Here is the full text of cryptography researcher Craig Costello's talk titled "The promise and peril of our quantum future" at TEDxSydney conference.

Craig Costello – Microsoft Research

I'm in the business of safeguarding secrets, and this includes your secrets.

Cryptographers are the first line of defense in an ongoing war that's been raging for centuries: a war between code makers and code breakers. And this is a war on information.

The modern battlefield for information is digital. And it wages across your phones, your computers and the internet. Our job is to create systems that scramble your emails and credit card numbers, your phone calls and text messages — and that includes those saucy selfies — so that all of this information can only be descrambled by the recipient that it's intended for.

Now, until very recently, we thought we'd won this war for good.

Right now, each of your smartphones is using encryption that we thought was unbreakable and that was going to remain that way. We were wrong, because quantum computers are coming, and they're going to change the game completely.

Throughout history, cryptography and code-breaking has always been this game of cat and mouse. Back in the 1500s, Queen Mary of the Scots thought she was sending encrypted letters that only her soldiers could decipher.

But Queen Elizabeth of England, she had code breakers that were all over it. They decrypted Mary's letters, saw that she was attempting to assassinate Elizabeth and, subsequently, they chopped Mary's head off.

A few centuries later, in World War II, the Nazis communicated using the **Enigma code**, a much more complicated encryption scheme that they thought was unbreakable.

But then good old Alan Turing, the same guy who invented what we now call the modern computer, he built a machine and used it to break Enigma. He deciphered the German messages and helped to bring Hitler and his Third Reich to a halt.

And so the story has gone throughout the centuries. Cryptographers improve their encryption, and then code breakers fight back and they find a way to break it. This war’s gone back and forth, and it’s been pretty neck and neck.

That was until the 1970s, when some cryptographers made a huge breakthrough. They discovered an extremely powerful way to do encryption called “**public-key cryptography**.”

Now, unlike all of the prior methods used throughout history, it doesn’t require that the two parties that want to send each other confidential information have exchanged the secret key beforehand. The magic of public-key cryptography is that it allows us to connect securely with anyone in the world, whether we’ve exchanged data before or not, and to do it so fast that you and I don’t even realize it’s happening.

Whether you’re texting your mate to catch up for a beer, or you’re a bank that’s transferring billions of dollars to another bank, modern encryption enables us to send data that can be secured in a matter of milliseconds.

The brilliant idea that makes this magic possible, it relies on hard mathematical problems. Cryptographers are deeply interested in things that calculators can’t do. For example, calculators can multiply any two numbers you like, no matter how big the size.

But going back the other way — starting with the product and then asking, “Which two numbers multiply to give this one?” — that’s actually a really hard problem.

If I asked you to find which two-digit numbers multiply to give 851, even with a calculator, most people in this room would have a hard time finding the answer by the time I’m finished with this talk.

And if I make the numbers a little larger, then there’s no calculator on earth that can do this. In fact, even the world’s fastest supercomputer would take longer than the life age of the universe to find the two numbers that multiply to give this one.

And this problem, called “**integer factorization**,” is exactly what each of your smartphones and laptops is using right now to keep your data secure. This is the basis of modern encryption. And the fact that all the computing power on the planet combined can’t solve it, that’s the reason we cryptographers thought we’d found a way to stay ahead of the code breakers for good.

Perhaps we got a little cocky because just when we thought the war was won, a bunch of 20th-century physicists came to the party, and they revealed that the laws of the universe, the same laws that modern cryptography was built upon, they aren’t as we thought they were.

We thought that one object couldn’t be in two places at the same time. It’s not the case. We thought nothing can possibly spin clockwise and anticlockwise simultaneously. But that’s incorrect.

And we thought that two objects on opposite sides of the universe, light years away from each other, they can’t possibly influence one another instantaneously. We were wrong again.

And isn’t that always the way life seems to go? Just when you think you’ve got everything covered, your ducks in a row, a bunch of physicists come along and reveal that the fundamental laws of the universe are completely different to what you thought? And it screws everything up.

ALSO READ: IBM CEO Ginni Rometty's CES 2016 Keynote (Full Transcript)

See, in the teeny tiny subatomic realm, at the level of electrons and protons, the classical laws of physics, the ones that we all know and love, they go out the window. And it’s here that the laws of quantum mechanics kick in.

In quantum mechanics, an electron can be spinning clockwise and anticlockwise at the same time, and a proton can be in two places at once. It sounds like science fiction, but that’s only because the crazy quantum nature of our universe, it hides itself from us. And it stayed hidden from us until the 20th century.

But now that we’ve seen it, the whole world is in an arms race to try to build a quantum computer — a computer that can harness the power of this weird and wacky quantum behavior.

These things are so revolutionary and so powerful that they’ll make today’s fastest supercomputer look useless in comparison. In fact, for certain problems that are of great interest to us, today’s fastest supercomputer is closer to an abacus than to a quantum computer. That’s right, I’m talking about those little wooden things with the beads.

Quantum computers can simulate chemical and biological processes that are far beyond the reach of our classical computers. And as such, they promise to help us solve some of our planet’s biggest problems. They’re going to help us combat global hunger; to tackle climate change; to find cures for diseases and pandemics for which we’ve so far been unsuccessful; to create superhuman artificial intelligence; and perhaps even more important than all of those things, they're going to help us understand the very nature of our universe.

But with this incredible potential comes an incredible risk. Remember those big numbers I talked about earlier? I'm not talking about 851. In fact, if anyone in here has been distracted trying to find those factors, I'm going to put you out of your misery and tell you that it's 23 times 37. I'm talking about the much bigger number that followed it.

While today's fastest supercomputer couldn't find those factors in the life age of the universe, a quantum computer could easily factorize numbers way, way bigger than that one.

Quantum computers will break all of the encryption currently used to protect you and I from hackers. And they'll do it easily.

Let me put it this way: if quantum computing was a spear, then modern encryption, the same unbreakable system that's protected us for decades, it would be like a shield made of tissue paper. Anyone with access to a quantum computer will have the master key to unlock anything they like in our digital world.

They could steal money from banks and control economies. They could power off hospitals or launch nukes. Or they could just sit back and watch all of us on our webcams without any of us knowing that this is happening.

Now, the fundamental unit of information on all of the computers we're used to, like this one, it's called a "bit." A single bit can be one of two states: it can be a zero or it can be a one.

When I FaceTime my mum from the other side of the world — and she's going to kill me for having this slide — we're actually just sending each other long sequences of zeroes and ones that bounce from computer to computer, from satellite to satellite, transmitting our data at a rapid pace.

Bits are certainly very useful. In fact, anything we currently do with technology is indebted to the usefulness of bits. But we're starting to realize that bits are really poor at simulating complex molecules and particles. And this is because, in some sense, subatomic processes can be doing two or more opposing things at the same time as they follow these bizarre rules of quantum mechanics.

So, late last century, some really brainy physicists had this ingenious idea: to instead build computers that are founded on the principles of quantum mechanics.

Now, the fundamental unit of information of a quantum computer, it's called a "qubit." It stands for "quantum bit." Instead of having just two states, like zero or one, a qubit can be an infinite number of states. And this corresponds to it being some combination of both zero and one at the same time, a phenomenon that we call "**superposition**."

And when we have two qubits in superposition, we're actually working across all four combinations of zero-zero, zero-one, one-zero and one-one. With three qubits, we're working in superposition across eight combinations, and so on.

Each time we add a single qubit, we double the number of combinations that we can work with in superposition at the same time. And so when we scale up to work with many qubits, we can work with an exponential number of combinations at the same time. And this just hints at where the power of quantum computing is coming from.

Now, in modern encryption, our secret keys, like the two factors of that larger number, they're just long sequences of zeroes and ones. To find them, a classical computer must go through every single combination, one after the other, until it finds the one that works and breaks our encryption.

ALSO READ: John Carmack's Keynote at Oculus Connect 2014

(Transcript)

But on a quantum computer, with enough qubits in superposition, information can be extracted from all combinations at the same time. In very few steps, a quantum computer can brush aside all of the incorrect combinations, home in on the correct one and then unlock our treasured secrets.

Now, at the crazy quantum level, something truly incredible is happening here. The conventional wisdom held by many leading physicists — and you've got to stay with me on this one — is that each combination is actually examined by its very own quantum computer inside its very own parallel universe.

Each of these combinations, they add up like waves in a pool of water. The combinations that are wrong, they cancel each other out. And the combinations that are right, they reinforce and amplify each other. So at the end of the quantum computing program, all that's left is the correct answer, that we can then observe here in this universe.

Now, if that doesn't make complete sense to you, don't stress. You're in good company.

Niels Bohr, one of the pioneers of this field, he once said that anyone who could contemplate quantum mechanics without being profoundly shocked, they haven't understood it.

But you get an idea of what we're up against, and why it's now up to us cryptographers to really step it up. And we have to do it fast, because quantum computers, they already exist in labs all over the world.

Fortunately, at this minute, they only exist at a relatively small scale, still too small to break our much larger cryptographic keys. But we might not be safe for long.

Some folks believe that secret government agencies have already built a big enough one, and they just haven't told anyone yet. Some pundits say they're more like 10 years off. Some people say it's more like 30. You might think that if quantum computers are 10 years away, surely that's enough time for us cryptographers to figure it out and to secure the internet in time.

But unfortunately, it's not that easy. Even if we ignore the many years that it takes to standardize and deploy and then roll out new encryption technology, in some ways we may already be too late.

Smart digital criminals and government agencies may already be storing our most sensitive encrypted data in anticipation for the quantum future ahead. The messages of foreign leaders, of war generals or of individuals who question power, they're encrypted for now.

But as soon as the day comes that someone gets their hands on a quantum computer, they can retroactively break anything from the past. In certain government and financial sectors or in military organizations, sensitive data has got to remain classified for 25 years. So if a quantum computer really will exist in 10 years, then these guys are already 15 years too late to quantum-proof their encryption.

So while many scientists around the world are racing to try to build a quantum computer, us cryptographers are urgently looking to reinvent encryption to protect us long before that day comes.

We're looking for new, hard mathematical problems. We're looking for problems that, just like factorization, can be used on our smartphones and on our laptops today. But unlike factorization, we need these problems to be so hard that they're even unbreakable with a quantum computer.

In recent years, we've been digging around a much wider realm of mathematics to look for such problems. We've been looking at numbers and objects that are far more exotic and far more abstract than the ones that you and I are used to, like the ones on our calculators.

And we believe we've found some geometric problems that just might do the trick. Now, unlike those two- and three-dimensional geometric problems that we used to have to try to solve with pen and graph paper in high school, most of these problems are defined in well over 500 dimensions. So not only are they a little hard to depict and solve on graph paper, but we believe they're even out of the reach of a quantum computer.

So though it's early days, it's here that we are putting our hope as we try to secure our digital world moving into its quantum future. Just like all of the other scientists, we cryptographers are tremendously excited at the potential of living in a world alongside quantum computers. They could be such a force for good.

But no matter what technological future we live in, our secrets will always be a part of our humanity. And that is worth protecting.

Thanks.

Resources for Further Reading:

Quantum Computing Explained in 10 Minutes: Shohini Ghose (Transcript)

Can We Make Quantum Technology Work: Leo Kouwenhoven (Transcript)

Michelle Simmons on Quantum Computation at TEDxSydney Conference (Transcript)

Transcript: What Popularizers of Quantum Mechanics Don't Want You to Know by Ron Garret