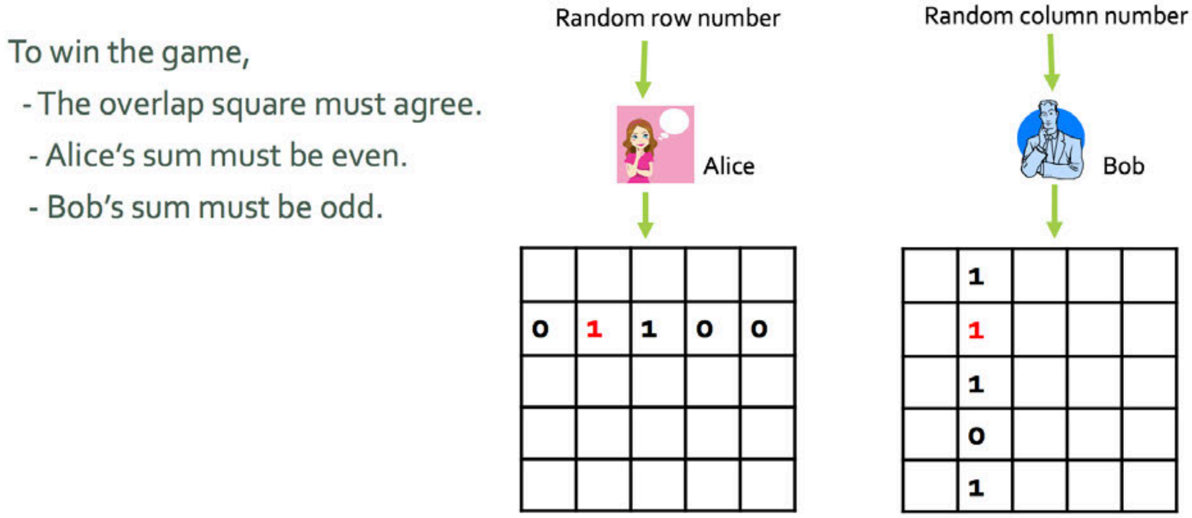
This shift I made was puzzling to my colleagues and mentors. Pure mathematicians are used to fixed rules, untroubled by the messiness and uncertainty of everyday experience. We set down "axioms," which are fixed assumptions, and then we build "theorems," which are deductions we make from those assumptions. A "proof" is a final (and immutable) certification of the truth of a theorem. In information technology, however, this is not so, although, before the 1980s, you could have reasonably believed that it was!

This makes a difference in everyday life. Every time you do a credit card transaction online, you are trusting that a certain cryptographic protocol is protecting the transmission against eavesdropping. But this assumption, as we'll see, is built on a sliding foundation. This is what makes information science challenging, and what makes it so much fun.

Quantum Logic

In the early 20th century, physicists found that things were going on at the subatomic level that were very hard to explain. The idea of quantum superposition came into play. In everyday life, I can put my car key on the kitchen counter, or I can leave it my pocket, but I can't do both. I may forget where I put it afterwards, but it's still in one place or the other.

At the subatomic scale at which quantum mechanics operates, this is not actually so. A key that behaved according to quantum rules could be *both* in my pocket and on the counter at the same time. And when I check to see where it is, it would spontaneously end up in one location or the other. This is the idea of quantum superposition, and it was eventually decided (despite skepticism from Einstein) that there was simply no other way to explain the results of certain experiments. Superpositions do not fit our usual notion of uncertainty – they are not governed by the laws of probability – but they can be understood with more advance mathematics (invoking objects like the square root of minus one).



To win the game,
- The overlap square must agree.
- Alice's sum must be even.
- Bob's sum must be odd.

Figure 1: The Magic Square Game.

In Figure 1, you see a math puzzle called the "Magic Square puzzle." It's the kind of puzzle that could have shown up on an early round of some of the math competitions that I used to do. Alice and Bob are not allowed to communicate, but to win the game they still have to come up with answers (of the form 00110, 01111, etc.) that satisfy all the given conditions.

With a short argument, we can convince ourselves that the Magic Square puzzle *has no solution.* If Alice and Bob share a script for their responses to the game, Alice will find that since each of her rows must sum to an even number, her entire script must sum to an even number. Bob's columns, on the other hand, must sum to an odd number, so his entire script must sum to an odd number! Since their scripts cannot agree, they don't have a perfect strategy.

The Magic Square game is impossible to win. Or is it?

If Alice and Bob get together in advance and share a certain *superposed* quantum state between the two of them, it turns that there is a strategy they can use to win the Magic Square game *every time*. The strategy involves Alice and Bob making cleverly chosen measurements on their shared state (without communicating) to produce the numbers in the 5x5 grid.

The curious thing about this strategy is that *there is no script*. If you asked Alice to tell you in advance what answers she would give to "row 1," "row 2," *etc.*, she wouldn't know -- the bits in the grid remain in a superposed state until Alice and Bob perform measurements and find out what they are. The outcome of the strategy is inherently unpredictable, even to the players themselves.

A mathematical "proof" has thus been undone because it made assumptions that didn't hold in the physical world. This is bad news! Information science is based on assertions about what computers can and—crucially for cryptography—*cannot* do. The introduction of quantum physics is a game-changer that requires us to rewrite the rules.

But we shouldn't be discouraged by this -- we should use it our advantage. This is where quantum information begins.

Quantum Randomness

In 2006, Roger Colbeck conjectured that multiplayer games (like the Magic Square game) can be used to create *certified* random numbers. Randomness is an essential resource in communication—every time you communicate securely online, you are using a "secret key," which is a string of 0s and 1s that must be random enough that no other person can guess it. Devices that play the Magic Square game successfully could (if the conjecture is true) give us secret keys of arbitrary length that are guaranteed to be random.

In 2010 I had moved up to the University of Michigan computer science department, ready to see if my quantum dream could be realized (although I wasn't yet sure how). A few months later my colleague Yaoyun Shi showed me Colbeck's conjecture, and it seemed like an excellent mathematical mountain to climb. It was a simple question that had defied the best available techniques.

I've been asked what math research is like. My answer is something like this: It's a lot of sweat, maybe a few tears, some blood (papercuts are the worst) … and a lot of daydreaming. (The importance of daydreaming should not be underestimated! Just don't do it all the time.) Periods of intense of activity are separated by periods of trying to think more deeply and draw out underlying patterns that you may have missed. Every now and then, you have a key insight and are reminded of why you love research. Once enough of these insights accumulate—and when momentum picks up, they can start to come very fast—you turn them into a successful research project.

About 2-1/2 years after Yaoyun and I happened upon the certified randomness problem, we solved it. It was undoubtedly the hardest math problem I've ever solved, and it took us 70 pages to do it. Our results (along with those of others in the field) mean that "certified randomness" is real—and not only that, we can create it with today's technology. For those who need secure communication that they can trust, this is good news.

The future:

The game-changing effect of quantum physics on cryptography is a double-edged sword. In 1994 Peter Shor invented a quantum algorithm, which, if implemented in a large-scale quantum computer (and we're not close to having one yet) would make many of the ways that we protect information completely insecure.

Today I work in the Cryptographic Technologies group at NIST. Here, we create services and standards for the public to help them stay ahead of the game in the ongoing effort to protect information. We lead the postquantum cryptography project, the goal of which is to design next generation cryptography standards that are resistant to quantum computers. We also manage the NIST randomness beacon, which intends to provide certified (quantum) randomness as a service to the public using schemes like the one Yaoyun and I developed.

The other half of my time is spent at the Joint Center for Quantum Information and Computer Science at the University of Maryland, where we are trying to prepare a new generation of quantum researchers.

The investments in the field of quantum computing are now at $XXX per year, and more quantum cryptographic solutions are being made available to the public—all of which means that there are many more quantum math problems to solve.

It's an exciting time be an applied mathematician.

Bio:

Carl A. Miller is a Mathematician in the NIST Computer Scientist Division, and a Fellow of the Joint Center for Quantum Information and Computer Science. Carl has lived in Maryland, North Carolina, California, and Michigan, and is now happy to back within three miles from where he went to high school. He lives in Silver Spring, MD, with his partner Andrea and their two cats (Autumn and Pepe), and really misses Leonard Cohen.

[NEED TO REPLACE FIGURE 1 – MULTIPLE ISSUES]
[HENRY YUEN WROTE A BLOG ENTRY ON A SIMILAR SUBJECT – COMPARE, CHECK FOR OVERLAP]