Constellations Podcast

Episode 136 – Post Quantum Hacks, Quantum Key Distribution for SmallSats and the Fully Entangled Future

Speaker: Dr. Mark Adams, Associate Professor, Electrical & Computer Engineering, Auburn University – 18 minutes

John Gilroy:	Welcome to Constellations the podcast from Kratos. My name is John Gilroy, and I'll be your moderator. Today, we are at the SmallSat Show in Logan, Utah. During today's podcast, we'll discuss the basics and just the basics of quantum information processing, how quantum key distribution, QKD, ups the game in data transmission security, and moving from the BB84 scheme to fully entangled sources for small satellites. Wow. To help us maybe try to understand this complex topic, we have invited Dr. Mark Adams. He's an associate professor of electrical and computer engineering in Auburn University Samuel Ginn College of Engineering and also assistant director of the Alabama Micro/Nano Science and Technology Center where he established the STORM lab. Nope, not Oklahoman tornadoes, this is a different storm. This is an acronym that stands for sensors, transducers, optics, RF, and MEMS. The STORM team focuses on progressing the technology of quantum key distribution. Boy, you sound like you're a Spock or something, with all this background. That's incredible.
Dr. Mark Adams:	Well, thanks for a host to me today, John. I certainly appreciate it. We do a lot of fun things in the lab.
John Gilroy:	Yeah. I guess yeah. Reputation out there and all the smart kids want to apply and work with old Mark, huh? Excuse me, Dr. Adams too.
Dr. Mark Adams:	Well, yes. They have to call me Dr. Adams. You're fine calling me Mark.
John Gilroy:	Well, here's the easy questions. Try to take you 30 hours to answer this, but you got try to give us like a normal human being answer. So, what is quantum information processing?
Dr. Mark Adams:	So let's start with classical information processing to kind of set a baseline. So, everything you do today pretty much revolves around some type of information and taking that information and making reasonable decisions with it. Classical computing for instance, the things you use on your PC, your laptop, your phone, those all just harness the properties of classical electronics and classical communications in order to make that happen. So what's the difference between quantum and classical? Well, when we start introducing quantum, we start to access properties that are unavailable in the classical realm. And so by

KRATOS

taking these inaccessible properties and leveraging them for quantum systems, we're able to do some pretty unique things that you can't do on a, kind of standard classical technologies.

John Gilroy: Yeah. I read this morning and you try to take and harness some rules of nature or some natural processes. Is that right?

Dr. Mark Adams: That's correct. And so back at the turn of the 20th century, in the 1900's, right? When quantum mechanics was really coming into existence, the theorist posturized that there was all these interesting properties that we could take advantage of if we could just figure out a way to harness them. And so these natural properties are things that now, we as engineers, have learned to harness and apply to more traditional processing. So the QKD, for instance, we're going to talk about today is just a quantum way of doing encryption. So it's all interesting.

John Gilroy: You think about the 1900, there were so many smart physicists that all just popped out. It's like it was springtime for physics.

Dr. Mark Adams: Oh, it was incredible, right? I mean, you just look at the number of just phenomenal intellects that existed from night, really the end of the 1800's to the early 1900's, 1920, 1930's. I mean, of course everyone knows Einstein, but there were so many more in that period of time.

John Gilroy: I'm sure your students have read Thomas Kuhn's book, The Structure of Scientific Revolutions. He talks about this, like two people been the forum at the same time. And so, we know breakthroughs were made around 1900, many areas and one was quantum. And so, this isn't the new kid in the block. This has been around a while.

Dr. Mark Adams: Absolutely.

John Gilroy: Maybe for our listeners, maybe give us some examples of how quantum information technology has been implied in the past.

Dr. Mark Adams: Sure. I think one of the things that people need to realize is that you interact with quantum systems on a daily basis you probably just don't really realize it. And so, lighting for instance, is one that comes to mind, fluorescent lights. Fluorescence is a quantum phenomenon. And so, if you didn't understand how that worked, you wouldn't be able to take advantage of the light bulbs that are in the ceiling right now. LEDs, once again, quantum phenomenon.

John Gilroy: Really?

Dr. Mark Adams: Lasers, most of the micro electronics technology we leverage today really stems from quantum mechanics. And so, there's just tremendous examples throughout the past of how we've leveraged that to really progress society from a technological standpoint.

John Gilroy: Who knew, huh?

Dr. Mark Adams: Yeah. I mean, I think people just overlook it and there's a good reason why don't get me wrong, right? Not everyone needs to understand the fine details of how all that works. They just need to be able to leverage and take advantage of it.

John Gilroy: So we have a concept of quantum mechanics and the whole idea of quantum is fine. And we're going to talk about applying it to one area of science, one area of mathematics, what are you going to call it? And this is quantum key distribution or QKD. Now I'm so old, my math teacher used to put QED at the end of the chalkboard there.

Dr. Mark Adams: Yeah. Chalkboards.

John Gilroy: So QKD.

Dr. Mark Adams: QKD.

John Gilroy: So, quantum key distribution. So we set the stage for quantum. Now we're going to up it up to key distribution, right?

Dr. Mark Adams: Correct. So we're going to take advantage of some of these properties to improve the security of communications. So let me set the stage just a little bit in terms of why it's important. So, most people are probably at least heard of quantum computing and the fact that quantum computing is coming online, maybe in the next five to 10 years, depending on who you talk to. Existing security relies on algorithmic type encryption techniques, which means we have a really hard equation we want to solve in order to encrypt data. That works perfectly fine with modern day computing. It's hard to crack it. It's hard to actually hack that quantum or that encryption. The problem is quantum computing because of it takes advantage of these quantum properties can do it very quickly. So as soon as those quantum computers come online, traditional encryption techniques are kind of go to the wayside. Pretty much all civilization knows that at this point. And so, most government entities are interested in finding ways to do what's known as post quantum.

John Gilroy: Ah.

Dr. Mark Adams: Yeah. So one of these is to actually take advantage of the quantum properties themselves to make it resilient against these type of quantum intercepts that can be done. So, QKD is just that. We're taking advantage of the quantum properties in order to create a secure communications technique that a quantum computer can't really hack.

John Gilroy: Another old fashioned analogy is, so you see the train coming and quantum's going to be a big impact. So they're thinking of alternatives to trying to maybe stop some of the impact of.

Dr. Mark Adams: That's correct. To get ahead of it.

John Gilroy: Like breaking your cryptography today.

Dr. Mark Adams: Absolutely. Everyone relies on cryptography. When you pay your bills online, right? You're expecting that data to be secure.

John Gilroy: Those Israeli guys, RSA guys, we're kind of relying on them and that's kind of the standard now and and so they're... Actually, human beings doing something preventative. I mean, is that's true?

Dr. Mark Adams: Yeah. I know. Now it's crazy.

John Gilroy: A breakthrough.

Dr. Mark Adams: Yeah.

John Gilroy: So, I go down to the old Best Buy and I walk out with a little computer and I start doing this technology on a standard garden variety computer. So what kind of infrastructure is needed to support this Q E D in a satellite or on the ground?

Dr. Mark Adams: Yeah. So it's a little bit more technologically advanced than you can buy at Best Buy.

John Gilroy: Oh, come on.

Dr. Mark Adams: I wish it wasn't. I really do. I would love to be able to just get buy it off the shelf. So, what we're doing currently with our scheme is relying on quantum optics. And so, we're using optical generation of photons, which is the quantum of light in order to do this quantum key distribution. And we're using a protocol called BB84 which was established by Brassard and Bennett, 1984, that's where the 84 comes from. So once again, been around a while, right? I mean, this isn't a new thing, but putting it into a small satellite is a fairly new thing. And so, a lot of what we're working on is taking the technologies that have been developed and demonstrated in labs over the past 30 years in reducing the size, weight and power, the kind of the swap as we like to call it, in order to put it into the size of a boom box.

Dr. Mark Adams: And so there's a lot of engineering that has to go into that. From a technological perspective, though, what we're doing is we're using the properties of light in their quantum nature in order to secure the communications by sending a secure key. And so we can go into the details of that in a little bit, but that's what we're trying to do right now with our satellite.

John Gilroy: I'm sure Auburn has computer science majors, and I'm sure they're forced to take courses in PKI, understand public key encryption and go back and forth with whole history of that. And so what you're saying is that, this is just a different way to improve that encryption. So if I take out my iPhone I'm pretty secure, but this makes obviously if it's a military application has to be the best encryption possible, doesn't it?

Dr. Mark Adams: That's correct. And so, one thing that all these techniques allow, so when we talk about QKD, they allow you to detect eavesdroppers. And so you can tell when someone's listening in on your conversation. And so that's a big deal, right? And so, you can imagine if we want to spy on someone else, we don't want them to know we're spying all them. So, these techniques allow us to know precisely that someone has monitored that distribution.

John Gilroy: Well, here we are at Utah State, let's go over and grab a computer science major and cyber security 101 is the man-in-the-middle attack.

Dr. Mark Adams: Absolutely.

John Gilroy: I mean, it's been around since forever, the man-in-the-middle.

Dr. Mark Adams: Absolutely the man-in-the-middle.

John Gilroy: And so normally this describes Bob and Alice and Eve, which is eavesdropping, man-in-the-middle or the person in the middle, but the man-in-the-middle attack. And so, there are ways that are designed with traditional systems to prevent man-in-the-middle and we can learn... They're in textbook now, they're literally in textbooks now, but there's no textbook for some of this stuff. It's really kind of new and applying it as brand new, isn't it?

Dr. Mark Adams: Yeah, it is. It's a relatively new field. I will say this, it's a little bit more developed for terrestrial applications. And so for instance, there's a number of companies now that are introducing quantum key distribution for optical networks, but those are fiber networks. And so, you've got to have Alice and Bob joined by fiber optic. That's not really practical for everything, right?

Dr. Mark Adams: I mean, you guys focused on communication from space. How do you do this from space? Well, that's what we want do, right? We want to show that we can do the same thing you can do through a traditional fiber optic cable and do it from a lower orbit satellite to a ground station on space.

John Gilroy: And if your students go to YouTube and type in QKD, you're going to get a whole lot of applications on fiber and talk about many meters and that many meters and you go, "Hey, wait, what about thousands of meters?" "Well, we can't have a cable going all up to."

Dr. Mark Adams: That's exactly right. No, we can't. And so, we want to be able to make this more accessible, right? So, the best way to do that is put it in space, right? If we have an operational system in space, then it's accessible anywhere on the planet.

John Gilroy: I love the Royal we, especially at universities, "We, and so your team, we are building a special proprietary open source QED system." Is that what's going on?

Dr. Mark Adams: It is, yeah. We're actually here presenting it at SmallSat. So, this is a project that's been funded through the University Nanosatellite Program, which is sponsored by the Air Force Research Lab. And so, we're doing this technology demonstrator, which will allow us to show that the key components of QKD can be accomplished from a small set. It's tough. I mean, it's tough. Now, a lot of this has been demonstrated in the past with larger satellites. You may be familiar with a Micius satellite, which was put up by the Chinese in 2016, it's a 600 kilogram satellite. So a large satellite, that was able to do this kind of QKD that we're trying to do with a 12-U CubeSat. So something, like I said, the size of a boot box. So, it's a lot of a challenge there.

John Gilroy: You used the magic phrase ‘AFRL’ and my ears perked up. And I thought, "Brainiac." It's the first word that came my mind. And I've talked to those folks over there and they study everything. For example, with the aircraft, they study, we have a plane on a desert, 140 degrees, it's got to go up 20,000 feet, then go back down. They look at extreme conditions, don't they?

Dr. Mark Adams: They do.

John Gilroy: So they have to test wire endurance for extreme conditions. They have to. I would imagine that in your endeavor, you have to test for extreme conditions as well.

Dr. Mark Adams: We absolutely do.

John Gilroy: So that's part of the, "Oh, we have the satellite. And what are the weather conditions in the satellite?" I mean, cold? Yeah.

Dr. Mark Adams: Absolutely. So, we do a ton of testing. And so at Auburn, we have the capabilities to do all the environmental testing that's necessary for small satellites. So we can test what the satellite would see on orbit. We can obviously test different types of environmental conditions. We can test vacuum. We also can test magnetic fields. So we can pretty much simulate what the orbit would look like for the small satellite. Now, the one great thing about small sets is they have short missions, right? We're not expecting them to stay up for 25 years.

Dr. Mark Adams: We're expecting them to stay up for six months to a year. So, we don't have to have the resiliency that you would have in a large scale commercial satellite, but it still has to work. I mean, I kid my students all the time. It's like, "We're not going to launch a space brick." Right? We need the satellite to work, so we have to fully test it and characterize it on Earth.

John Gilroy: Mark, thousands of people from all over the world have listened to this podcast. Go to Google and type in “Constellations Podcast” to get to our show notes page. Here, you can get transcripts for all 100 plus interviews. Also, you can sign up for free email notifications for future episodes. Well, Dr. Adams, humble John Gilroy is going to give you some advice, recruit some physics majors. Because my experience with physics majors is, we have to build a machine to test, and they'll build the machine right in front of you and to test it and that's not going to be an obstacle at all for a physics major. They just going to plow right through it.

Dr. Mark Adams: Well, John, we have a number of physics major on the team.

John Gilroy: Oh, good for you. You’re putting a good team together then.

Dr. Mark Adams: Yeah, we have a very large team through our student program. We have the Auburn University Small Satellite Program it's student led. It combines teams from physics, engineering. Pretty much any type of stem field.

John Gilroy: At Auburn, we say, "You can't have all quarterbacks on your team. Can you?"

Dr. Mark Adams: Can we get one?

John Gilroy: Give them one, it looks good. Yeah. Well let's talk about a different team. The Chinese team. I think maybe a couple years ago, 2020, there was some researchers may I saw press release for something about they released their QKD technology. So big deal, speed bomb or?

Dr. Mark Adams: Well, so one thing that Chinese government has done is put a tremendous amount of money, significant investment into quantum. It caught the U.S. off guard, I think a little bit. And so, we're starting to really ramp up our investment in quantum technologies. We had been relying on the commercial industries to really push quantum computing, but the other types of quantum, quantum communications, quantum sensing, those kind of things, we were kind of caught, I think on a back foot by the Chinese when they put this up. And so, they definitely showed that they were a little bit further ahead in some of the space born technologies for quantum communication.

John Gilroy: So the questions, how does your approach differ from theirs?

Dr. Mark Adams: So, one of the things that we're doing is, as I mentioned, we're trying to shrink it. And so, they have a single test bed satellite around 600 kilograms. It's a fairly high altitude satellite. And so, we would like to be able to do this across a constellation of satellites in low Earth orbit to produce global coverage, right? They have a single system up in space right now.

John Gilroy: Degree of difficulty much higher.

Dr. Mark Adams: Yeah. However, the technologies are similar, right? So, the fact of the matter is, all of these techniques were developed as I mentioned in the eighties or in early nineties. And so, from a quantum optic standpoint, we've known from a laboratory how to do this for quite some time. It's a lot harder moving it from a laboratory to a spacecraft, moving it from a spacecraft to a small set. So to me, it's the next generation of what they've done. To do it in a much smaller spacecraft.

John Gilroy: Well, I talked about the physics majors and I'm going to talk about the English majors at Auburn. Now they've all read George Orwell, and he wrote a book about 1984, didn't he?

Dr. Mark Adams: He did.

John Gilroy: He thought it was an apocryphal year. Well, guess what? It was.

Dr. Mark Adams: To some degree.

John Gilroy: Because of BB84, right?

Dr. Mark Adams: Yeah.

John Gilroy: And your role's got to be. So I read this article and thought something about BB84 and someone maybe you, made a prediction that, "Probably by 2024, well maybe to launch this project." So, good prediction, bad prediction or?

Dr. Mark Adams: We definitely hope so. By maybe late 24, early 25, as you guys know COVID has kind of done a number on everyone. And so, we have experienced some delays due to the pandemic, but we're making very good progress.

So I do think that we're on track to see like a late 24 early 25 launch.

John Gilroy: So our friend George Orwell tried to predict the future? So I'm going to have you do the same thing, buddy. You're probably as smart as he is understanding quantum. So, what exciting developments plans do you see in the next few years for you and your team? Or maybe just as transition away from BB84?

Dr. Mark Adams: So for starters, we really want to get away from optical communications for the keeps. So, as you guys probably know for optical comms, satellite to satellite optical comms works really well. You don't have the atmosphere to attenuate it. You don't have clouds, you don't have dust, but as soon as you start to try to get a key from space to the ground, all those artifacts start to impact you, right? "It doesn't work real well if it's raining. It doesn't work real well if you're in a dust storm." You need secure reliable communications. So the next step for QKD, is to transition away from optical photons to microwave photons. And so, we want to do microwave comms. You guys understand microwave comms, right?

John Gilroy: Yeah.

Dr. Mark Adams: So, we want to be able to do the exact same thing we do currently using microwave technologies for high speed communications, except for apply them to the QKD problem. So, we've got efforts ongoing right now to do that. So we're really interested in developing entangled microwave sources to do quantum key distribution.

John Gilroy: Well, I think this interview is going to get a lot of applications to join your program. I mean, covered all the bases here. It's really an interesting interview. I think what you've done here is you've helped our listeners untangle some quantum concepts.

Dr. Mark Adams: I hope so.

John Gilroy: I'd like to thank our guest Mark Adams, Auburn University, associate professor electrical and computer engineering as well as assistant director, Alabama Micro/Nano Science and Technology Center. Thank you, Mark.

Dr. Mark Adams: Well, thanks so much, John. Thanks for having me.