

Tuesday, November 17, 2026 12 PM Rayburn House Office Building

SUMMARY KEYWORDS

Quantum computing, Cybersecurity, Post-quantum, Cryptography, NIST standards, Digital signatures, Data encryption, Risk assessment, Blockchain technology, Cloud security, IoT devices, Financial services, Critical infrastructure

SPEAKERS

- Eugenia **Lostri**, Senior Security Policy Analyst, Google
- Lindsay **Fraser**, Chief Policy Officer, The Blockchain Association
- Ari **Schwartz**, Managing Director of Cybersecurity Services, Venable LLC
- Vincent **Voci**, Director, Global Government Relations & Partnerships, Cloudflare

KEYWORDS

Quantum computing, Cybersecurity, Post-quantum, Cryptography, NIST standards, Digital signatures, Data encryption, Risk assessment, Hardware migration, Blockchain technology, Cloud security, IoT devices, Financial services, Critical infrastructure, Public policy

Tim Lordan 00:00

So, again, thank you for coming. This event is hosted by the Congressional Internet Caucus and with the Congressional Internet Caucus Academy. Ari is one of the expert panelists, but he's also agreed to kind of like a moderator in a sense, so Ari Schwartz is the head of cybersecurity services at Venable, which is a great law firm here in Washington D.C. And Ari has had stints on cybersecurity in the White House and at the Center for Democracy & Technology. And I'm just going to leave it up to Ari. Thank you.

Ari Schwartz 01:34

Thank you and welcome. So, just to get a level setting, especially before Eugenia speaks here and gives the basics of quantum. How many people here feel familiar enough that they could

explain quantum computing to someone else? Okay, that's not that's more than I thought it'd be. How many people understand post quantum cryptography? So basically, maybe about half the people that para. Okay, so that's a basic start. You still have to go all the way to the beginning for everybody, but that's a good starter. So we have a great panel today. We're going to cover the basics, and then we're going to go in a little bit further into why this is a security issue and where we stand on trying to address the security issue, because this is the good thing about this is it's sort of like a one-time security issue, which most of them are not. Most of them last forever. Most of the security issues, but the old issues don't go away, and we just keep getting new ones. But this is one that actually can be solved, so that's the positive news about it. But we have a lot of work to do. So rather than kind of keep you talking at a high level, I'm going to pass things over to Eugenia Law Street. She's a senior security policy analyst at Google, and she's going to give the basic overview here.

Eugenia Lostri 03:01
Thank you, Ari, and thank you, Tim, and thank you to the Congressional Internet Caucus for hosting us today. I'm excited to be here to talk about why it's important to focus on the PQC migration. So, as Ari said, before we kind of dive into the conversation about quantum computers' impact on cybersecurity, you know, I wanted to outline a little bit why we're trying to build quantum computers and how they work. There's generally a common misconception that a quantum computer is just kind of a faster supercomputer, but they're actually a new kind of computer hardware. They use the principles of quantum mechanics to store and process information in a completely different way. Unlike classical computers that store information in those binary bits that we're all kind of used to, the one and the zero, quantum computers store information in qubits. Quantum bits, very, And those can be a zero, they can be a one, and they can also be in complex combinations of both, which is usually called superpositions. Additionally, the qubits can interact with each other, and they can become entangled, and so that information and so that information can be kind of related across the qubits. In practice, what that looks like is that while a classical supercomputer will need to kind of brute force many possible solutions before finding the correct one, for some problems, a quantum computer is going to kind of organize superpositions of those entangled qubits so that incorrect answers cancel each other out, and those in the correct answers kind of emerge at the end of the computation. These properties that qubits have make quantum computers well suited to solve some problems that even the most powerful classical supercomputers can't tackle, and that's especially evident. In simulating the quantum mechanical nature of nature itself, and so quantum computers are going to have great implications for what we currently consider impossible problems in areas like drug discovery, or material science, or energy. Unfortunately, it's also this that makes quantum computers a real threat to current cryptographic standards, which we rely on to protect things like our bank transfers or our private chats or you know sharing classified information. Today's cryptography rests on the assumption that certain math problems, namely prime factorization and discrete logarithms are too hard to practically solve with classic computers. For example, standard RSA encryption works because we have a very large number that's the private key, and breaking it up into its prime factors, which are the private key, the sorry, the public key, and breaking it up into its prime factors, the private keys, is so difficult that it would take it would take today's fastest classical computer millions of years to

solve that. But in 1994, a mathematician Peter Shor showed that a sufficiently capable quantum computer, what we call a cryptographically relevant quantum computer or CRQC, that's a term that I think you're going to hear a lot in today's session, could solve those factoring and discrete logarithm problems with practical practical speed and resources. So running Shor's algorithm on a future CRQC would bypass the asymmetric encryption that we use to, for example, secure data in transit, and it could break the digital signatures that we use to prove that documents or software updates are authentic and that they haven't been tampered with. You can kind of see the implications of that. There are basically two main risk areas that we need to address for this. Our Google's threat model at least prioritizing these two at the top of the at the top of the list. One is the immediate threat that asymmetric encryption faces from what are called store now, decrypt later attacks. These attacks don't require a quantum computer. Basically, what we anticipate and what we think is happening is that threat actors can collect encrypted data with the expectation that it will remain relevant by the time a CRQC is able to decrypt it. So, if you think about information that your offices handle that needs to be sensitive and will remain sensitive for the next 5, 10, or more years. Then you need to be thinking about what type of cryptography you are relying on. The second risk area is the forging of digital signatures. So if an adversary can forge a signature, they can impersonate a trusted software vendor. They could push malware that then the systems think is genuine.

Eugenia Lostri 08:04
This threat is only going to materialize once a CRQC exists, but the complexities involved in migrating the systems make it so that we need to tackle that migration as soon as possible because it's going to take time. So, like Ari said, we have good news here. It's not all bad news. We know what to do to protect ourselves, and that is to adopt post-quantum cryptography. These are algorithms that are designed to be secure against both classical supercomputers and future quantum computers. We even have, after a very lengthy multi-year process, an international process in 2024, NIST put out its first set of PQC standards. So adopting those should, you know, get us closer to being quantum safe. A question that we usually get is, if there is no CRQC, we don't know when it's going to be here, and if it's going to be here, it's still several years away. So why should we focus on this issue now? Where is this like added urgency coming from? And there are at least three things that I want to outline here. One is that we think that the timeline to a CRQC is shrinking. There's been over the last year theoretical leaps in error correction and quantum algorithms that could drastically reduce the estimated physical resources that we would need to break cryptography. That is why Google earlier this year announced that our PQC migration deadline is 2029, which is ahead of some of that conventional wisdom that you know you may have heard about 2030, 2035 as a deadline. Now, just to be clear, We're not saying that there will be a CRQC in 2029 that will break cryptography. We're saying that the probability is no longer zero, and that we are not gambling on the possibility. The second is pretty straightforward. Cryptographic migrations take time. We've experienced other cryptographic migrations in the past; those were simpler, and they still took over a decade. So, if it takes 10 years to migrate complex systems, and a CRQC could be here in less than 10 years, I don't need to do the math for you. And the third is the reality of hardware. We are constantly shipping satellites, devices, infrastructure that is going to remain in the field for years to come. And so, if that hardware remains in the field by the time a CRQC

arrives, you want to make sure that if it's unpatchable, but it is already quantum safe. So I feel like I've been talking a lot there. All right, hopefully that kind of did a great job. Yeah, I thought you did a great job. Yeah, but happy to know you can go deeper into any of those. I don't know if the people that knew nothing

Ari Schwartz 11:16
About quantum now feel that they can describe it, but I think we can have a conversation now. The rest of the conversation. So I think that was very helpful in getting to this point. Right. We as as Eugenia said, the focus has been on trying to put these new algorithms out there so that when this day comes that this computer that can solve Shor's algorithm comes out, that we we have things out in the field that can protect things going into the future, and progress has already been being made in that area. And Cloudflare has been one of the leaders in helping to do that and to kind of measure it. And so we have Vince Voci here, who's the director of global government relations and partnerships at Cloudflare, to kind of go over some of that work for us.

Vincent Voci 12:08
Sure, thanks very much. Delighted to be here. Thanks, Ari. Thanks, panel, for convening this discussion. Looking forward to it. So, for those that don't know Cloudflare, we're a 15, 16 year old company. We're a cloud-native, cloud cybersecurity, and content delivery network. Most people know us. We proxy about 30% of the internet. So when you go to a website, you see the little cloud thingy spinning. You're connecting through the Cloudflare network. So we own and operate a proxy network, a content delivery network, where we're one of the most tied-in networks in the world. So our business really is in helping to build a better internet, and like that underlying philosophy kind of drives our post-quantum encryption plan. So we've got a number of different kind of point products that I'll talk a little bit about in the context of our PQC migration story. Primarily, that's in our content delivery network. So, how do visitors go from being a visitor to the Cloudflare network to a website and anything that is running on a website? That's applications. That could be agents, that could be APIs, and then from a website, from a website to an internal network, and all of those different kind of links need to be post quantum encrypted all along the way. As Eugenia had laid out, we are most concerned about Harvest now, decrypt later attacks attacks today, and that you know, classic example of that is the OPM breach from a couple of years ago. It's widely suspected that a Chinese entity had stolen 10s of millions of former government, current government employees' sensitive personal information, and they're just waiting until a CRQC is available to decrypt it and build profiles on all of us, right? Like that's the attack today that we are most worried about. The good news is Cloudflare, Google, a number of browsers have been working in partnership along with NIST and other standards development bodies, largely since 2019 on the development and deployment of a particular suite of standards on the on the key agreement side, that's ML-KEM 768, which is a NIST developed standard adopted in the Internet Engineering Task Force (IETF) and broadly deployed at scale today. So for us, you know, roughly you know 20 30% of the world's internet traffic, we see roughly 60 almost 70% of that is encrypted and protected from Harvest now, decrypt later attacks today. That is like the product that's solution number one that is deployed today. Like I said, that work has been going since 2019 on the encryption side. There's a lot more that is coming on the signatures and their certificate side. Eugenia also touched on that as

well. ML-KEM is the standard that we have adopted? Not just we have adopted. Europeans have adopted that. G7 countries broadly have adopted it. Largely, the world has adopted ML-KEM 768 as the default standard, and that is a good thing. That is deployed at internet scale. What remains is on the authentication side. Once a CRQC computer comes available, potentially you could have nation states, adversaries impersonating and attacking live systems. So for us, the work that remains is on the post quantum encryption side, there is a standard ML-DSA 44. We have adopted it. Others have adopted it. It is in deployment. We have done visitors to Cloudflare side of the deployment on the signature side, but it is big and it is complex and it is not fit for purpose. So something that we are working with Google on is the deployment of Merkle tree certificates. Something that we hope will go into product testing. Well, actually, we've already tested it. We hope it will go into internet scale deployment next year. And we also are aligned with Google, IBM, and others on the 2029 timeline. We moved our timelines. It's not like Y2K where like there is a particular date and time. This is math. It's really hard math. It's imprecise in terms of when we can predict the future and when that day will come. But we know that it is coming. So the question we get a lot is how is AI either making this more difficult or making this easier to do? There was some news over the summer where AI, one of the frontier models, broke one of the one of the encryption algorithms.

Vincent Voci 17:15
It was widely expected that Hawk would fail. We don't think that AI is necessarily going to make our jobs easier or harder, but it is something that I think we will also have to deal with as well. So, looking forward to the questions from the audience. Great, thanks, Vince. So our next speaker is is Lindsay Fraser, who's chief policy officer at Blockchain Association, you'll remember Johannia spoke about the three different areas that they're looking at for where there's concern, and one of them was kind of around the digital authentication, digital signature piece of it, and obviously some of the things that are encrypted and that kind of follow that line are things that blockchains are used for, including crypto. So we know a lot of people are interested in that. So,

Lindsay Fraser 18:02
Thank you very much, and thanks for having me. My name is Lindsay. I lead policy at the Blockchain Association. We're a nonprofit advocacy organization that represents U.S.-based companies operating in the digital asset space. So, not to throw more terms into the mix here in what is already a complex topic, but just to take a step back and kind of define what we mean when we're talking about blockchain technology. So, blockchain, all it is really is a distributed ledger system, and it enables a decentralized method of verifying transactions. And so, a lot of the benefits of blockchain technology is also what is going to make PQC hard for the industry to adopt. So, to take a step back, when we're looking at blockchains like the Bitcoin blockchain or Ethereum, the fundamental concern, as I mentioned, is around digital signatures. These are what allow individuals to authorize transactions and prove ownership of digital assets. And in order to do so, they use a technique called the elliptic curve cryptography, which utilizes a combination of public and private keys. Your public key, people can see and have access to your private key is what ensures that you are the one who's signing off on the transaction yourself. And you know why this is so important from a security standpoint. One of the

innovations of blockchain technology and crypto more broadly is the ability to self-custody your own assets in a digital wallet, and the combination of this public-private key is what allows you to make transactions. But maintaining access and keeping your private key private is incredibly important to securing your own assets, rather than knowing a bank that holds your dollars in custody. Assets for you. Many in the crypto ecosystem use these self-custodial wallets, where you are in complete control of your assets, and it really hinges on the security of that private key. If someone you know discovered my private key for my self-custodial wallet, they would have access to my assets. They could do transactions. The good news is now, you know, in this pre quantum computing world, it is impossible to derive a private key from a public key. The concern in a post quantum world is that Shor's algorithm would allow for the private key to be derived simply from the public key, which is something that can be visible by all in the network. And so, this is obviously, you know, as mentioned before, the concerns around digital signatures are not just a concern for the blockchain digital asset ecosystem. It's a concern across the entire financial ecosystem. But blockchain technology presents unique considerations. I think when we look at the benefits of blockchain technology, its decentralized nature compared to a bank that's a centralized authority, it would be nearly impossible to attack all of the Ethereum validators in the network at once and compromise the system. Whereas that is not the case with centralized entities, but that same benefit also poses potential issues as we're looking to upgrade to quantum resistant systems in the future. Ethereum, for example, has a broad network of validators who validate transactions that are happening on the protocol, but that being said, it's an immutable protocol, and updates can only be made through wide governance votes, which require majority of validators and people in the network to sign off on upgrades. So again, it's not as easy if you know Chase as a bank decided we're going to roll out our updated security system. We're going to do it over nine months at this date. All the updated security features will be in place, and that's what's happening. That's not as simple with a decentralized blockchain, but the good news is that the industry is starting to prepare for it now. Ethereum, for example, the Ethereum Foundation has started a quantum security program at the foundation where they are looking to upgrade the protocol to be quantum resistant, as they call it, by 2029. So similar to some of the timing that the Google team is is working with.

Lindsay Fraser 22:37
We also have centralized exchanges like Coinbase, who are investing resources into figuring out from a custody perspective how to ensure that assets are being safe in a post-quantum world, and then we're already seeing real-world deployment on several blockchains. Algorand, for example, has already introduced quantum-resistant accounts and process transactions using post-quantum signatures. So we know, you know, as mentioned earlier, that it's technically feasible. The particular challenge with blockchain technology is just that the migration process will likely require a longer timeline, given the decentralized nature of the technology.

Ari Schwartz 23:21
Thanks, Lindsay. That's a helpful description of where we stand. I'm going to speak very briefly on the role that federal agencies are playing. So, we had some discussion of NIST's role, but I think I want to take it back a little further for NIST's piece of this and talk about a little bit of the history of how NIST has done cryptographic chosen cryptographic algorithms. So going back to

the 70s, actually the first time NIST had a role in security. I know for some people, NIST-like names are synonymous with computer security. But NIST before the 70s, NIST role was totally standards measurement, not doing really security pieces. It does. They do have some history like fire safety and building safety codes, which and that it's sort of where some of these pieces are tied together. So to security, but in the 70s, there was was starting to use companies were starting to use cryptography, and they were selling things to the government, and they each had their own proprietary cryptography and couldn't speak to each other, and so the government and the agencies were trying to decide which one of these was the best, and in having that conversation, they ended up not being able to speak to each other, which clearly was a problem. And industry was fighting among itself how to go about choosing this and pick a standard. So it was decided that NIST would come in and do a competition for the best algorithm to choose from. So they actually. Did an international competition, chose the best algorithm, and then everyone in the world, basically the whole world economy, started using those algorithms chosen by NIST. And it has been a strategic advantage for the United States to make sure that we trust those algorithms that are being used, and that NIST is the one that has been doing this year after year. And that, and by making an open international competition, other countries have kind of agreed to that and worked with us through that, through that work. And this latest work of trying to find the post quantum cryptography is proving that that's still the case. The EU and others still want to kind of put a stamp and say that they're using post quantum algorithms, but they're still looking to the U.S. to choose it. And in fact, a lot of the mathematicians that that NIST ended up approving are in Brussels or Belgium, right down the street from the EU. And so they wait for NIST to decide, and then they have their own European Anna organization that then like blessed that same standard that NIST chose as well. So it has been a success and continues to be a success. That NIST budget though has been greatly decreasing over the years, and some of that work is at risk in the future. And keeping NIST strong remains a kind of a key point here. If you're going to end up with this ability to keep that kind of advantage that the U.S. has, that we we trust and kind of help to build the world's infrastructure in this space. Then, secondly, the thing, other thing I wanted to raise was that there is a OMB there is OMB guidance for agencies to for for agencies to become PQC compliant and use the NIST standards, and the date that they have is is 2030. Which after this panel, you everyone hearing you're hearing everyone say 2029. But when they came out, actually that was actually pushing things forward. You know, at one point it was 2035, and then it was 2034, and now they moved it to 2030, which was seen as a big jump. But as Eugenia said, I mean, the chance at 2029 goes from zero to some small amount in 2030, and if things are advanced faster than people think, there still could be some risk there. So there is still some push to get agencies implementing before the deadline and looking at it before the deadline, and which is which is key and important here. And I do want to stress here. I mean, I think it's very difficult. Most security problems that we have, and the way that most policymakers think about security.

Ari Schwartz 27:41
They wait until the moment that something bad has happened, and then they invest in it after the bad thing has happened. If we do that in this case, we lose. Like that, there is no coming back from the bad thing happening, right? If if so, if we wait until the quantum computer that

breaks Shor's algorithm is out there, that's too late. So it's a very difficult message to give to policymakers that we need to invest a lot of money in something. Vince raised Y2k as an example, and I do think that that is probably the only other time we've kind of had that situation, and you know, some people think that well, it wasn't as bad as we thought. Other people will say that was because we were prepared and we actually invested in it and we stopped it from happening. Either way, in this case, we need the kind of investment that we made there in order to make sure that we can get there. So that's my non-moderator part of the role here. So I will open things to questions. I have a bunch of questions too, but I know that this is a topic that lends itself to lots of questions. So if people have questions about things people said or things that they want to raise and ask questions about, happy to do that. Do you have a mic, or should they just say it? We should repeat the question. Okay, go ahead.

Speaker 1 29:07
Thank you guys so much for coming and talking about this important topic. Not a lot of knowledge on not just on the Hill, but in the country right now on this. My question was around IoT devices, and I think Lindsay, you mentioned Algorand, which I think uses Crystal's FALCON as their PQC method, which is lightweight. But I've I've heard from some I am not a quantum physicist, but I've heard from some quantum computing specialists that the lightweight requirements and like the low latency requirements of an IoT device could be particularly difficult to fit QC standards to. I was just hoping maybe you guys could flesh that out. You know what is already being done? Is this an active problem? Are there fixes? That sort of thing.

Vincent Voci 29:57
I'm not, again a PhD cryptographer, but my understanding on the ML-KEM side of the kind of two-part problem, we actually see a security and performance equivalency in PQC algorithms running in hybrid with older algorithms. So we don't have kind of the performance and security considerations that we do on the encryption side, on the signatures and certificate side, that's where we have you know ML-DSA 44 deployed for our internet facing and our origin facing traffic. That does see a significant performance hit. The certificate lengths are six or 10 times longer, so that is why we, in particular, are working with Google on the Merkle tree certificates that will far simplify that side of the handshake. So I think, particular for low compute devices like IoT devices, but I think the broader problem is probably like older hardware, which we're seeing play out in the AI frontier model side, seeing that play out for years on the generally like more vulnerable, can't be updated. This week we're seeing it play out in just like things working. So yeah, patches not getting maybe not getting deployed, you know, with adequate testing. But I'd probably have more concerns, you know, less on the software side, less on the cloud infrastructure side, probably, and less on like those tunnels between, probably more on the legacy hardware side, which isn't necessarily a PQ problem. That's a hardware replacement problem, and that goes back to where I think Ari was talking about on the infrastructure investment side. If anyone else has,

Ari Schwartz 31:42
I mean, maybe we can put this into one of the other questions that we had talked about, which is what kind of investments do people need to make in general? So you did for IoT, but do you

know how this work in other areas? What you talked a little bit about what some of the crypto folks are doing in certain areas. What kind of investment is it going to be for different players in the ecosystem?

Lindsay Fraser 32:08
Yeah, I think speaking from the perspective of our member companies, who we represent several layer ones, who are those base blockchains that we talked about, but also projects that build on top of them. And I will say, a year ago, this was not very top of mind for our members. I'm sure staff in this room have heard from us a lot on market structure legislation and stablecoins and all of that. But I have seen over the past year more and more of our members having to dedicate resources to thinking about these issues, I mentioned the Ethereum Foundation. Bitcoin is also working on what their solution will entail. We have other companies that are solely focused on building solutions that blockchains and projects built on top of public permissionless blockchains can use to ensure that they are ready for a PQC world. I think another big piece of it is expanding public-private partnerships and information sharing as we approach this future state. We've been doing a lot of work with the Department of Treasury's Office of Cybersecurity and Critical Infrastructure, and they have been asking to meet with our members to learn about how they are preparing, and then also at the same time figuring out what are the standards, guidance, et cetera, that they are going to put out for those who don't have the resources to get to dedicate a full research team to PQC other companies. How can we share that information? So, you know, the small startup with five people who are trying to build, you know, a new blockchain or a project on top of a blockchain has the resources that it needs to become PQC compliant, even when they don't have millions and millions of dollars to dedicate to researching what you know the best path forward is. So I think another area that I would implore staff on on the Hill to think about would be how to expand those private-public partnerships with key agencies like NIST, with the Department of Treasury, and others, so that we're making sure as we're kind of thinking through what the world looks like, it's not just the largest, most well-established companies that are able to be secure. We're sharing enough information so that you know the entire ecosystem is able to be prepared for when when the time comes. Anna,

Ari Schwartz 34:30
Anna, do you have thoughts on? You talked about a lot of different types of infrastructure, but

Eugenia Lostri 34:35
yeah, I mean, I think I'm plus one to what my co-panelists have been saying, but you know, unfortunately, the answer I think is also it will depend on what kind of organization you are. I think you know what we recommend is you need to start by understanding your own exposure, right? Understanding what type of cryptography you're relying on, where. What is the risk of exposure? You know whether it is one of those systems that you need to really be thinking about right now, or if it's something that is not a high priority asset. Like I think that is really going to shape what the migration of each organization looks like. You know I think for example if you rely on a cloud service provider, they're going to do you know a lot of the migration. There's still going to be something that you need to do. You can't. This is not something that one

company or just a couple of companies are going to solve for everyone. But yeah, I think having that understanding of your own exposure and then making decisions about the risk based off that is yeah. I mean, following up on

Ari Schwartz 35:44
that, and anyone can answer this. I mean, so you gave the example of someone that has like most of their infrastructure in the cloud. Well, that will get updated almost just by the fact that your cloud provider is update is upgrading. But what for what kind of organizations? What kind of infrastructure for in those organizations is is going to take longer and have more complications? Can you give some examples of things that fall into that category?

Eugenia Lostri 36:11
I mean, we've we've talked about you know I I think like Vince said, the hardware component is something that we really need to be thinking about if you have hardware that is going to remain in place for years to come that you don't want to be modernizing again in five years, then you need to be asking those third-party vendors what their plan for PQC is, you know, and and just kind of build that into your risk assessment plan.

Ari Schwartz 36:45
We didn't have this in our questions, but there is a question I want to follow up on on that point. Maybe Vincent can pick up this too. There's been some discussion of doing hybrid implementations. Can someone explain what that it means, and then also, are is that going to work, and how will that work? So, I'm

Eugenia Lostri 37:04
happy to get started.

Vincent Voci 37:05
Yeah, either or.

Eugenia Lostri 37:06
Sure. So, hybrid implementations would basically require that you do classical cryptography and PQC at the same time. I think the expectation with that is, if somehow you know there's if the PQC ends up not being safe against a CRQC, which you know I want to caution against thinking about it in those terms that this has been you know the result of like a very lengthy process by very smart people, but if that happens, then you remain protected against at least classical attacks. I think that there's a lot of trade-offs that you need to consider when you're thinking about hybrid. We've done some hybrid migrations in the past, but I think that you need to really think about the latency issues, and you know how that is going to affect the performance of the systems that you're relying on. So I don't know that we have kind of a set approach. It's something that it's an evolving conversation about where we are choosing to prioritize,

Vincent Voci 38:22

yeah. And so for Cloudflare, we're running hybrid cryptography through our entire global network. It's all deployed on ML-KEM 768, running over TLS 1.3. So that is the standard. We are running hybrid because so many different customers are coming to us with so much different cryptography that if we were to go to ML-KEM by default, we think that we would probably stop global internet traffic like tomorrow if we were to do that. So for today, like it's hybrid it's hybrid deployment at global scale for all internet communication. But I do think that there's probably an end state. We're not really sure when this will be, where hybrid will go to ML-KEM like by default at some point. Not sure if that's 2030. No government has really said when, but I think that's an end state that's coming. There is a government standard primarily through the DoD and the IC called CNSA 2.0, which does not permit hybrid post-quantum cryptography deployed at any part of its network. There's advantages to CNSA 2.0, especially for national security, DoD, and IC applications. However, it does use key links in particular for ML-KEM that are double, so that does not allow scalability to critical infrastructure. Most critical infrastructure are companies, financial services, and others are adopting ML-KEM 768. We are seeing mission creep in CNSA. Deploying out to other communities where that is being adopted, that is not an IETF standard. That is a bunch of cryptographers at DoD saying we think this is the way the world should go. It is not a standard that is in common practice. So there is, for us, a policy in an operational standpoint, that is an area of divergent risk that we are looking at, but that is back to Ari's question. We run hybrids. There will be a point in time where we don't run hybrids, but it's probably not in the next five years or so. Yes.

Speaker 2 40:33
Operational technology, power systems, industrial controls, things like that. A lot of these systems, some of them can be decades old, and they don't get over the air updates. I'm wondering is what's the solution there where you have old encryption.

Ari Schwartz 41:12
I mean, if I think if you talk to the hardware companies that support it, they'll tell you that at some point they're going to have to upgrade the hardware, right? And so that's part of the determination. Here is you really need to think about how you're going to do those upgrades from a hardware perspective. But there are ways similar to IoT to kind of upgrade even those older systems, and try and make them work in the future as well. I don't know if you want to talk about some of that. Anyone?

Vincent Voci 41:51
I'm happy to take it. So OT is particularly hard. It's very old. Some of it's been in you know, for those that don't know, operational technology that could be your industrial control systems, your SCADA systems, your PLCs, anything that's in the electric grid that is helping to do remote monitoring, pipelines, doing remote operations, big big threat vector, right? And largely because it's old, can't be upgraded, and if it's installed correctly today, it is not internet facing. It should be segmented from your IT networks, it should not be internet facing. That is how the Iranians get into our pipelines and our water and our wastewater systems in other nation states. So one, I think it's old technology probably needs to be generally upgraded, but there are compensating controls that you can put in place. So for for Cloudflare, that would be virtual private networks,

Cloudflare tunnels, anything that is doing inter enterprise communications that can be running over a TLS, ML, or ML-DSA standard. But the bigger problem is probably the hardware itself, something that is uniquely exposed, especially in the AI and cyber frontier model world, but has long been targeted by nation states anyway.

Ari Schwartz 43:09
You want follow-ups? Yeah.

Vincent Voci 43:37
I'm happy to give an answer if someone else wants to. I mean, I can give a policy answer to that, which is right. Most

Ari Schwartz 43:42
of these are run by companies that are regulated, and they have utility commissions they have to go through, and they need upgrades. And utility commissioners need to be aware that there's going to be a cost, and that they probably should switch out the technologies, and that they should give these companies the cost upgrade for the purpose of switching out the technology. That's my, you know,

Vincent Voci 44:05
I'm not sure I could rank order you know sectors that should you know start and begin. Obviously, like comms and IT are doing you know broadly a ton of work. You know, as software and cloud companies, as kind of the custodians of cryptography on the internet. You know where we are deeply invested in that. I'd say financial services like is asked the most amount of questions. They've been the most forward leaning in asking their technology companies, and part of that is informed by regulations. You know, SEC, FDIC, OCC go down the list of regulators, and they're asking. You know, there are critical third-party dependencies to IT and comms companies that they have to ask. So they've been very forward-leaning on that. After that, you know, it really kind of falls away, and I probably lose a bit of visibility. But you know, I mean, it's very interesting

Ari Schwartz 44:56
to have conversations with the financial sector because I think they're further along than a lot. Of the other critical infrastructure sectors, and if you talk to them about the problems that they ran into, they found it to be very expensive to implement. So, I think that there is a lot of work that people need to discuss in the space. So, yep.

Speaker 3 45:14
Did you comment on medical devices and maybe FDA?

Vincent Voci 45:18
I can't. I wish I could. I'm wearing one, and I can't. I got an insulin pump, so

Speaker 3 45:25

uniquely interesting. A subset of IOT, and a pretty scary subset. Yeah. So I mean, can you imagine the FDA or someone else

Vincent Voci 45:31
regulating

Speaker 3 45:31
it in some

Ari Schwartz 45:36
way? The FDA does have guidance. Yeah, it does have guidance in the space for medical devices specifically. So I do think that I mean you can look there. I don't know it's not something I've read recently, but I do know that they have guidance in the space. I don't know if they've updated it either since the OMB memo came out, et cetera.

Speaker 1 46:00
In the process right now of trying to address, I saw an article this morning on AI hacks. Yeah, and the risk there. Well, you

Vincent Voci 46:10
can see how you industry. If I was at Medtronic or or Abbott, if I was in one of those companies, like how I would want this to play out. You know, FDA would promulgate cybersecurity guidance for connected medical devices. That would be based off of you know, hopefully, what we like we we in industry like to see either NIST special publications or NIST cryptographic standards. So FIPS 203, FIPS 204, we would want to see that embedded. Those are the MLCAM and MLDSA standards for next generation for the post quant. So that's how I would want to see it play out. I just can't speak to if that is how it is in play.

Ari Schwartz 46:52
I mean, they have had strong guidance for a number of years now on medical devices and cybersecurity, and then PQC is a piece of that, right? So my point is, I don't know what the latest has been in that guidance for the updates, but it is embedded in that. So that's the place to look. Yes. Get lunch going, then.

Speaker 4 47:13
Yeah. Relates to policy. So you talked about NIST and essentially being in communication with the EU to inform a lot of the standards that should be mandated, but if you look at the EU, they're kind of following the CRA, and that's legally binding. While this is somewhat voluntary, if I understand it correctly, maybe not all sectors, but most of the questions so far have been about how do you actually do this very expensive migration, informed by internal assessments? Well, it's sort of a question mark for me as a sort of well, we will do it when we are able to do it, and we sort of would probably default to having it been done if it is financially zero. It seems like it's not.

Ari Schwartz 48:06
Yeah, I mean we've we've always taken this sectoral view on technology issues in general, technology regulation, and there are some sectors that have very strong regulations in place and that rely on NIST and other standards bodies to kind of put them together, whereas as the EU recently moved to CRA, which was specifically designed actually originally around IoT and has expanded to become all software for every purpose. So it has now affected the entire marketplace, as you say, so it is pretty broad in its coverage. I think if you ask how PQC is is being implemented in the EU, you'll find like there aren't dates and they haven't really set it yet. They are working to come up with those those pieces and put it together. Anna is spending time, a lot of time on it, and they stand up.

Vincent Voci 49:02
You can speak for it.

Ari Schwartz 49:04
Yeah. Yeah. Excellent.

Vincent Voci 49:09
Perfect.

Ari Schwartz 49:10
Am I doing an okay job in the description? Go ahead. To NIST standards in general, or to NIST? You're saying for PQC purposes? I mean, there. So there. I mean, they had a competition, and there are a number of standards that were part of the competition, and people can choose other standards. And they've actually broadened what is acceptable since they first started it, because there were some questions. There's been some questions about different pieces of it. So they broadened. I don't remember how many algorithms they end up going with.

Vincent Voci 50:00
Six that were originally on the ML-KEM. I think there were six algorithms that were originally selected by NIST. It was part of an international competition. Incidentally, more Europeans won than Americans won. And even if they were like American standards, there were like European cryptographers that wrote them, as is the case at Cloudflare as well, our lead cryptographer is Dutch. So it's funny how the world works. But I think like you know what survived so far, industry has generally accepted, adopted, and like that's global industry. Do we envision a world in which there are more? There's more cryptography developed. Yeah, absolutely. I mean, there have been people that doesn't like bifurcate the internet. Absolutely, is that a risk in China? Absolutely, is that a risk in Korea? Absolutely. There are governments that from time to time will talk about developing their own cryptography, and we have to, you know, try and push like this message of one internet. Yeah, absolutely.

Ari Schwartz 51:02
China has had its own cryptography standards as time has gone on, right? And people have had to build it in if they're building for the Chinese market, so that you have a hybrid approach

for that, right? So you can imagine that they would do that again for this as well. But it has been. I mean, the fact that I do think that the fact that that we've come to this position where most of the math is done in Europe and then most of the implementation is done in the U.S. has meant that there is this kind of U.S.-EU-EU alliance around cryptography, and the rest of the world has kind of followed along with that. It's been strange to me that, and I've said this to EU, you know, people in the EU, like we want an EU standard for everything that we did. We should come up with our own standard. Well, like I've said, well, why don't you invest more in PQC? This was years going back 10 years. You know, why don't you invest more in PQC in Europe and make sure that you're so far ahead and you have the whole implementation chain as well as the mathematics? But it's still turning out. We're still ending up in the same place now. There are some more implementation companies, especially in the Netherlands. There's a bunch of implementation companies that have gone into place that make things easier to implement. But we're still ending up with mostly the Europeans doing the math and the U.S. kind of building how the implementation should work and then coming together and making it all happen. So,

Speaker 3 52:22
we're pretty happy about that. The news is that we have a complete limit on QKD in Europe, whereas the US has completely moved ahead with PQC and solely PQC. In Europe, there's still debate as to whether we should not move on both fronts at the same time and completely give up on potential use cases.

Speaker 1 53:09
Yeah.

Vincent Voci 53:12
Anyone want to take QKD? So QKD is a suite of technologies that runs a little bit in competition with where Google, Cloudflare, others have adopted ML cap. QKD is a quantum key distribution, and largely that is point to point hardware solution. So you can see in the OT world or in a national security system world where you would want particular fiber links between certain systems that are not internet facing, where a QKD technology would feel would fill in a niche. The problem is, it doesn't scale. It doesn't scale at internet scale. It will always be point to point. DoD has come out and said that it is more of a science experiment than it is a realistic technology for PQC migration. But I think like it's a science, and like science evolves, and time will change. The other problem with QKD is that it works for ML-KEM, or it works on the encryption side. It does not work on the certificates and the signature side, and that is the biggest problem. So you can solve one part of the post quantum migration, you can't solve part two on the QKD. So vendors number one that you will hear from, like generally in Hill offices, when you hear when you take meetings with companies, you'll hear quantum key distribution companies come in and say we've got a point product that can solve like all of your PQC at the highest level of security. And then number two, you'll hear a lot of cryptographic discovery companies that come in and say if you pay us a million dollars, we can discover all of your crypto inventories. We can prioritize your library upgrades. We can prioritize your software. Updates by far and away the loudest to different types of companies in the world. As Eugenia said, like organizations definitely need to prioritize where their risk is. They need to understand

their dependencies. But I think, like as we kind of alluded to, email certainly really important. If you might not be on a Google shop, and maybe return to work on Thursday and Friday. Email would be certainly a number one area of migration for me. And you can see, you know, it's remote workers, virtual private networks, or similar products would be another kind of technology that I'd be certainly very interested in. And you really don't need a consultant to come in and tell you that you know email is super important and VPNs are important.

Speaker 5 55:46
Johanna, you want to cover?

Ari Schwartz 55:47
Yeah, go ahead.

Eugenia Lostri 55:48
Oh no, I just wanted to add that the guidance that Vince was referring to from DoD referring to is the feasibility of QKD as a scalable solution. It's also co-issued by a lot of European governments, so that's going to be an interesting dynamic as the EU continues to consider those two. But a lot of the governments have expressed their support for PQC over QKD. And if anyone's interested in like a more technical overview, we do have very nice blog posts from our cryptographers explaining why at Google we're choosing PQC over QKD. That's kind of a very good post. Yeah,

Speaker 4 56:31
yeah. That's

Ari Schwartz 56:32
basically that's what I was going to say. You want to talk quick because it's the most complete post that I've seen on the topic. So I will say one one thing that's tied into that that's mentioned in that post is most you know most cryptography is not broken because the algorithm is bad right like that rarely happens key management issues are the are the problems so the more complex you make the key management issues the more likely it is to be broken so that that that's one of the the basic flaws there that that a lot of people have discussed, and and people and there's been other key distribution efforts that have been broken by just like people physically going in and being able to show up with keys at the same time. So and I won't go into more detail than that. If you can read it, you can read more about it in other places. But I think those are two kind of high-level things that people can understand why we focus more on PQC than QKD here. So, yeah.

Speaker 6 57:32
So you talked about in your previous question and answer how you know devices after quantum or whatever Q day, whatever you want to call it happens. They're going to need more compute, maybe more bandwidth to deal with quantum stuff. We'll need a lot more devices to upgrade all our hardware. What is the impact going to be on the prices of the products and the components and the availability of them? Like, are we going to expect things to get a lot more expensive or

like a little more? And if you don't have any good details on that, who should we be talking to to figure that out?

Ari Schwartz 58:04
So I mean I've said it already. I think it's going to be very expensive. I don't think we should be. I don't think we should sugarcoat it and say, oh, we can solve this problem and we should get started on it. And it's going to be we'll figure it out as we go along. And

Speaker 6 58:19
then

Ari Schwartz 58:21
consumer products. I don't. I don't know as well. I know the enterprise side because I talk to companies, very large Fortune 500 companies that are very far into the process, and they find it to be very expensive. So that's where I come up with my like. Well, the agencies haven't started yet, and they don't even know what they're getting themselves into and they have all these old hardware situations. Some of them may have to migrate to the cloud, who have avoided it for years and years. Like there's a whole bunch of things out there that are just going to be super expensive for agencies to deal with. On the consumer side, I think it's. I actually don't think it's going to be as expensive on the consumer side. I think the IoT issue probably in some cases is and some of the hardware issues are probably more a little bit you know they're going to have to be upgraded and that's where the expense is going to be. But a lot of the basics are in the cloud already, so it's going to get upgraded. So I mean, if you I don't know you haven't given the numbers yet of like where the percentage of traffic that you see that's I mean

Vincent Voci 59:20
We are so non-human traffic, agentic traffic that's at about 30% that's post-quantum encrypted today. Human traffic, it's just over you know 65%. We see somewhere between 20 and 30% of the internet, so it's all that's a lot of traffic. We've turned that on for free. You won't see any sort of markup from Cloudflare when it's post quantum cryptography, like not in our enterprise solutions, not in the the free solutions. CISA, to your question on like where to go, I can't. I probably shouldn't call out specific companies, but CISA, the Cybersecurity Infrastructure Security Agency, they published a PQ. Product list, or like kind of vendor categories, like types of products that are going to be higher risk, higher profile types of devices. Like throw that into Gemini or Copilot, and kind of figure out who's at the top of the list there. So basically, I think there's

Ari Schwartz 1:00:15
going to be a long tail, and at the end of the tail, it's going to be expensive. But I think to get to the tail, it's actually for consumer stuff. It's probably not going to be that expensive. It's just the tail that's expensive, but for enterprise that's avoided things or that has runs into issues, it's going to be super expensive. And that's where we have to be. We have to brace ourselves for that. Okay, I don't think we have time. I think we got to cut it there. But I'm supposed to tell people to take cookies back to your office and to your family, that we have plenty of them, and

they are dated for today. So you need to take them and get rid of them. Thank you, and and join me in thanking the panelists. I really appreciate it.