Episode 42: Quantum Twins Talk in Code
Physicists: Miles Steininger, Dr. Katherine Brown

Transcribed by Denny Henke

Ben: Oh. Hello old friend, it's good to see you. Let's talk about this word fascination. It describes an unquenchable urge which compels our hearts to quest and be captivated. As long as there are elegant explanations to complicated phenomena science will never lose its romance. Over the years I've traveled the world indulging in my fascination with physics and now I find that a new hunger has woken within me. A fiery need to share these great ideas with the people around me so I have assembled a team of some of the greatest most lucid most creative minds I have encountered in my travels and I call them my Titanium Physicists. You're listening to the Titanium Physicists Podcast and I'm Ben Tippett, and now allez physique!

[1:49]

Ben: Ellohay. Isthay isway anway exampleway ofway anway encodedway essagemay. Iway amway eakingspay inway Englishway utbay anymay eoplepay inway earinghay isthey onway tey ebay ableway otey anslatetrey hatwey iway amway angsay ackbay intoway Englishway andway onway tay understandway hatway iway May angsay. Odaytay, onway - itaniumway hysicistphay of odcastpay eway eray alkingtay aboutway usingway uantumquay echanicsmay otay oday ryptographycray.

Hello. This is an example of an encoded message. I am speaking in English but many people in hearing this won't be able to translate what I am saying back into English and won't understand what I'm saying. Today, on the Titanium Physicist Podcast we're talking about using quantum mechanics to do cryptography when we're trying to communicate. Speaking of message quality, my guest today is, as far as I am concerned, one of the most electrifying people in the Canadian media scene. For years he was the person who explained the Internet to people on the CBC and then on the tv, his show, *Search Engine* ran in its various forms for five years. This last autumn he started an exciting new project. It's a podcast called *Canadaland* where he analyzes and criticizes the current state of Canadian media. The Canadian media, for all of you who don't know, has somehow spent the last decade reading all of its news off a newspaper printed in 1993 about how Ralph Klein is a great guy. The *Canadaland* podcast is a brilliant and interesting and infuriating, if you're Canadian you should probably be listening to his show. Welcome to my show Jesse Brown!

Jesse: Thank you very much, a pleasure to be here.

Ben: I'm super excited. So, Jesse today I have assembled two of my finest Titanium Physicists. Arise Dr. Katherine Brown! Dr. Katherine did her PhD at the University of Leeds in quantum computing and she's currently training to be a patent attorney in the U.K. And arise Miles Steininger. Miles did his undergrad with me at UBC and he's currently the IP Manager at D-Wave Systems, the quantum computer company. So, let's start talking about cryptography. Jesse do you know anything about cryptography?

Jesse: Yeah. It's encoding things. Encrypting them, like PGP. I have the basic concept but none of the guts of it.

Miles: Yeah, no, if you've used PGP, I mean configuring PGP, I think, is mentally more taxing than actually thinking about the basic concepts of cryptography. Cryptography is something that lots of us have a basic understanding of. We use the words codes or ciphers. A code can be a, like Ben was talking in code and you use certain words to mean, to stand in for other words or certain symbols to stand in for other symbols. Ah, ciphers are when you substitute letters for each other. And cryptography is usually about ciphers. And in regular cryptography we have, you know, various schemes of doing it. So, have you heard of public key cryptography?

Jesse: Public key, no.... Yes... Okay, let's just say no.

Miles: Okay. No, alright. We'll get there but ah, there's also a very basic form of cryptography and that's called one-time pad and that is a very simple form of cryptography. But it turns out that it has a very cool property which is provably secure. And if you wanted to send a message to somebody and you wanted to encode it, you could take the message, write it down and then you can use something called a one time pad to encipher it. And the enciphering operation is just for every bit of your message you're going to do an exclusive or operation, that's a binary operation between two binary bits and you're going to get an enciphered message.

Ben: Jesse, did that make any sense?

Jesse: No.

Ben: Okay, so, you remember when you were a kid. You probably got taught, you were told to write down a message and to change the letters in your message,to, say to some other letter. So, one thing you could do is move each letter subsequently down the alphabet, right? So, every time you see the letter a you write the letter b and every time you see the letter c you write the letter d and anytime you see the letter zed you write the letter a, right?

Jesse: Now we are dumbing this down exactly to my level. Yes, I am with you.

[6:14]

Ben: Yeah, so the deal with that is it changes your lovely sentence into a bunch of gibberish. But, it's really easy in those cases to figure out what they've done. So you can look at this list of letters and you can say, hey look, e should show up maybe 10% of the time. Every time we see an f that shows up about 10% of the time I think this person has just shifted the letters one over. So, these one time pads, what they do is they garble up the number of letters down the alphabet. Each one goes okay, we're going to agree that first letter in your message is going to get shifted down 5 letters and the second letter you use is going to be shifted down 13 letters in the alphabet and the third letter you use in the message is going to be shifted down two letters in the alphabet and like that, right? So you have a string of numbers that represent the number of letters shifted down in the alphabet. But then the coded gibberish is really difficult for somebody to figure out what the original letters were. But the person you're trying to communicate with knows how many letters you've shifted each letter down by so can shift them back and regain the original message.

Jesse: Because they have the key.

Ben: Because they have the key.

Jesse: No matter how complicated a form of encryption is as long as it has a consistent key then anybody will be able to crack it so it's necessary to have unique keys for every encrypted communication.

Ben: Yeah.

Miles: Right. And that's why it's called a one-time pad. You use the pad once.

Jesse: Gotchya.

Miles: And in implementation, you know, you can do this in binary, you can do it with letters in the alphabet and shifting certain numbers, it doesn't make a lot of difference. Binary is just very convenient mathematically, you can get a computer to do it and traditionally when we talk about sending information we send it from person a to person b. Conventionally, we call person a Alice, person b is Bob, and then you can have an eavesdropper, and she's usually called Eve. And I've never worked out why the eavesdropper is a female but that's just convention.

Ben: Eve is short for eavesdropper.

Miles: I know but it, like...

Jesse: It could be Eve like Yve. This is obviously...

Miles: Yeah.

Laughter.

Ben: Well, yeah.

Jesse: There ya go. The original cryptographers that figured this out are showing their gender bias.

Ben: At least there's a pun in there.

Miles: Basically one-time pad cryptography it is, pretty well the only one that is provably secure. But, because you have to share these one-time pads it's pretty difficult. And in the 1970s or so, you know, banks would really want to have secure communications and they would have people on airplanes going around the world with briefcases that were literally handcuffed to their wrists. And...

Jesse: Hold on, inside the briefcase was... The key?

Miles: Yeah, it would be a disk with a key on it. Or magnetic tape probably, actually.

Jesse: Right.

Miles: Or punch cards for all I know.

Jesse: So, the challenge is that, in order for the recipient to decipher any encoded message you must send them the key and if anybody intercepts the key then the security is compromised.

Miles: Mmmhmmm. I mean, the system probably fell apart because you had to pay these guys with briefcases too much money, you know, and vet them too much and things like that.

Jesse: Spy assassinations and sexual encounters and what not.

Miles: Oh yeah, honeypot traps, etcetera. So, alternative schemes were developed, the most interesting which is public key cryptography.

Jesse: See, now you lost me because when you say public key my very simple understanding is well that's not going to work, the key is public. If everybody has the key then the key is not going to work. So I'm missing something here.

Miles: Yeah, well, no, you're not. I mean, it's absolutely true that the key is public but it still works. The key that is private, is never shared... Jesse, if I wanted to send you a message it's no more difficult than looking up Jesse Brown, finding out what your public key is, using it to encode a message sending it to you and then you use your private key which is paired to your public key to decode it and that's public key cryptography.

Jesse: Ahhh. I see. I see. Okay.

Miles: And, you know, how does it work? You want a very simple introduction to it there's a book by Simon Singh, a very good science journalist in the U.K. It basically works on the notion that you have mathematical operations that to do it in one way is very, very easy and then to do the inverse is very, very difficult. You know, are you any good at long division?

Jesse: I wouldn't say that I'm good at it but...

Miles: Right, but do you, most people find that division really a lot harder than, say, multiplication. If I gave you two numbers and asked you to multiply it together, not so hard. If I asked you to to divide one number into another, some people take a lot longer.

Jesse: Okay.

Miles: Um, same thing happens for computers. There are certain operations that are really easy to do. Turns out that it's really easy to multiply two numbers together but to find the two numbers that made that number can be really, really difficult.

Jesse: And that applies to this because that's what you need to do in order...

Miles: In order to get the private key from the public key, you would have to do the difficult operation. That's basically the notion of public key cryptography. It relies on the notion that there's something that's really hard to do and that's how it secures it.

Jesse: You say it works but not provably so? What does that mean?

Miles: Everybody believes that it is sufficiently hard to do but nobody can prove that it is impossible.

[11:16]

Ben: You know, if I sent you a message encoded with a one-time pad and somebody intercepted it, they would know how long the message was but anything else would be gibberish to them because there's no way to figure out which letter got transposed to which letter.

Jesse: Right.

Ben: With this one there would be a way to figure out what the private key is using the public key. But the deal is it would take a regular computer, even a supercomputer so long to do it that it is essentially, secure. It's like, imagine like a lock pick, this is a lock that you can pick it would just take you 17 years to pick this lock and by that time the security guard at the bank is just come wondering around and say hey, what are you doing with the lock pick there?

Jesse: Even with the processors getting stronger and more complicated and powerful all the time, no one has demonstrated the ability to crack this?

Ben: Not with a regular computer.

Miles: When they came up with a scheme in the late 70s they went and they showed that even if, basically, the problem grows exponentially hard and it therefore you could make an assumption that if you were interested in securing a message for, say 25 years, this was an appropriate scheme.

Jesse: So how can my private key then, get compromised?

Miles: You could use, potentially, a device that does not exist, which is a gate model quantum computer and run an algorithm developed in the mid 90's and potentially, in a reasonable amount of time, find your private key from the public key. There's a lot of interest in quantum computing but it's all motivated by this algorithm and it's developed by Mr. Peter Shor.

Jesse: And when you say quantum computing I'm just picturing a really, really good computer. Is that...

Ben: Quantum computers differ from regular... The thing you need to know about quantum computers  is that regular computers can do one computation at a time, and they can do it really, really fast. But they can only kind of explore one possibility at a time. So, we were saying that it has to do with kind of like factoring large numbers. So if we say hey you can get the number 15 by multiplying two prime numbers together. Find those prime numbers. To figure out what that is you have to go through all the possibilities you can go like, okay, can I get 15 by multiplying two with any number so 2 x 3 is 6, no,  2 x 4 is 8, no, 2 x 5 is 10, no, and just going through all the different possibilities until you find one. And that's why it takes so much time because you start out with a really, really big number and they ask you to find the two prime numbers that multiply together to make it and it just takes forever. Quantum computers do all the different calculations at once.

Jesse: Right.

Ben: Like, it's like it turns into a thousand million different computers and then so one of them is going to figure out what the answer is in a reasonable amount of time. We're on the brink of developing better and better quantum computers. So, maybe in the future one of these quantum computers will get developed and then suddenly all of the secure transactions that we do over the Internet will be compromised because using the public key anybody can figure out our private key using one of these weird quantum computers. So, the deal is that physicists have come up with a method to use quantum mechanics, to create and communicate a one-time pad between two people that can't get intercepted. But to understand how we can do that you need to understand some of the basic properties of quantum mechanics.

Jesse: Oh good.

Ben: Yeah, I know, right? So, quantum mechanics, it was developed in the early 20th century, after we'd discovered that everything was made out of atoms we started figuring out the properties of these atoms. How they move, how they interact with each other. The very earliest models imagined that atoms were like these little billiard balls that would like fly together and if they hit each other they would clink and bounce off each other like a game of pool or something. But the deal is that over the course of the early years of the 20th century and ever since we've been doing research on it, it turns out that the rules governing the Universe, at it's smallest scales, atoms, the binding forces between atoms, the binding forces of the things that make up atoms, are governed by a set of rules called quantum mechanics that are really bananas. They don't really make too much sense in terms of classical physics. Sometimes in this case the billiard balls will pass through each other and not hit each other, weird, weird stuff. But, the deal is that a whole bunch of  new physical principles have emerged at these smallest scales that we can use to, essentially, do cryptography. Um, and the first property of quantum systems is something called entanglement. And the deal is that, you might of heard of, say, the conservation of mass that says, you know, in any physical system the total mass of the system has to stay the same, right?

Jesse: Okay, yeah, right.

Ben: So there are various conservation laws that govern the Universe. One of them is, say, conservation of electric charge. So, if you want to make, ah, something that have positive electric charge, if you want to build a particle or get a particle that has positive electric charge, you're going to make part of the system have negative charge to compensate for it. So, similarly there are things involving, say, the spin of a particle. If you make a particle with the spin going one way you have to make another particle spinning the opposite way. And say you smash two things together really heavily, a particle comes out of it that's spinning upwards, you'll need to make, simultaneously, another particle that's spinning  down. But you might capture those two particles, you don't know which one is spinning up and which one is spinning downwards unless you check. And until you check all you know about the system is that one of these particles is doing the opposite of what the other one is doing.

[16:20]

This system is called entanglement. When you know that one part of the system has to do the opposite of what the other part of the system is doing, that's called an entangled system  and

you can do a whole bunch of really clever things with entangled particles. Ah, but I like to imagine it in terms of, like, lunch boxes. So, you've got a  mom right and your mom makes your lunch for you. Presumably. You and your sister, you're both seven, your sister's about to go off to Spain or something. And she's made you and your sister lunches. And you looked at the kitchen counter that morning and you saw that there was a red apple and yellow apple. And you know that your mother put one red apple in one lunch box and the yellow apple in the other lunch box, and you're not sure which is which. Then you would say that those two lunch boxes, metaphorically they are entangled with each other. They both can't have red apples in them. They both can't have yellow apples. So, if you open your lunchbox, even if your sister's off in Spain, if you open your lunchbox and it has a red apple you know that her lunchbox has a yellow apple in it. You dig?

Jesse: I do. It's about inference.

Ben: Yeah, yeah. So, entanglement is really neat because it allows you to infer what's going on in a system that's potentially really far away from you without any new information based on what's happening in the system in front of you. You open up your lunch box and say hey, my particle is spinning up so I know the particle in her lunch box must be spinning downward.

Jesse: Yup.

Ben: Ah, Katherine do you want to talk about superposition of states a little bit?

Katherine: Yeah, I guess you're familiar with, in your computer, the data is stored in bits. So, your bits can be, either a zero or a one. So, it's a two state system.

Jesse: Yeah.

Katherine: With quantum mechanics we have something similar. So, we have something called a cubit or a quantum bit and the quantum bit has the interesting property that it can be in a superposition of zero or one but when you measure it it always comes out as either the zero or one. So, superposition is some bits being zero and some being one. This comes out to Schrödinger's cat  and you can see why the idea of superposition is counterintuitive. So, in Schrödinger's cat  you imagine there's a cat who's locked in a box and in the box you have a particle that
has 50% chance of decaying and a 50% chance of not decaying. If the particle decays it knocks over a vat of poison and kills the cat. And so, you have a 50% chance that the particle's decayed, knocked over the vat of poison and killed the cat and a 50% chance it hasn't. And until you open the box you have a superposition. So, you can't say the cat is alive or dead until you observe the cat and look to see if he is alive or dead. It's in a superposition of alive or dead. But, part of the point of Schrödinger's cat is that this doesn't really make sense. You are, either alive or dead, you can't be somewhere between alive or dead. And it shows really that quantum mechanics doesn't make sense on the kind of macroscopic, everyday life scale. But in the quantum mechanics you can be in the superposition of alive or dead, this is a key property that we use in the quantum cryptography. The other thing that's fairly important to understand is measurement basis. If you could imagine this, if you're talking to a member of the public, you can find out their political views. And you can ask them if they're socially conservative or liberal. You could also ask them if they're fiscally conservative or liberal and there's no reason why there should be any correlation between their answers so obviously they only have two states

they could be in, either conservative or liberal, but they might be different for each factor. And now, if you can imagine a very stupid voter who can only remember one thing at a time. So, if you ask him if he's socially conservative or liberal he can answer that question. If you then ask him if he's fiscally conservative or liberal he'll answer that question but he'll forget whether he's socially conservative or liberal and the next time you ask him the question he'll make up his mind again and he might change his mind. This is what's important in quantum mechanics is you have these variables where if you ask, measuring what we call a basis in one basis such as socially conservative then you can get a result. But if you then measure in the next basis which is say fiscally conservative, that actually can change your initial result. So that's basically what stated as Heisenberg's uncertainty principle, there are certain variables where we can't know both at the same time. This is illustrated in, there's a famous scientific experiment with photons. A photon is a particle of light your photon can - polarization and it can have any direction in this polarization at random. And you can pass several photons through a polarizer and the polarizer controls the direction. So if you pass it through a vertical polarizer it will only let photons that are vertically polarized through. And force everything else to either be blocked or actually go through as vertical. So, you can imagine passing, you know, a bunch of photons through this polarizer and if you pass them through randomly you'll get about 50% of your photons passing through the vertical polarizer. If, after your vertical polarizer you put on a horizontal polarizer, now the vertical and horizontal are opposite directions so, you can't be both, you're either one or the other. So, you get no light through.

[21:26]

An interesting thing that happens in quantum mechanics is if you put your vertical polarizer you use half your light. If you then put a polarizer at an angle, say, a 45° angle to your vertical polarizer you could loose another half, so you'd end up with about a quarter of the light. You could then put in a horizontal polarizer and you'd loose another half again, get it down to an 1/8th. So that adding this extra polarizer actually increases the amount of light you get out between the horizontal and vertical polarizer. So, putting this extra one in increases the amount of light you get out. And that's because these basis can't be measured at the same time. You can't measure whether it's horizontal, or vertical, or 45° at the same time and that's quite key to understanding the quantum cryptography because it helps us understand why we can detect when there's an eavesdropper.

Ben: So, the deal is, you've got your two people, Alice and Bob, and they live down the street from one another, okay? What the deal is, is Alice is going to be sending Bob a particle which is entangled with one of hers. So, all we imagine is Alice has a twin building machine that makes twins, right? You're familiar with twins, they have opposite opinions, right. So, she presses a button on the twin making machine and a pair of twins pop out. And they'll have opposite opinions from one another, okay. So, if you ask one, hey, are you liberal or conservative. He'll say, aw, I'm liberal. And then his twin will say well I'm conservative. Right?

Jesse: Okay.

Ben: So, the deal is, that what you do is you say, Alice, take one twin and she goes okay, I'm not going to ask you whether you're liberal or conservative yet. I just know that you'll have the opposite opinion of your twin. And he'll go yeah that's right. And you go okay. Walk down to Bob's house and Bob will ask you if you're liberal or conservative. And so he goes okay. And then he walks down the street and what they'll do is then, they'll do this over and over and over

for a certain number of times. Ah, they'll have five twins in a row and they'll be asking each twin, are you liberal or conservative. So, Bob will ask his, liberal or conservative? And the first guy will go I'm liberal. And then Alice, at her house, will ask the first person, liberal or conservative, and the other person will say the opposite, I'm conservative, right? Very straight forward. So, the deal is that there's this liberal or conservative axis you can imagine. It can be one or the other. But, imagine that somebody intercepts the twin. So, you've got Eve I guess, the interceptor, so she goes up to the twin while it's walking down the street and goes alright, I know that Alice and Bob are asking some questions of these twins and I know that if I figure out what the answers is I can figure out what the key they're using is so I'm going to go up and I'm going to ask a political question, she doesn't know if its a liberal or conservative, she doesn't know what question Alice and Bob are asking the twins so she goes up to the first one and asks do you think the government should go into debt? And the first one will be like, ah, that's a good question, um, let's see... And then suddenly the axis that it's thinking on won't be liberal or conservative, it will be thinking in terms of debt, no debt. And so, it might say I think a government shouldn't go into debt. Ah, suddenly, because it's come down hard on going into debt you switched it from its definitely one or the other to it might be a mix of liberal or conservative. So, the deal is that she's messing up the axis of questions that they are asking. The two, ah, the twin goes down the block and Bob asks hey are you liberal or conservative, it won't necessarily say the opposite of what it's twin is saying.

Jesse: Okay, I was with you up until Eve asking the leading questions to kind of deduce high probability if you're into debt I can deduce from that that you're liberal and therefore that your twin is conservative. That's where I last understood you.

Ben: So, the deal is, that she's not asking to figure out whether the twin is liberal or conservative, she's guessing that Alice or Bob are asking their twins whether or not they're going into debt or not. She doesn't know know which question they've been asking so she guesses at a question Then, her guessing at a question disentangles the two because suddenly this particle. This person could be liberal, could be conservative, them coming to a strong decision about whether or not they go into debt messes up. He stops being 100% liberal or a 100% conservative. Suddenly him answering one question changes his answer about liberal or conservative. Because maybe he was conservative  before and then they ask him if they can go into debt and he goes well you know... As he's walking down the block he goes yeah, I guess the liberal party is more willing to go into debt and I said that you could go into debt so... So it changes, it disentangles the two and changes his answer.

Jesse: Did I jump the gun on something? Is there any relationship between the two questions? Is one question meant to give you a clue as to the answer to the other question? Or...

[26:16]

Katherine: Ah, when you ask one question the person you've asked the question to completely forgets their answer to the other question.

Jesse: Right.

Katherine: So, a person can't have an opinion which is why you don't really have a good classical analogy and we try to come up with one, you can't really have an answer to both questions at the same time.

Jesse: But is Eve trying to figure out the answer to one question by asking a different question?

Katherine: No. So because Alice and Bob are randomly choosing between the two questions Eve can't know what question they are asking so she's trying to just guess what question they'll be asking.

Jesse: Right. Eve doesn't even know what she's trying to intercept.

Miles: Eve's ultimate aim is to try and get what will ultimately be the one-time pad that Alice and Bob will use for secure communication later.

Jesse: Which requires both question and answer.

Miles: Yeah, exactly. Eve wants to get as much information out of her measurement as Alice and Bob get out of the process. But Alice and Bob are asking these questions at random and Eve has to second guess this and ask these questions. And then these twins have this weird property where they are quantum bits and you ask them in one basis, you ask them one question, you can't simultaneously ask in the other basis, you can't simultaneously ask the second question. So, Eve's at a disadvantage because Alice and Bob are using quantum bits, or these twins in Ben's example.

Ben: So, um, the fact that Eve interacted with the particle and didn't know the types of questions that were being asked by Alice and Bob changes the outcome that Bob will get.

Jesse: Okay.

Katherine: So, what Alice and Bob are doing when they are talking to the twins is they are writing down their code so they are saying if the twin says he's liberal that will be my 0 and 0 is my code. If the twin says he's conservative I'll use 1. If he says he's pro debt I'll use a 0, if he says he's against debt I'll use a 1.

Jesse: Yeah.

Katherine: So, that code is, the code that they're sharing, is the twins answers to the questions.

Ben: Yeah so Eve intercepting it scrambles up what the answers going to be that Bob gets on his end.

Jesse: Right. Okay.

Ben: So it was, before, when they were entangled, if Bob got a 1 Alice would get a 0. If Bob got a 0 Alice would get a 1. But suddenly because Eve went in and asked them leading questions, suddenly they don't know what they are once they arrive at Bob's house. So, when Bob asks them ah, he might get a 1, Alice might get a 1 or they'll both get a 0. They won't match anymore.

Jesse: So the rub being that the act of, or the attempt at interception can scramble the encryption itself.

Ben: Yup.

Miles: Mmmhmm. And one of these protocols for doing this is called BB84. Ah, Charles Bennet and Gilles Brassard, in 1984 published this paper and they basically worked out a scheme where Alice and Bob can exchange entangled particles, measure in random basis, confer later, one of them just needs to send them the basis and then they can check for errors and if the errors exceed, it turns out, 11%, it's just how the math works out, they shouldn't be using that pad and they should start again. If it's less than 11% they are good to go. And it works. They can generate a pad from there and securely communicate.

Ben: So, the deal is that this method generates their pad, right? So, they don't know which, whether, the first twin going out is liberal or conservative. It will just be one or the other. And then, what they'll do is, Bob will ask, Alice will ask, and they'll end up with a string of numbers. 100101, right? And then Bob's will be the opposite 01 etc. Okay? And the deal is that after they've done it a bunch of times they're going to use that number to generate a pad, maybe, but they're not sure if somebody's been intercepting. So then Alice sends over the first half of her numbers, 1001... And compares it with Bob's and if they aren't opposite everywhere, I mean, there's going to be there's going to be a little bit of error in it, but if they don't match to a degree over 11% it means that somebody is has been intercepting the twin halfway down the street and asking them questions. It means that somebody else is intercepting their transmission and so they know that the code they developed this way might not be secure and so then they just start over and do something else. So, it's not just a method of generating one of these one-time keys, and a nice random way of generating a one time key, it's also a way of determining whether or not somebody is listening in between.

Jesse: Ahhuh, okay.

Ben: And if they haven't been listening then you can use that code, that one-time key to encode all of your regular information and send that straight, email them using that code and nobody will be able to break it because it's a one-time key.

Jesse: So, it's encryption that can actually test it's own strength.

Ben: Yeah.
Katherine: I have the caveat that the proof of security relies on perfect hardware which, obviously, doesn't exist. So, as far as the majority of commercial quantum cryptography systems on sale at the moment have, actually, been hacked by exploiting the weaknesses in their hardware and there's a group in Singapore that's dedicated to doing that. So, that's the negative caveat.

[31:30]

Miles: But, you can go out and buy a quantum communication system now and operate it over at least 140 kilometers in optical fiber and that number's probably five years out of date. You can operate at great distance, you can operate these things through the air, that sort of thing. The very first experiment to do this sent horizontal and vertical polarized beams of photons and the polarizer emitted a different sound if it was either horizontal or vertical. So, it was, you know, went 10cm, or whatever, and so it was secure over 10cm provided you were deaf. So... Trust me, it's been improved since. So...

Katherine: At the moment it's relying on the fact that there are two main weaknesses. It's the fact that you can't really easily generate two single entangled photons all the time, you often get more photons which allows Eve to do a certain attack. And the other one is the fact that your detectors can't always detect your photon so Eve can do attacks that make the detector think that hasn't detected something when it should have detected something and that's her other attack that she can use.

Jesse: Hearing the dates on some of the research that you guys are citing, this has been an area that's been under development a long time. Would I be correct in assuming that since the Internet the need for good cryptography and the entire financial system of the world and communications system now relies on this stuff working?

Miles: Mostly. It relies on good cryptography. It doesn't rely, necessarily, on quantum cryptography. You'd have to have a very specialized need for quantum cryptography.

Jesse: Is that just trying to get ahead of things, cause...

Miles: Yeah.

Jesse: Right.

Miles: People are playing around with this, I mean, these systems do have slight vulnerabilities. Um, and they're people trying to hack them. So, sometimes people playing around with them right now are just, they are purchasing the system in anticipation of getting to know how to use it and use it properly and to develop protocols around it. Because they want to constantly be ahead.

Katherine: You have to take into account these people are hacking the system so they know the weaknesses so that they're not in there anymore. They're not hacking a commercial communication - - communication and hacking it in the lab so they're communicating in the lab and hacking it at the same time.

Jesse: Sure.

Katherine: But they are there commercially. You could go out, if you had enough money you could go out and buy one tomorrow. So, they are, very much on the market now but as you say, you need a specialist system because you both need your little quantum channel between you. There isn't, as yet, quantum internet where I could send you a quantum message. We would both need to go out and set up a dedicated link.

Jesse: I see. Would I be correct in assuming that there are black hat operators and state operators who are doing the same research in the hopes of being ready so that as soon as everybody, should everybody switch over, they'll already have the hack, the keys, waiting for that day to arrive.

Miles: I filed an ATIP request on that but they haven't got back to me.

Laughter.

Katherine: I don't know, I mean, if I was the government I'd just be downloading research papers from the white hat hackers and save myself some money. But...

Jesse: I see.

Katherine: There's certainly no official release that I've heard of from the government saying they are doing that but.

Jesse: But there wouldn't be, right.

Katherine: You don't know what research they're doing, so.

Jesse: Okay, alright.

Ben: Well, that was wonderful. Thank you Katherine, thank you Miles. You've pleased me. Your efforts have born fruit and that fruit is sweet. Here is some fruit. Miles, you get a rambutan.

Miles: Nom, nom.

Ben: And Katherine, you get a kiwi fruit.

Katherine: Nom, nom, nom, nom, nom.

Ben: Yeah. Alright, I'd like to thank my guest, Jesse Brown, the host of Canadaland, thank you Jesse!

Jesse: Thank you. You too and a pleasure meeting you all over Skype.

Ben: Alright. Hey Ti-Phyters, listen I love this show and I hope you do too but for every listener of the show I know there's a hundred other people who would love to listen but they just don't know how. I want you to spread the word and there are three ways you can do this. First, there's the iTunes. iTunes is still the biggest place to go around and find new podcasts and iTunes puts the shows with the most ratings at the front where everybody can see them so if you've got a minute give us an iTunes review. It will increase our rank and more people will see us. The second is to teach people how to listen to podcasts. Everyone has a smart phone or tablet these days and a very low percentage of them know how to use podcasts. So, if you have somebody who might like the show tell them that there are easy, fun ways to listen to podcasts. Point them to the Stitcher app. It's free and easy and works on other devices. Alternatively you could point them to Podiversity which is a podcast app and it's curated and it chooses the best podcasts for you to listen to. And it's easy to use on Android phones. The third way to spread the word is tell people online about us. The Internet is full of explanations about physics, if you see someone on the Internet talking about a topic that our episodes cover post a comment telling them about the show.

Okay, so that's it. I hope you'll help us out and point new listeners in our direction. That's it for the main show. Remember, if you like listening to scientists talk about science in their own words you might also want to listen to other shows on the Brachiolope Media Network like the Weekly Weinersmith or Science Sort Of or Astrarium or Technically Speaking. The intro song is

by Ted Leo and the Pharmacists and the end song is by John Vanderslice. Until next time my friends remember to keep science in your hearts.

[37:34]

Jesse: Can I ask like a dumb question? How do you arrive at any of this? Like, how do you measure, or... How is physics done? I can understand if people coming up with formulas when they're actually watching billiard balls slam into each other, and observing the affects but when you get into what happens in the space between atoms, how do you figure that out?

Ben: Yeah, okay, so part of it is we've been bootstrapping ourselves up. So, early in the 20th century we could only consider very simple systems right? So, you'd look at a very simple, you'd take a piece of iron and you'd throw it in the fire and it would heat up and it would just be a big ball of Iron. Very simple system. And then you would look at how it emitted light and what color the light that came off it was. And you'd try to build a model describing it or you'd look at a cup of water and you would look at, say, how little grains of dust bounced around inside the cup of water. Because they're getting, presumably, knocked back and forth by little atoms and so you can glean information about that system off it. And so we started off very simple systems or what you would do is you would fire electrons at a big sheet of metal and you would look at, after the electrons hit the metal, what they would do. So, you would look at very simple scattering problems. And so from that you would develop a system of, you know, laws.

Jesse: That was a huge leap from a dust in the glass, in the water but alright...

Ben: I mean, they discovered...

Jesse: Just shoot some electrons...

Ben: I mean, they discovered radiation around that time and so they were like, hey, we know that little, really fast moving particles are moving off this, let's what happens when it bounces into this other thing. And so, so, what happened is technology has kind of been bootstrapping our way though this. We'll develop a set of technologies that will let us study nature at some scale, at some energy say, and then we'll develop laws and those laws will let us develop slightly better technology like the ah, like the transistor, right? And then your technology will get better and you can understand, you can fire, smaller particles at each other at higher speeds and then you can develop technology that kind of senses where the particles go. The deal is that over time we've come up with better and better ways of seeing where the particles go, how fast they're moving and better schemes for firing particles at each other. So, the answer isn't simple, it's changed over the years. Ah, like, early 20th century there was a lot of, you have to do an experiment and look at really subtle things to deduce what's going on on the inside. And now we have the capacity to fire really heavy objects at each other and smash them together and see what comes out. And we have really complicated detectors. You've seen the photographs from the CERN particle detector, right?

Jesse: Yes.

Ben: The Large Hadron Collider, right? There's that big octagonal shaped, it looks like a giant pencil sharpener, right?

Jesse: Yeah.

Ben: That thing is to see what happens when you fire, two nuclei get fired, they have a ton of energy, they have... they get accelerated and they smash into each other. Tiny little effect, that big, giant octagonal thing is just to measure what happens when two of these nuclei smash together. So, the answer isn't subtle and it's not simple. Um, it's kind of, technology has marched in progress with our ability to study these things. There's no simple answer to your question.

Jesse: No, that's helpful. Thank you.

Ben: Right. It's not like we're just imagining it and... There's experiments going on. The theories get bootstrapped along with the ability to do measurements. And then our technology gets increased by our theoretical understanding of nature.

Jesse: Gotchya.

[41:12]

Ben: Do you know anything about quantum mechanics Jesse?

Jesse: I do not, no.

Ben: Okay, that's fine. Ah, most of the time, when somebody from the public says they do know quantum mechanics they take out a piece of crystal and they say that they are beaming healing waves to their mother using quantum mechanics.

Jesse: I mean, I do, I am surrounded by my crystals and I am using them to beam waves to my mother but I don't have the...

Ben: Well, then you do know some quantum mechanics.

Jesse: oh good, okay.

Ben: Fantastic! Oh, awesome. Okay. So, ah...

Laughter.

Jesse: And PGP, is that pretty good privacy. That's what people use to protect their email. Is that a public key form of encryption?

Miles: As far as I know it is.

Jesse: So, a day will come when that and everything that people thought was protected, at that moment, cracked. Is that...

Miles: Yeah. But don't forget, you'd have to spend a lot of money so... Potentially somebody could do it but how likely is it somebody is going to go back 25 years to crack somebody's

personal email. You do design crypto systems such that you say I want this protectable and then you consider for how long. And ah PGP is vulnerable to future attack if someone had a quantum computer.

Jesse: I'm just thinking of this in terms of when journalists get their hands on, you know, like an access to information request finally comes through and something is released to the public domain and there's not going to be some magic day day when troves of secret information and private information suddenly becomes public.

Miles: Not in the sense that the British, they wait a certain amount of time, 25 years and they release the secrecy orders and things like that.

Jesse: Nothing like that.

Miles: Yeah, no.

Jesse: Because you've got individually point this at each type of...

Miles: Yeah

Jesse: Communication you're trying to decode.

Miles: Yeah.

Jesse: Um, help me out with this because I'm, I've covered this and it's sort of an unfortunate aspect of covering technology and not being a technologist to not really understand the guts of the stuff you're talking about as you report on this but... I covered the story of the NSA encryption that, or rather the encryption that the NSA was able to find a back door to decrypt with the acquiescence of CSEC in Canada. Ah, how does that work when everybody is, you know, I have kind of like a very simplistic understanding that there's a key that everybody thought was secret but America had it and was spying on everybody the whole time.

Miles: Yeah, that is certainly, I shouldn't say, yeah. Yes. As far as I understand that related to something called elliptic curve cryptography which basically has this notion of a pretty good one way function. That it's pretty hard to work to compute in one direction but easy to compute in another. How that actually played into the NSA having a back door. Basically, they would have either access to or knowledge of the private key. Um, so, they may have actually known the private keys or they may have had a scheme which was just easier to find the private key. Um, elliptic curve cryptography is very complicated and one could imagine, actually, them proposing a set of protocols for elliptic curve cryptography in which recovering the private key was not as hard as people would have hoped it to be. When I say people, the people securing the message would have hoped it to be.

Jesse: Had they been using a one-time pad encryption would they have avoided decryption from the NSA?

Miles: Yes. You would have had to gone to physical means to actually get the message. You know, breaking into the black bag jobs. You know, breaking into places and stuff like that.

Jesse: So, why are, why are like international standards organizations and countries constantly developing new encryption schemes if the possibility of some back-door access is there when they've got a perfectly good solution in the one-time pad?

Miles: Ah. Well there, I personally think public key cryptography is a wonderful tool and I work for a company that develops quantum computers D-Wave Systems and so I personally feel that the rate at which quantum computers will be developed is so slow that you can always increase the key length for public key cryptography such that anybody's messages will be secure. I would secure my own personal. I use, you know, I use Internet banking, I am securing my financial information through public key cryptography. I would secure my own health information and I would trust dissidents in, you know, a country, organizing a revolution against a dictator to use public key cryptography. You can make the key's length so long that you have to have a very large supercomputer working for about the age of the Universe to crack them. You could always, to make a quantum computer just a little bit bigger, takes billions of dollars. To make a key just a little longer takes, you know,  it's trivial. So...

Jesse: This is the difference between 64 bit and 128 bit...

Miles: Yeah.

Jesse: It's just a longer string is the key, so you're, you double that and it's going to take decades longer to create a computer that's able to deal with it.

Miles: Yeah. So, these organizations are, for the purposes of protecting people's information, doing good work. It's definitely not a fool's mission. They're being very pragmatic coming up with good, usable standards that will thwart a - on a computer.

Katherine: I think the other question you probably want an answer to is what is the problem with one-time pad. And the problem is you need to somehow securely transmit the one-time pad. So, you end up with the say problem. So, if you're transmitting a 128 bit message you need a 128 bit one-time pad. So that you've got to transmit your 128 bit message securely you need to transmit another 128 bit message securely. So, the problem with, basically, the problem is you get back to your original difficulty. You have to somehow transmit your one-time pad securely which, if you don't have a way of doing that, is the same problem as transmitting your message securely.

Jesse: Right, right. Okay, so, that explains it. Thank you.