#221 - Microsoft Majorana is Taking the Quantum Leap

[00:00:00] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host for today, and we're going to be talking about Microsoft's Quantum Leap.

INTRO

[00:00:26] **G Mark Hardy:** Hey, the week that I'm recording this episode, Microsoft had introduced Their new quantum chip, the Majorana, it's a microprocessor that's supposed to harness the properties of some elusive material called a topological superconductor.

And it's a particle that's neither a liquid, nor a solid, nor a gas. Now go tell that to your high school physics teacher and see how well that works. Anyway, I'm going to try to get into a little bit about what the announcement means, what it consists of. And I'm going to try to revisit some of my physics courses, and I'm sure I'm going to get some stuff wrong.

So feel [00:01:00] free to go ahead and respond in the comments and tell me how I can straighten out my knowledge. But hopefully I put enough in here that goes a little bit beyond just the press releases to get your head around what's going on here. By the way, if you like our podcast, Make sure you're subscribing to us.

We're on all the different channels that obviously you're listening on. We're on YouTube. Follow us there. Follow us on LinkedIn. We've got a lot more than podcasts to make life interesting for you. let's go take a look at this Majorana and this release from Microsoft that came out, okay? It came out on the 19th of February, 2025, and they're talking about some subatomic particle that, up until last year, was just theoretical.

But now, not only is it observable and controllable, they can build an entire structure around it. Wow! And the idea is, and the promise, they can scale this concept of quantum computing to millions of qubits or quantum bits on a single chip. not yet. So I'll talk a little bit about what a quantum bit is.

Some of you may know already, but I'll, get into all this stuff. And what a quantum, I'll just do it right now. So a quantum bit suggests [00:02:00] one, that on a typical bit in a computer, it's got two states, zero or one. A quantum bit exists in a way that it's zero and one at the same time. how is that possible?

it relies on, quantum computing, which we said is weird. And, I think it was Richard Feynman who said, if you think you understand quantum computing, you do not understand quantum computing. And I feel a little bit better about that statement because of all the courses I took at the university, my undergraduate and even graduate level, it was the one thing I just didn't quite get.

how could something be true and false at the same time? How could it be one and zero at the same time? But in the quantum world, things get a little bit weird. Now they don't exist in normal everyday. Motion. You have to get really cold and really specialized and things like that. But the whole idea is what?

The concept of quantum computing suggests that if a value can be 1 and 0 at the same time, then that means that if you have enough of them strung together, that all possible values exist. So if I say pick a number from 0 to 1023, Okay, there [00:03:00] would be 10 bits involved in that. 2 to the 10th power, and therefore I should be able to represent that.

If, however, I have quantum bits, I have 2 times that, or 20 quantum bits, because I have a pair of them, one says a zero, the other one. And imagine this quantum soup. And somewhere in the quantum soup, all possible values exist at once, so if I could reach in there somehow and magically read just the right information, I've got the answer.

one of the things we worry about in cybersecurity is that about cryptography, and specifically symmetric cryptographic algorithms. Symmetric cryptographic algorithms? We're safe. You're good. Asymmetric algorithms, however, could be a problem. Biggest difference in symmetric, we have a key that we share between the two entities.

And usually these symmetric algorithms are iterative. You go through like DES or AES, you go multiple steps and things like that. And quantum isn't going to help you because you can't have it do different things. But asymmetric key Like a Diffie Hellman key exchange, or RSA, where I'm using [00:04:00] large prime numbers, and I have two large primes that are multiplied by each other to get to one ginormous prime.

if I know one prime and I know the ginormous number, I can do a simple division and get the other one. But, if all I see is that ginormous number, trying to go ahead and figure out what those prime numbers that go into it Would be one heck of a mathematical problem. One that we estimate would take all the conventional computers on the planet billions of years to chew.

The idea of a quantum computer, though, is that if you can get enough quantum bits to be stable and to behave themselves, that you should be able to reach into that quantum soup and then pull out just the right answer. And we've been able to do and we keep hearing over time that, hey, next year is going to be the year of quantum.

And this has been going on for about 15 years. Right now, we may be up to about 150 quantum bits. But Imagine if you had 150 bit computer, how much work could you do? that's your storage, right? you're like, wait, I need something bigger. And so what we're talking about here is Microsoft's promise to create a technology that could [00:05:00] scale to millions of qubits or quantum bits on a single chip.

But that's not what they're announcing. They don't have that right now. And right now, I think other companies have said, yeah, we can do about 150. stable, but think about this. If you're using RSA, what's your key link? Because if you're using an old key link of 768 or 1024, maybe even 2048, bits is sometime in the next few years, quantum computing may be able to go ahead and split that thing into two.

You're not to worry about it now because you'll change when that happens. Your adversaries are already recording all of these conversations, the key exchanges. And granted 99. 9 percent of what you say and do today would probably be of no use to anybody in five years from now. But if you happen to be logging into your Bitcoin wallet or you happen to be doing a national secret or something like that, it could still be valuable.

So you ought to be moving to post quantum crypto now. All right. Enough of a little ad for that. So let's go back and I'll try to go ahead and do my best I can with the physics of what's going on. [00:06:00] So it looks like now Microsoft has leapfrogged Google and Nokia on their concept of topological quantum computing.

Although those companies are pursuing some other technologies, we're trying to figure out what's going to get us there first. The idea of a topological property, it's as a property of interacting particles. But when you interact particles and

their features are conserved, that is to say they're not going to change each other and you can go ahead and they'll be stable.

It's reasonably robust against noise. The biggest problem with quantum computing is that the act of reading it tends to change the values. Okay. It's a little bit of Heisenberg uncertainty principle that's involved in there. And we're not going to get too deep into the physics, but essentially you can know what it is or what it's doing, but you can't do both.

Now, the concept of a topological state here, they're talking about a Majorana zero mode. What's that? The idea of a topological superconductor, topological meaning you have substrate or laminates on top of each other, isn't a new idea. It's not a new technology. [00:07:00] And some object to even calling it a new state of matter, like Microsoft is saying.

It's something different. Now, important to note, this is not a fully functioning computer. This is not something you can go ahead and plug in and do your taxes on. It's really the first step. toward a production quantum computer, and that in and of itself is valuable. And the premise here is that you can shorten complex problems that, today, are beyond the scope of all the world's computers, using all the remaining time left in the universe to solve.

what are the challenges? first of all, you've got to remember, this thing will not run on your desktop. Even if you're up in North Dakota, it's not going to run on your desktop. It has to be cooled to nearly absolute zero, minus 273. 10 degrees Celsius. Now for those of you who remember trivia, you say, wait, absolute zero is minus 273.

15. it runs about 05 degrees above absolute zero. So you have to cool that thing down, meaning that the apparatus to cool this chip is going to be immense, even though you've got a little tiny chip right in the middle of it. [00:08:00] Microsoft talks about the concept of materials having defined our culture over the years.

We had the Stone Age, and then we progressed to the Bronze Age, the Iron Age, and then Silicon Age. And in our Silicon Age, we started out with vacuum tubes. As we got better with that, we moved toward eventually the transistors. And transistors, by combining them, we got on the integrated circuit.

And now we're really into quantum. Now this may be the first generation quantum, and it probably doesn't necessarily have the right properties that we need to solve all the world's problems, just like the very first vacuum tubes that were developed didn't end up becoming state of the art, or the transistors that

came out didn't end up state of the art, or your first IC, We didn't still keep using the old 8080 chip, for example, we got better and better.

But quantum development has been slow. And the part of the problem is these quantum bits or qubits are not reliable. And they're subject to noise, they're subject to interference, and they're very delicate. They die off very quickly. They lose their state. So you want some stability. And it'd be great if you could go ahead and make them stable, [00:09:00] but you can't make them huge because how are you going to put a million of them if they're the size of a basketball?

You want them really tiny. And then, of course, you could slow things down a little bit to make them more stable, but then you want to solve a problem perhaps in minutes, not in years. Now, Microsoft had pointed out that this is their longest running research project, going at 17 years. That, to me, is fascinating.

In a world where most companies are driven to their quarterly earnings reports, and they will sacrifice whatever they can to make the numbers look good, the fact that Microsoft has got something going for 17 years, it is finally now showing some serious results. That's, very impressive. so thumbs up for them.

Now, how about a little quantum about quantum? if you think about a quantum state, let me give you an a, an analogy, like an employee. So if I think of all the impossible information on employee, who's their superior, what's their health care plan, their assigned projects, what team are they working on?

what type of after [00:10:00] work activities they prefer and things like that, we could catalog that, but until you actually talk to the employee, you won't know exactly what assignment they're working on in any particular day. And similarly, a quantum state is like a full profile of a particle that tells us all the probabilities for all the different things you could measure, like its position, its energy, or its spin.

But until you actually measure it, you don't know. Now, if you ask it, go to the employee and say, Hey, what is the primary project you are working on today? You'll get one answer. And that specific answer is like a property of a particle when you measure it. If you're measuring electron spin, it could be a result of up or down, or plus one half minus one half, depending on how you want to do it.

But the act of measuring is going to pick one of those possibilities that the quantum state describes. Now, the key difference in a quantum state is that it's

all the possibilities, it's all the outcomes, as we've talked about in this quantum soup, where all the answers there are once, as compared to a single A measurement which would say, hey, here it is, its spin is up or down, or [00:11:00] it's positive or negative, or it's left or right, or something like that.

And so from that perspective, when we look at quantum entanglement, you end up with two particles where they will be, if you will, opposites of each other. And classically, if you had one, if this is a one, that's a zero, and this is a zero, that's a one. the act of measuring one defines the other. And so if you can get spooky action at a distance, I think as Einstein used to call it.

You could have things that are separated by a significant difference if they were initially developed as quantum entanglement. Here's the interesting thing that we're looking at here is that Microsoft has said that we don't have two different things, but we have two of the same. let's progress a little bit and try to decompose what it might be.

If we go back to our basic high school physics class, we'll learn that a Matter could be a solid, or a liquid, or a gas. Now a solid, it's going to keep its state. If it's solid and you don't change the temperature or the pressure, it just stays there. It just sits there. A liquid, though, will go ahead, it will keep their volume.

You [00:12:00] can't really compress a liquid, which is why hydraulic brakes work, because when you push pressure here, the liquid doesn't go squish in like that, but it goes down there. An air or a gas is going to expand to fill the volume, which is why air in your brake lines is a problem, because if you've got a big bubble there, when you apply pressure, it just compresses the air.

Gas that's in there. It doesn't push the brakes down there and life gets really exciting now There's other properties that could change because if you go ahead and you change the temperature you change the pressure You can go through what's called a phase transition. If you take, ice, and you increase the temperature, you can get water, and you keep increasing the temperature, you'll boil it, and you will get steam.

Now, if you add pressure, it's gonna change the state, which is why an ice skate works. You put all that pressure on an ice skate from the weight of the skater, and that pressure turns that ice into a little thin coat of water, and so you're literally running around on water, which immediately freezes right afterwards, because, that Goes away.

So that's your typical thing you have. You [00:13:00] have phase transitions, but it's discontinuous. They go from one to the next, one to the next, and there's a transition. So ice melts over time, and therefore you have a certain amount of energy that's in there. other things they could have on properties. You could have particles that have a magnetism.

Some could be conductive, some are not conductive, some are super conductive, and things like that, where they don't dissipate any current. And The quantum state that we're looking at is some interacting particles. Now I'm going to dive into the physics a little bit. this may be too much, but I thought it was fun researching it.

So bear with me. And normally electrons repel each other, right? Because they both have negative charge, and it's yeah, we don't get along too well. But in certain materials, at very low temperatures, electrons can, pair up, even though they naturally want to stay apart. And these pairs of electrons are called Cooper pairs.

And what happens is you have a material where the atoms are arranged like a lattice, And if electron moves through there, it could pull the atoms a little bit toward itself. As you remember, the [00:14:00] nucleus is going to be positive, electron is negative. Creates a little ripple, they call that a phonon.

Another electron can say, I'm attracted to that. And then all of a sudden you've got the two electrons joined as a single pair. Now, once they're paired, these two electrons behave more like a single entity than two separate particles. Now, normally electrons are fermion, which means they'll follow rules that will keep them from being in the same state.

as another electron. Okay, if you've got two electrons though that form a Cooper pair, their combined behavior makes them like a boson, which is unlike a fermion, boson can all have the same state. So think for example a regular electron, is going to have certain characteristics and a neutron is going to have different characteristics.

Yeah, it's into the details, but bear with me. when you get into superconductivity, the thing is, that these Cooper pairs can move together as a very, almost frictionless way, which is where you get the superconductivity, no loss of signal, so to speak. [00:15:00] And that's why electricity can flow without any resistance.

And this is what we call superconductivity. And Here's an example that I came up with, actually I'll admit on this one. I actually looked at ChatGPT for a good example that I could explain. So I will confess to that because normally I just write all my episodes myself. Like I said, if any of the electrons like individual dancers on a crowded dance floor, they might bump into each other, call it's chaos.

But when they form Cooper pairs, it's like couples that they join together, maybe like even a long conga line, they'll follow each other around, so they're not going to bump into each other. they'll have a very efficient and energy saving performance. And so Cooper pairs of electrons move together the same quantum state.

So you've got two things that are the same, which is odd, and it will carry this current without dissipating. So at this really low temperature. Although a single electron can have a spin of one half, a Cooper pair of electrons can have a total spin of zero, plus one half, minus one half, or one plus one half, meaning the wave functions are symmetric.

If you exchange [00:16:00] particles, you get the same thing. And so multiple Cooper pairs can be in the same quantum state. These two possible states can store information, and this is how you get quantum computing. if you apply a small voltage. You can go ahead and potentially detect whether or not there's an odd electron in there.

It's called a Majorana mode. And that unique electrical signal says that, hey, there's something out there. a Majorana zero mode, which is half an electron. Pretty weird. And as you build more complicated devices, you can have more of these things on different wires. You can get superposition, and you can do some really cool tricks with quantum processing.

Now. All right, almost done with the physics, although I might dip back into it one more time because I still want to understand this stuff. Four years later, I'm still trying to figure out my undergraduate, right?

Microsoft's research was supported by DARPA, the Defense Advanced Research Projects Agency, the government agency that's tasked with funding a lot of these research for national security applications. And the [00:17:00] idea was that a particle could be its own antiparticle was an unusual theory. It doesn't make sense.

You have an electron and a positron or things such as that. But the idea is what? Maybe there is something. And for the first time, This Majorana particle as they coined it, was observed in 2024 and Microsoft to say, Hey, we're gonna create a topological superconductor or a topal conductor, which is going to be a semiconductor that mimics a superconductor.

Now you get into the materials in here, the details in Indium arsenide with a semiconductor with aluminum superconductor, and which you do is you end up as a laminate. And it creates a little energy gap. And so you don't end up using electrons for computing. You use these Majoranas. Basically the equivalent of a half electron.

These zero states that go through. And now you combine that with a classical computer that can go ahead and send out instructions. Then quantum computer does its thing, you get the results back out. That's pretty bizarre. I said Microsoft's been doing this for [00:18:00] 17 years. And they published this out on a peer reviewed paper that went out in Nature this past week.

So if a quantum bit can be 0 and 1 at the same time, how about this Majorana 1 chip? Can you really do a million at the time? right now it only holds 8 qubits. But they said it can be expanded to a million. It's difficult to do this. As they say, the material engineering challenge, they solved that by combining indium arsenide with aluminum and make it a nanoscopic wire, get it down to nearly absolute zero, about 0. 05 degrees Kelvin. And that's where they were able to observe these particles. They called Majorana particles. And these seem to be less error prone. In fact, Microsoft estimates that their error probability of detecting these is only about one percent. If you want to read about the physics, go do I came up with a whole bunch of stuff about anyons and their quasi particles observable in only two [00:19:00] dimensional systems.

And it read about braiding and you know what, that's just too much in a billion groups. I remember that from my math class. So I'm going to skip all that. Lucky for you. So we have a shorter episode. How about this Majorana? Where'd that name come from? Who's this Majorana person? So Ettore Majorana was a theoretical physicist born in 1906 in Catania, Italy.

And he was a gifted mathematician. He did early work in atomic spectroscopy. Relativistic Theory of Particles. He was really the first person to predict the existence of the neutron, although he did not publish his work. James Chadwick did later that same year, and he got a Nobel Prize for that.

He said that he really didn't care so much about getting honors and stuff. You also hypothesize the existence of a fermion. Remember that things could be like an electron to different states, but it would be its own antiparticle. And that's unusual that, how could that be? It would have to be an electron positron, things like that.

Anyway, he [00:20:00] disappeared the year he became the full professor of theoretical physics at the age of 32 at the University of Naples. He bought a ticket to travel by ship to Naples, to Palermo, and nobody ever heard from him again. And they really don't know what happened to him. They've done some investigations to figure this guy out.

But because he was the person to say, Hey, I think this thing might exist. And now going from 1937 all the way up to 2024, they said, Hey, we found it. He gets the name. So that's where he came from. So what can you do with these things? Some of the applications are to, of course, augment AI capability. The idea of a quantum AI computer sounds a little bit frightening, but also sounds like it could be incredibly powerful if and when they get it working right.

The other thought, though, is that you can model some of the laws of nature. Nature is almost a chaotic system. Weather prediction, very difficult to do in longer term because there's just so many variables that are out there. But imagine that you could put this thing to work on that. You might be able to have a much more accurate model and not just guess how many hurricanes you are.

Going to [00:21:00] happen a year or go look at the Old Farmer's Almanac to see how bad the winter is. You might be able to mathematically calculate that based upon a whole lot of information. self repairing construction materials, potentially designed. Accelerating drug discovery, being able to fold proteins, do all kinds of things like that.

The thought is that if you can do some of these calculations completely accurately without having to guess, you don't even have to do the experiments. You know what it's going to come out with because you've already modeled it and you've been able to say this would work. But of course, for us in the IT security world, the biggest concern might be stronger codes, and maybe breaking non quantum resistant codes.

As I alluded to earlier in the show, if you have not looked at your quantum resistant algorithms, you should start doing so. And you should also ensure that you are able to swap out your algorithms without a whole lot of difficulty if it turns out that somebody discovers a vulnerability with what you're using.

Who else is out there? What's the competition? NVIDIA. their CEO, Jensen Huang, had said just last month that, [00:22:00] useful quantum computers are at least 15 to 20 years away. And, of course, that tanked the stock quite a bit. People saying, wait a minute, why are we bidding up right now? And, of course, DeepSeek came along and that shaved about 600 billion off their stock.

So there's a lot of stuff going on out there. Microsoft. Announcement came after Google had unveiled its own quantum chip they called the Willow, and Google says this chip could make a calculation in five minutes that would take a conventional computer 10 septillion years, albeit for some little problems with use cases, but they're getting there.

That was a very specific case, but it's a proof of concept. Now Google says is it lower the error rate by Grouping the qubits in a special grid foundation and Microsoft says they only came out with a different workaround going ahead and using these special types of capabilities that we're going to build in terms of the materials engineering, which is The semiconductor iridium arsenide and superconductor aluminum.

So we're still trying to figure out what is going to actually work correctly. and Intel and IBM are [00:23:00] also racing to develop their own quantum computers. the Chinese government has committed over 15 billion to go ahead and get involved in that. and also remember that, there's a publishing.

A paper published in 2018 entitled Quantized that was retracted back in 2021. that was a Microsoft paper, and that was a little bit of embarrassment when they came out with that. And they said, it turned out you cherry picked the data, and that really wasn't proof. One of the advantages, if you will, of peer reviewed papers is somebody else takes a look at it.

So this may or may not be the way forward, a Schrodinger's calf problem. Because there's paper states, and I quote from it. These measurements do not by themselves determine whether the low energy states detected by interferometry are topological. Is it or is it not? I don't know. I guess we'll find out.

It is a definitive breakthrough. Yeah, to a certain extent. But it's not going to translate into big revenues for Microsoft for quite some time. I don't think it means sell your house and buy their stock. Although Microsoft has [00:24:00] done quite well. But what are the next steps? They're going to make more complex devices.

And they're trying to get better at the error correction. having a qubit right now is a little under 10 microns in size. You can't make it too small because then you can't connect a wire to it. You can't make it too big because then it becomes unwieldy. So it's one of these three bears problems where you don't want to pop a bear, you don't want a baby bear, you want it like just right.

And a lot of thought is that it'd be really surprising if this were it. What do First generation of anything usually ends up not being the standard. we ended up with Vacuum tubes, but they progress. We ended up with transistors, but they progressed. Integrated circuits progressed. In fact, it's interesting.

I'm not going to get a political debate. we say, Bitcoin, that's version 1. 0 and that came out back in 2008 and still the standard. We'll see. But who knows what's going to happen. But Microsoft says, hey, by 2030, we might have 100 qubits available to our cloud customers in Microsoft Azure and give you something to [00:25:00] play with.

Okay. So for those physics majors out there, if I went ahead and I bungled everything, give me some comments in LinkedIn so I can improve it. I'll put myself on a remedial study program. I have some stuff on quantum physics. It was interesting. I got a book from David Bohm, who had written a book on quantum physics and it's back here

on quantum theory. And I found out that going ahead and reading this, in spite of the fact that I had a degree in mathematics, if you go ahead and take a look at the contents, it is all advanced in mathematics. And you know what? It's going to take me a few years to study to get back up to understanding what this is.

So maybe this will be my retirement project to be able to get my head around this and someday. But meanwhile, your project is to go ahead and understand a little bit about the implications of this. So how do we summarize it? Does Microsoft come with some interesting breakthroughs? Yes, it's more interesting and from a physics perspective, I think, than a [00:26:00] calculative or computing perspective, because you can't use the thing right now, you can't buy one.

Also not going to fit in your desk, it's going to fit this gigantic cooling system that's going to go ahead and super cool all the way down to about 0. 05 degrees Kelvin, which is quite cold. And We're not even sure that this is the right way forward because there's competing technologies to get to quantum, but we're getting there and the whole idea of not taking time to provide quantum resistant capabilities for your cryptography is a bad idea.

I would make that a priority. I would go ahead and look at the algorithms that you are using in terms of key exchange. Make sure that you take a look at NIST has come out with some quantum resistance. Algorithms, look at implementing those, and in general, make it so that your cryptographic key exchange processes could be interchanged, so if you find out that there's a vulnerability, you can rip it out and replace it.

will we have quantum computing in our lifetimes? I hope so. I hope I lived long enough, and maybe I [00:27:00] will based upon what we're seeing in progress. But also think about what types of problems We might be able to solve, not only could we go ahead and create great new drug discoveries and solve for things, but there's potential that it can be used to develop really, nasty weapons and things such as that as well.

So like anything else, the technology itself is neither good nor bad. It's how we use it. And maybe that's just the quantum state of how things are. So thank you very much for listening. This has been CISO Tradecraft. I hope you found something useful in this episode. If you have, give us a note. We're on LinkedIn.

We're also on YouTube and we're on most of the regular channels that are out there for podcast transmissions. And if you have any episodes you'd like us to talk about, let us know. We'd love to hear from you. Until next time, this is your host, G. Mark Hardy. Stay safe out there.