From: Esser, Mark (Fed)
To: Miller, Carl A. (Fed)
Subject: RE: Esser, Mark (Fed) has shared "Quantum Information Changing the Rules of the Game_ver2_mde"
Date: Friday, April 28, 2017 6:13:03 PM
Attachments: image005.png
image007.png
image009.png
image011.png
Quantum Information Changing the Rules of the Game_ver3_mde.docx

---

Hey Carl,

Sorry, Sharepoint has been acting a little squirrely lately. I've just attached the doc.

Since we're talking about entanglement, I thought we should go ahead and make that explicit. We don't need to go too far into the nature of the clever measurements, partly because I don't understand them, but if you wanted to elaborate a little I'd be okay with that. I think it would be satisfying to reveal how exactly the entangled encryption scheme works in some detail, but see what you think.

I also thought we could use a little more discussion of what you actually showed, if you don't mind. I don't want it to be a research summary, but we spend a lot of time on background and never really go all that far into what you actually did, and I don't want you to be shortchanged. I don't want you to spend all that much more time on this, but I do want people to understand and appreciate what you did, even if only a little. As it is, it's still a little too handwavy in the quantum randomness section. Now less so in the Magic Square game discussion, but I don't know if my additions helped.

I apologize for the frustration, but I think we're really close. We'll get there, just need one last push.

From: Miller, Carl A. (Fed)
Sent: Friday, April 28, 2017 2:54 PM
To: Esser, Mark (Fed) <mark.esser@nist.gov>
Subject: Re: Esser, Mark (Fed) has shared 'Quantum Information Changing the Rules of the Game_ver2_mde'

Hi Mark –

See what you think of the current version. I gave a detailed explanation of why the Magic Square game is hard to win.

I don't know if we can explain what the clever measurements are without using a good deal more space. I did include a link to a paper (https://arxiv.org/pdf/quant-ph/0407221.pdf) for the scientifically interested reader. I can write more although that will probably change the blog entry from a narrative into more of a scientific exposition (which is ok, if that's what we want to do).

Microsoft Word online seems kind of buggy – apologies that I may have not been able to read some of the comments, and that some my edits may be imprecise – next time I'll just use regular Microsoft Word.

-Carl

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

From: "Esser, Mark (Fed)" <no-reply@sharepointonline.com>
Reply-To: "Esser, Mark (Fed)" <mark.esser@nist.gov>
Date: Tuesday, April 25, 2017 at 1:33 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Cc: "Esser, Mark (Fed)" <mark.esser@nist.gov>
Subject: Esser, Mark (Fed) has shared 'Quantum Information Changing the Rules of the Game_ver2_mde'

Carl,

I this is coming along, but I'm still pretty hazy about the encryption scheme and the magic square game. I tried to clarify the game, but I think it might be more impactful if we showed how the game fails under classical rules.

I'd also like to know what clever measurements Alice and Bob are making and how that helps them win the game, and eventually secure their communications.

Just give it your best try. Don't fret about math month.

Open Quantum Information Changing the Rules of the Game_ver2_mde.docx

See more related to Esser, Mark (Fed) in Delve.

Quantum ~~information~~Information: Changing the ~~rules ~~Rules of the ~~game~~Game~~.~~

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Space Before: 0 pt, After: 0 pt

I was a math researcher at the University of Michigan ~~Back ~~back in 2008~~, I was working as a math researcher at the University of Michigan,~~ when ~~and ~~I ~~dreamed ~~had the crazy—one could even say random—~~up the ideadream~~notion to shift from studying pure math to a branch of information theory called ~~that wanted to work on the theory of ~~quantum information. Why would I willingly abandon the ivory tower? Well, ~~M~~math is both an art and tool, and I wanted to ~~see the other side of the subject~~become more familiar with its practical aspects. Perhaps more importantly, though, quantum information just seemed cool.~~ More importantly This was a major departure from what I was used to. Most of my career atup 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. I didn't have any particular academic reason for this, other than the fact that I'd read about the topic, and (in the words of a skeptical mentor) it just seemed interesting to me.I had learned about quantum information from popular science articles, and it seemed mysterious and quite interesting.~~

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

~~This was a departure from what I was used to. Most of my career had been devoted to mathematics -- I was a “Math Olympian" in high school, I had studied math in graduate school, and I was on a course to look for a tenure-track job in math after my time at Michigan. But, for some reason, I was interested in doing applied science, and, to me, quantum information was the neatest thing that came to mindout there.~~

Formatted: Space Before: 0 pt, After: 0 pt

The shift took me in an interesting direction~~I made was puzzling to my colleagues and mentors~~. ~~In mathematics, weWe~~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 ~~the ~~deductions we make from those assumptions.~~ The basic assumptions are completely fixed, and have been for at least the past 100 years. ~~ A "proof" is a final~~(~~—and immutable~~)~~—certification of the truth of a theorem.

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

Formatted: Normal (Web)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Space Before: 0 pt, After: 0 pt

~~But i~~In information ~~technology~~theory, however, this is not so.~~ , (although at earlier points in history, you could have believed that it was!).~~, . ~~(Aalthough, before the 1980's, a personyou could have reasonably believed that it was!)~~

Formatted: Font: (Default) +Body (Calibri)

~~You see, EeInformation science affects us every day. ~~Each~~very~~ time I~~you~~ do a credit card transaction online, I am~~you are~~ trusting that~~trusting that ~~ a certain cryptographic protocol ~~is ~~will encode my information well enough to ~~protecting the transmission from against eavesdropping~~prevent criminals from stealing my credit card number and going on a shopping spree.~~–~~ But this assumption, as we'll see, is built on a ~~sliding ~~shaky foundation.~~–~~ This is what makes the ~~theory of information~~information theory so~~information science~~ challenging, ~~and also~~and what makes it so much fun.

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Quantum ~~logic~~Logic~~:~~

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

In the early 20th century, physicists found ~~that~~ things ~~were~~ going on at the subatomic level that were very hard, if not impossible, to explain.~~–~~ For instance, ~~The idea of "local realism"~~ ~~quantum superposition came into questionplay. I~~in my everyday life, ~~""Local realism"" is simple:~~ 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 ~~microscopic~~ subatomic scale~~s at which quantum mechanics operates~~, ~~this is actually not so~~things are … different. ~~: they~~ A key that behaved according to ~~the~~quantum rules ~~of the subatomic world~~ could be *both* in my pocket and on the counter at the same time.~~–~~ And when I check to see where it is, it ~~will~~ would spontaneously ~~decide to be~~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~~that, ~~(~~as counter~~-~~intuitive as it seems~~)~~, ~~it is~~ this concept provides the right way to explain results of certain experiments.~~–~~ ~~It turns out that "Superposition" is real. These superpositions are not governed only by the usual rules of probability, but by complex and imaginary numbers, (which, as it turns out, are not so imaginary).~~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 advanced mathematics ~~(~~by invoking imaginary numbers ~~objects~~ like the square root of ~~minus one~~ -1~~, which is an imaginary number)~~.

~~Now~~ It’s here where things begin to get interesting. Below you see a math puzzle called the "Magic Square game."[1] It's the kind of problem that might have shown up on an early round of math competitions that I used to do.

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Commented [SB(1]: I don’t think we should invoke "local realism" in this argument. Locality brings up issues of faster than light communication. To me, it's a more simple argument of superposition of states. And that the key is in both places at once, but you can't really "use" them at both places. If you reached for the key in your pocket, and then tried to use it, wouldn't the key on the counter disappear?

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Commented [SB(2]: We don't explain how imaginary numbers come into play in the following example. I propose removing this reference unless it is important and we can explain it more.

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Normal (Web)

Commented [EM(3]: We can’t do footnotes. At least, I don’t know how to format them in the software.

Formatted: Footnote Reference, Font:

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

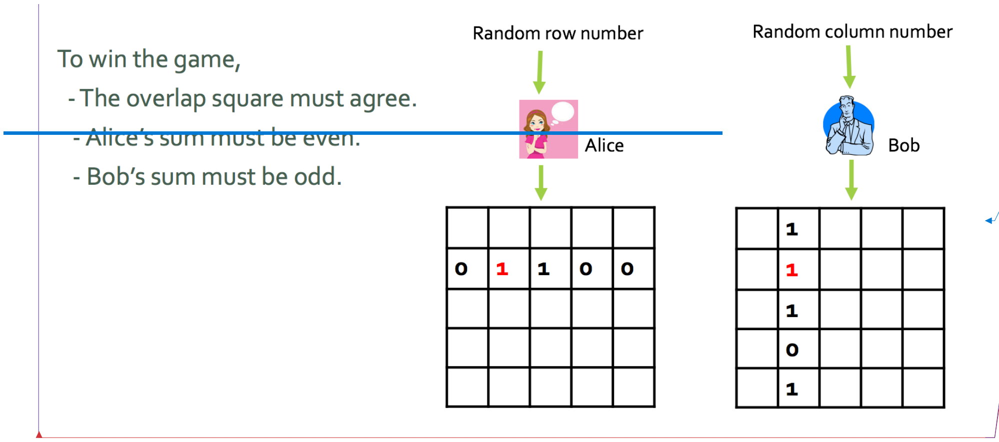
---

[1] Is it a puzzle or is it a game? It depends on whether you’re a mathematician or a computer scientist!

Formatted: Footnote Reference

Formatted: Font: (Default) Calibri, 11 pt

Formatted: Footnote Text

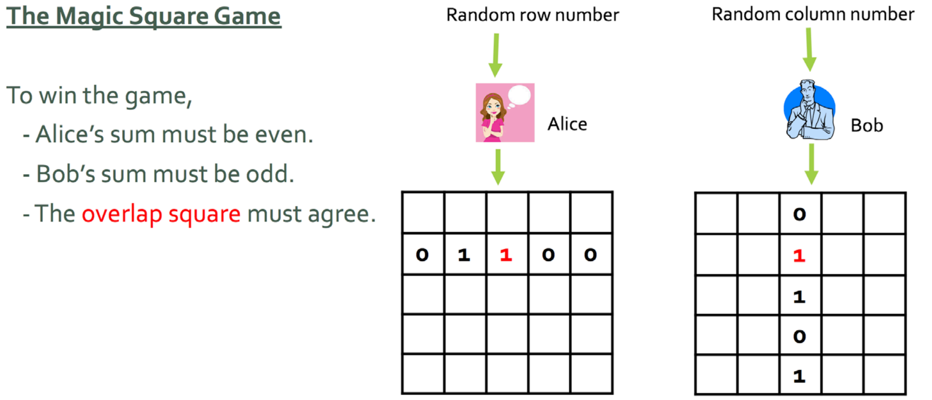


To win the game,

- The overlap square must agree.
- ~~Alice’s sum must be even.~~
- Bob’s sum must be odd.

0	1	1	0	0

	1			
	1			
	1			
	0			
	1			



The Magic Square Game

To win the game,

- Alice’s sum must be even.
- Bob’s sum must be odd.
- The overlap square must agree.

0	1	1	0	0

		0		
		1		
		1		
		0		
		1		

Alice, who is assigned a random row, and Bob, who is assigned a random column, ~~are~~ each ~~given a random number from 1 to 5, and they~~ have to fill in b~~its~~oxes in a grid ~~in the corresponding row or column to~~that satisfy all three of the given conditions. -Most importantly, they can't communicate when the game is underway. -Is there a strategy that will allow them to win this game every time? (In the example shown, they have won, but maybe they just got lucky.)

We can imagine Alice and Bob trying to work out a script in advance. -Here~~ i~~’s an attempt:

Commented [SB(4]: What is the "overlap square"? Not clear. Is it the red "1"?

Formatted: Font: +Body (Calibri)

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: 12 pt

Formatted: Font: +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

Formatted: Normal (Web)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

Commented [EM(5]: Caption: Most maddening game of Soduku ever!

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

0	0	1	1	0
0	1	1	0	0
1	0	1	1	1
0	0	0	0	0
0	0	0	1	??

This strategy is good (rows are even, columns are odd) except that there is no way to correctly fill in the last square. ~~-~~If you try filling in the grid in a different way you will always run into a snag like this one.

~~Figure X~~1~~: The Magic Square Game.~~

~~-~~

~~In Figure X~~1~~, you see~~~~This is a math puzzle called the "Magic Square puzzle." It i'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 nonetheless they still have to come up with answers (of the form 00110, 01111, etc.) that will satisfy all the given conditions.They win with the column/row chosen here, but try to complete the rest of the puzzle without breaking the rules. And remember, Alice and Bob are only told which column or row to complete—they can't share answers in advance. Any disagreement means they lost and the game is over.~~

With a short ~~argument~~argument, we can convince ourselves that the Magic Square puzzle *has no solution.*~~–~~ In any script,~~If Even if Alice and Bob share a script for their responses to the game, we will~~Alice will find that since each of ~~Alice's~~ her rows must sum to an even number, her entire script must sum to an even number~~,~~. Bob's columns, on the other hand, ~~while since each of Bob's columns~~ 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~~With a little help from quantum physics~~ 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 using entangled particles, another weird quantum phenomenon whereby particles can be put in a relationship with one another such that, say, when one of the particles is spinning clockwise, its partner particle~~s~~ will always spin counterclockwise *no matter ~~where in the universe~~how far apart the particles happen to be*. By leaving nine of the squares undetermined, ~~and~~ Alice and Bob can make~~making~~ cleverly chosen measurements o~~n their~~f their entangled particles ~~shared state~~ (still without actually communicating!) and use those measurements to fill in th~~ose~~eir numbers ~~if asked~~.

Formatted: Font: +Body (Calibri)

Formatted: Font:

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt, Not Italic

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), Italic

Formatted: Font: (Default) +Body (Calibri)

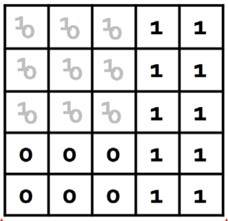
Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

~~The odd and even conditions will always be satisfied~~Using this strategy, ~~. This is c~~called pseudo-telepathy, they will win the game *every time*~~ (https://arxiv.org/pdf/quant-ph/0407221.pdf)~~.



10	10	10	1	1
10	10	10	1	1
10	10	10	1	1
0	0	0	1	1
0	0	0	1	1

~~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~~ that ~~they can use to win~~s ~~the Magic Square game *every time*.~~

The curious thing ~~about this strategy~~ here is that *there is no script*.~~–~~ If you asked Alice to tell you in advance what answers she would give to any of the nine entries,~~"row 1," "row 2," *etc.*,~~ she wouldn't know~~-- --~~—those bits~~. iIt's only after she applies measurements to her system -- and achieves certain inherently random outcomes from those measurements -- that she is able toc~~~~an perfectly win the game.~~ remain in a ~~superposed~~undetermined 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 ~~assumed~~ made ~~physical~~ assumptions that didn't hold in the ~~real~~~~everyday~~physical world.~~–~~ This is bad news!~~–~~ Information science is based on assertions about what computers can ~~do, and also~~and~~--~~—crucially for cryptography~~--~~—~~what they~~ *cannot* do.~~–~~ ~~Introducing~~ The introduction of quantum physics ~~into the mix~~ is a game-changer~~. We~~ that requires ~~-~~us to ~~need to~~ rewrite the rules.

~~Quantum information was born of the realization that this is not a bug --~~ —~~it's a feature.~~But we shouldn't be discouraged by this~~--~~—we should use the new rules to our advantage. ~~-~~This is where quantum information begins.

Quantum ~~randomness~~Randomness~~:~~

In 2010 I moved up to the University of Michigan computer science department, ready to see if my dream of becoming a quantum mathematician could be realized. ~~-~~At this point I had left behind a conventional academic track and was taking an improvised path that was sometimes exciting, sometimes quite daunting. ~~-~~(Advice to young researchers: it is possible to switch fields after a Ph~~.~~D~~.~~, but very difficult, so only ~~-~~do it if you have a good reason!)

A few months later my colleague Yaoyun Shi found a fascinating problem for us to study. ~~-In 2006,~~ Roger Colbeck had conjectured that multiplayer games (like the Magic Square game) can

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Commented [EM(6]: Since we're talking about entanglement, I've included a very basic discussion that I think will suffice. No doubt I misconstrued something.

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt, Not Italic

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

be used to create *certified* random numbers. Randomness is an essential resource for communication~~ in communication --~~ —every time you communicate securely online, you are using a "secret key,"~~,~~ which is a string of 0~~'~~s and 1~~'~~s that must be ~~sufficiently random~~random enough that no other person can guess it. Colbeck conjectured that d~~D~~evices that play the Magic Square game successfully ~~might~~ will produce ~~(if the conjecture is true) give us these numbers that are~~secret keys of arbitrary, unguessable, random length.~~ guaranteed to be random.~~

This seemed like a great starting point: a simple question that had defied the best available techniques.

~~After a few years of kicking around in the University of Michigan computer science department and trying to find the best approach to creating certified random numbers, Together with mmy colleague Yaoyun Shi at the University of Michiganand I joined forces and , we set our sights on climbing theis mathematical mountain that is quantum randomness this problem in 2011. At this point, having already given up the math academic track to go into quantum information science, I was in a grant-funded research position at the University of Michigan at the computer science department at the University of Michigan, having given up the math academic track in pursuit of something that excited me more. Quite adrift, I was ready to see if what I dreamed up in 2008 might be real, and the quantum randomness problem seemed like an excellent mathematical mountain to climb.~~

I've been asked what math research is like. ~~I would say this~~My answer is ~~always~~ something like this: ~~it's~~ It's a lot of sweat, maybe a few tears, some blood (papercuts are the worst)~~, —~~ , and a fair amount of~~lot of~~ daydreaming. (The importance of daydreaming should not be underestimated! That's where some of the best ideas begin.~~ 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 have been missed beforeyou may have missed.~~ Eventually~~Every now and then, you have a a key insight happens, a and nd we'are reminded of why we you love research. Once enough of these insights accumulate -- —and when~~ the momentum picks up, insights start to come fast, and ~~they start to come fast -- —we~~ you turn the whole thing~~ them into~~ a successful research project.

About 2-1/2 years ~~from when we originally~~after ~~we~~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 ~~led us~~ us ~~to write a~~ 70 pages~~ paper.~~ to do it. Our results, ~~(and~~ 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:

~~There is much more to the quantum story.~~ The game-changing effect of quantum physics on cryptography is a double-edged sword. In 1994 Peter Shor invented a quantum algorithm~~,~~,

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Space Before: 0 pt, After: 0 pt

Commented [EM(7]: Studying what? I'm a little confused about the chronology here.

Commented [EM(8]: Did you dream something specific? I thought that you had just wanted to switch tracks. Did you have some idea about QIS because of your reading that you were ready to explore or that had crystallized in some way?

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: +Body (Calibri)

Commented [EM(9]: Can you briefly describe what you showed? That Colbeck was correct and that you can use entangled particles to create random numbers?

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

which, ~~puts in jeopardy most of the secure communication systems available today. It means that~~ if implemented in a large-scale quantum computer ~~is built~~ (and we're not ~~there yet~~close to having one yet) ~~then~~ would make ~~much of our~~ many of the ways that we ~~secure~~protect information ~~will be completely insecurobsoletecompletely insecure~~completely insecure~~e~~.

Today, I work in the Cryptographic Technologies group at NIST.~~ and at the Joint Center for Quantum Information and Computer Science at the University of Maryland, which is mercifully abbreviated as QuICS, . where Here, we create services and standards fo~~ Here, we create services and standards for the ~~r the~~ public to help them stay ahead of the game in the ongoing effort to protect information.~~–~~ We lead the postquantum cryptography project, whose goal is to design next~~-~~-generation cryptography standards that are resistant to quantum computers, and also manage the ~~HYPERLINK "https://www.nist.gov/programs-projects/nist-randomness-beacon"~~NIST randomness beacon, a public randomness service. ~~-~~I'm an adjunct faculty in~~whose the goal of which is to design the next generation of cryptography standards to be that are resistant to quantum computers, which can play tricks that ordinary computers can't to crack encryption codes. 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 aboveYaoyun and I developed.~~ the Joint Center for Quantum Information and Computer Science (mercifully abbreviated as "QuICS") ~~(http://quics.umd.edu/)~~ at the University of Maryland ~~(which is mercifully abbreviated as "QuICS")~~.

~~The investments in the field of quantum computing are now at $XXX per year,~~Right now, large companies are competing to build quantum computers, 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 ~~scientist~~mathematician~~, which is not something we get to say all that often~~.

~~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 at the University of Maryland at the University of Maryland. 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. One of his proudest achievements from high school was learning to play all of "Rhapsody in Blue" on a single piano without an orchestra. He lives in Silver Spring, MD, with his partner Andrea Andrea Tanner and two cats (Autumn and Pepe), and really misses Leonard Cohen..~~

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri)

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Hyperlink, Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Hyperlink, Font: (Default) +Body (Calibri)

Commented [M(10]: Same problem here -- I can't figure out how to insert the link.

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font:

Formatted: Normal (Web)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri), 12 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: (Default) +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt

Commented [EM(11]: I wouldn't name Andrea, but I would like to get your cats' names.

Formatted: Font: +Body (Calibri)

Formatted: Font: +Body (Calibri), 12 pt