That's the point. Yeah, it's not a few things that we kind of still not entirely clear about the paper. Unfortunately the dude, you know, the specific difference between measurement device and device

is actually be that devising a measurement device dependent assumes the police pursuit of dimensionality of the Hilbert space of the system that is being measured for instance in device-independent. You don't make any assumption which is a Hilbert space of assistive could be a photon and that we don't care you'll get up with Sigma X Sigma y you just have a system and you get an outcome. That's all that's device-independent.

Now I guess although I think I might be wrong. But I guess that measurement device independent is when you

you say I'm going to measure three dimensional system. Okay, but I don't.

You know if I'm measuring Sigma X or Sigma X every tilted or sigma's at okay?

That's my guess but let's see if I can see.

So you have any particular question or we threaten some questions here so we can ask you and he asked me yeah. Okay. Yeah, I guess let me just read the abstract first. Yeah, of course.

What means to relay this is these things that pass on the signaling?

the artists involved

okay.

Can I hear one of your questions? Yeah, I guess first question used to be in your opinion how important you think demonstration of measurement device Independence has

I think it's important because you know

There is there is no such thing as security if it always requires some assumptions. Okay, if the adversary is god that can know everything you you are not going to be able to do secure communication. So you need some assumptions. Okay, what are the limitations of the adversity maybe adversary is constrained by the laws of physics also or more because phrases and the type of

Feed the Bears experimentally available or even in the market nowadays you is good. It works well, but you have to trust the device, okay.

And and they don't work. Actually I would say that what they do commercially now is not is not network is just to point communication not relating to him and if you trust the by sense you you can you can see the communicate. Okay. Now if I

I went to communicate and I want to be sure that my communication is not spying is my being inspired by some bursary party and I I may not necessarily trust the the company that makes it a license. Okay. So this is this is

that theoretically that there are methods to be able to

device independent security, but it's not yet practically available. Okay. It's ready to loophole free Bell experiments and things like this now the

but yet so in between what we have in in the market and we have in theory, you know is this race but from experimentalists and engineers and companies and I think that this is a good step in that direction. Okay. Also, this has the thing of network stuff, which I'm not an expert. But yeah, I suppose that not everything is just to party communication. You may want to do other cryptographic tasks other type of communication or thanks of cryptographic protocols. So yeah, that's also so this is good.

In these two directions and saying that in the more General applicability than just to point communication and some steps towards device-independent.

constructions

this is useful when I'm saying very easy really really is the key also for longer distance for things that

If you want to print it yet these there are these.

the existing procedures they have a few kilometres of

okay distance because they don't have repeaters or relates. Okay. So this is a limitation. So I suppose that dealing introducing relays also opens a positive and making it secure because once you put a relay

You open the door? Because the release of control by Alex robot? Okay, it's something totally out of the helps. So you open deposits on our way on one hand you can.

Increase the distance between the parties the hottest parties, but you introduced Maybe.

An advantage to a potential adversary that you have to to analyze. What's what can the adversary do if she has control over the relay? Okay, maybe if you do things cleverly, there is not much that you can do.

The tiger indicates that they think they've got it.

So also even in the simplest case of edid for when you don't have relays you may think that if the adversary has the optical fiber in between and can measure and prepare everything you may think that's enough for breaking protocol.

Anytime it turns out not to be the case. So yeah, I mean when you think you can do you can analyze what will be the optimal attack and still be protected against this?

Yeah, and then the next question would be what issues might arise when you scale up and out and then bi Network to a city size population is in. Yeah what the scaling issues associated with it and we are network.

I don't know that so you ask what are the issues what for scaling this year?

I mean love you for instance, like used. I think it's three users and one relay in this experimental setup. I think they're proposing, you know, you could then just keep adding users.

so we're not really sure how what

yeah that depends on the analyses of Errors how they have or

Yeah, I don't know about this. Uh, I know about want to repeat this and so this is when you want to just have two parties, but extend the input quantity of it has and yeah actually errors add up in a pretty bad way for me to get Peters. Okay. So although is something that it may be the solution for long.

It's something that they are people still being developed such as oh, let's do that problem solved.

So I do the existing long-range sort of Arrangements. They have a contour Pizzeria couple of kilometers sort of things that are sort of thing. Yeah, they're also long-range things with satellites because the atmosphere gets the

Upwards okay. So

if you are able to get above the dense (atmosphere), in almost free space, the signal is less vulnerable to attack.

Dr. Cerf, he mentions that slices. Well, I think he said that that might be a potential next step to sort of demonstrate a satellite version of this network that can go into the quite as much detail as to why it would be so beautiful things. Yeah.

“Well, the satellites are very convenient, because otherwise, when the network is big, you need to build lots of optical fibres, for instance”

Well the satellites and a very convenient thing because even they are around when the network is officially beak.

You need to build.

Optical fibers from and as I said

in

The atmosphere is pretty dense for free space. I mean there are also experiments with free space Community institution. But yeah, even it depends on the atmospheric conditions is not good. I mean you need to go inhales bad beliefs. That's okay. You can do a one kilometer. I don't really know that.

So years ago it was about less than but yeah, once you go above the dense part of the atmosphere.

You just feel you know meters. I don't know.

you know the density decreases exponentially As You Are

So yeah, then it's pretty much something for everybody in satellites are around is like TBS. I mean you just you will find some above so it seems

I mean it's an expensive thing. But once you have it on there is really for everybody GPS.

But yeah still not by any means is not there. But yeah.

He's very he's not far away. They're saying

yeah.

Yeah, I guess I'll next question would be unless you have mentioned yesterday that measurement device Independence is the ultimate approach to Quantum key distribution. And I guess which website Kona that bit and whether you think there's any competition to where there's any competition to.

Yeah, I would say measurement device independent is not the last thing the last thing is device-independent. Yeah.

So what happened with the rise in the bed and I think abandon means that I don't care. What is my Black Box? So I have a laptop. I trust my laptop and then my laptop has a USB connection to the to the box and the Box basically what it does is with a another box that Bob has almost No Malice and there is a box somewhere else. The two boxes do like bellick Spectrum data being that experiments. Okay, so my laptop is feeding which inputs of an experiment in doing and getting out.

getting out the outcomes of the experiment Okay, so

A perfect so then I don't care what is going on inside the Box? Okay. So really really really that I'm going to say this is not actually the case but it seems that I could really the boxes could really

Deliciously constructed here if I have that statistics. I'm not okay. I there's no way someone can spy on my signal communication and and at the same time obtain that statistics and violates that inequalities. Yeah. Okay. So with this method seems is the best in the individual Securities the best people have done.

Even more I mean you could even not need to so in the present days people trust the validity of quantum mechanics and the part and the validity of the particular 12 modeling of these boxes. Okay. Now as you make the measurement device independent or just pure device independent of there is also semi device-independent is another one part is device-independent and the other trusts devices. Okay. So yeah, there are these different levels but let's suppose that say that the maximum one is just device-independent the one

Some many qualities. So yeah, this seems to be the ultimate thing but actually is not the case because

if if I really don't know if I really have no idea what's going on in the Box, what the box could be doing is yeah the particle genuinely regenerating statistics that violates our inequality and hence the adversary cannot be prepared that beforehand but the Box could be broadcasting the outcomes.if that's the case, then I cannot do Secret communication, but

clearlly there can exist logically is logically impossible to have any method of secret Communication in which my devices broadcasts the value of a secret key. Okay. So then in the devence of the device independent is that saying easing is to say that it Is the most secure framework

But in a in a in a given that you define the problem in a way that it is possible at all to to do it. Okay, if my device is broadcast my secret key. Yeah. I mean, it's not about doesn't matter what you do. I mean it's impossible.

So yeah, so it's though the name device-independent is correct.

Some claims in some papers maybe even some of my paper saying that you could just get the devices from the adversity. There's actually accurate so you should steal.

You still trust devices

with some Central isolate them or seal them in some way.

but yeah, but it makes the ice independent makes very good proof because you know, even if I trust my device and I have a particular model where I measure Sigma X and sigma said, you know after a month this Sigma X will be a bit misaligned. Okay, and you will have no choice and you will have you will have a model exactly advice. So what seems to write a security proof that he's amazed on that is based on a model is okay to do physics based on a Model but it's not okay to do security proofs based on a Model you want to do know how it behaves a true thing. Not just a model. It's not all modeling for photography is not okay modeling. You need more than modeling so and device independent security proofs using Bell's theorem get around this, okay?

Yeah, I think about your toast to my yesterday as well.

I think yeah, you've covered question for a bit with satellites. What would you think? Yeah. So the question is what what the next steps to achieving the sort of thing they're going for but we talked about Suspects.

Actually, I think you also dressed question 5, which is about time frame for you, huh general public with what you said about satellites as well because you and if you had to give a general time period between now when the general public will have access to Quantum key distribution just a rough number.

okay, if I have to say

Amber

I would say it could be possible.

In 15 years (it might be possible) just to say something. Yeah, but I don't think that in 15 years our society will have this (quite yet).

In 15 years (it might be possible) just to say something. Yeah, but I don't think that in 15 years our society will have this

it will take you know, I'm just making this.

Yeah. Appreciate Oxford. Well, I was gonna add hope that did you have anything else first?

I don't know your first well, I was just going to say asked if you knew that other things that might be pertinent of happened in the interim since 2016 3 all the things that have happened since 2016 either. Okay, in terms of will ever own terms of taking this any further sort of it.

Yeah, and to go into them all the time because I'd the reason why device Independence is so valid is for Network such as that's in the paper to know to know what you're getting receiving is based on what you are sending yourself. If that is that why it is so secure and adding to that is that why one of the assumptions is that you fully know your own state that you are sending?

So now you you ask me that see if I understand are you asking about the particular just more of the actual process the actual process of a measurement device independent? Yep, and how it relates to how that

of some of the loopholes associated with standard qkd

so just explain maybe so these

the way this works is by you know, you had some sort of reflection of the state you send the state and it comes back or I think that it's from what I gather there's each each user the network sends their state to the central relay and the central real like Farms about measurement and from the outcome of that and knowing your own State you sent you can work out what the other person is sending to you. Yeah. Yeah.

Yeah, it is. I understand if you're not now, what is the question?

why this is better than