00:00:00  
*Speaker 1:* Great. And. So can you tell me a little bit about yourself and your background in cybersecurity?

00:00:09  
*Speaker 2:* So I do research on, uh, cryptographic protocols. So protocols that use cryptographic primitives to ensure certain security guarantees. And uh, I've been doing that for 15 years. They focus on, um, protocols for privacy preserving computation and, uh, consensus. Uh, and um, also blockchain consensus. So that's what I do in cybersecurity.

00:00:43  
*Speaker 1:* So how does how does cryptography play a role in modern cyber warfare. And what are the key challenges in securing national infrastructure?

00:00:55  
*Speaker 2:* Well, cryptography is needed for essentially every kind of communication over insecure networks, which are all the networks we have. So you need proper cryptographic protocols to ensure that communication among um institutions, both governmental and private, remains, uh, confidential and uh, and retains integrity. And, uh, it's a key component of any, um, secure communication solution.

00:01:35  
*Speaker 1:* So how would you describe the current state of the cybersecurity in Denmark based on the cryptographic knowledge?

00:01:50  
*Speaker 2:* Um, I, I'm not sure if I know how to answer this. As I said, I do theoretical research. I don't know how the intelligence community or the government is, uh, dealing with this. Uh, um, in general, at least I know that, um, uh, Denmark is a highly digitalized country. So most of, uh, public services are using information systems and those demand protection. So there is a good, uh, data protection authority established in Denmark. But, uh, in terms of cyber warfare, I have no idea what is being done. I don't work with intelligence.

00:02:40  
*Speaker 1:* So what are the most effective cryptographic techniques for defending against state sponsored cyber attacks? So, like, what is the best way to secure information?

00:02:53  
*Speaker 2:* Um, so it depends on exactly what you're trying to do with that information. If you're just trying to send it from point A to point B, or if you're trying to compute on that information, or if you're just trying to make sure that no one, uh, changes some publicly available information. We do have a number of standardized protocols that can be used for secure communication, and the best idea is always to stick to the standards and not come up with their own schemes.

00:03:25  
*Speaker 1:* So what are the biggest cybersecurity risks posed by the small information leak, and how can they be exploited in cyber warfare?

00:03:35  
*Speaker 2:* By what information leak?

00:03:37  
*Speaker 1:* Yeah, by a small information leak. How does it impose, uh, the risk on the cyber warfare.

00:03:49  
*Speaker 2:* But I don't understand what what what kind of information leakage. You mean any information leakage?

00:03:54  
*Speaker 1:* Uh, so, for example, if we have the healthcare and we have the patient data.

00:04:01  
*Speaker 2:* Yeah.

00:04:04  
*Speaker 1:* So how can the leak of the personal information can be imposed by the cyberwarfare, and how can it be exploited?

00:04:14  
*Speaker 2:* Well, any information leakage can be exploited by, uh, adversaries and bad actors. It depends on exactly what they managed to leak. But if you manage to leak, for example, secret keys used to encrypt information, that's bad, because now the the adversary is able to read the information you're trying to securely transfer or store.

00:04:45  
*Speaker 1:* So how can secure multi-party computation be optimized for scalability and large scale applications like blockchains.

00:04:57  
*Speaker 2:* Well, uh. Secure multiparty computation can be used to compute, uh, any arbitrary function on private inputs. The way to make it more efficient and scalable so far is to actually construct specific purpose protocols for specific functions that are more efficient than the protocols that can compute every single function. So usually you would, um, construct the specific purpose protocols that will give you better performance for the specific functions you want to compute in a in large scale.

00:05:36  
*Speaker 1:* Can you give a couple of examples? For example, if you ever had to experience a cyberattack on the script?

00:05:50  
*Speaker 2:* A cyber. Sorry, a cyber attack on the script. What do you mean?

00:05:54  
*Speaker 1:* So, for example, if the actor tried to intercept the key.

00:06:03  
*Speaker 2:* Well, I do theoretical research, so I don't deal with cyber attacks, I prove theorems.

00:06:13  
*Speaker 1:* So basically, how does information theory contribute to strengthening modern cryptographic cryptographic security?

00:06:25  
*Speaker 2:* Well, do you mean information theoretical cryptography there? There is a it. There's a number of protocols that are based on information, theoretical, uh, tools. And um, we can also use them to achieve better efficiency in some protocols. Uh, besides, um, achieving better, uh, security. Uh, as you probably know, using purely information theoretical tools is not efficient in practice because then you need to have keys as large as the messages you are encrypting and so on. But it is possible to benefit from information theoretical techniques when constructing protocols that have computational security but achieve better efficiency or scalability or or security as well.

00:07:22  
*Speaker 1:* Do you have any advice? How what is the best way to store passwords and what is the most secure way to do that? So how is better to encrypt them?

00:07:35  
*Speaker 2:* It's not really my area of research, but the best idea is usually to use a good password manager with one very long, strong password that you can use to access the passwords in that password manager. Instead of trying to store any local database of passwords that you created yourself. So that's the the good practice at this point.

00:08:06  
*Speaker 1:* So can you explain how do quantum computing threats influence the design of future cryptographic protocols?

00:08:16  
*Speaker 2:* Uh, yes. So quantum computers, uh, would if we are able to construct a quantum computer that is large enough and stable enough, it would be able to run an algorithm that solves some of the problems, the computationally hard problems that underpin the most widely used cryptographic algorithms that we have now. So a large enough, stable enough quantum computer would be able to break our current, um, our most widely used cryptographic primitives and protocols. Um, so this is indeed a threat if this if such a computer is built. Uh, just it's important to note that we are still many orders of magnitude away from constructing such a computer. I mean, current quantum computers have very small number of qubits, and they're very unstable. So they wouldn't be able to run this algorithm. Um, but the solution to that is actually constructing new, uh, cryptographic primitives and protocols based on problems that are still hard, even for quantum computer.

00:09:39  
*Speaker 1:* Can you make an example?

00:09:42  
*Speaker 2:* Uh, for example, the LWE problem, that's a problem defined on a mathematical structure called a lattice. Um, you can use it to construct digital signatures, encryption, key exchange protocols, and so on. That would, uh, be still secure against the quantum attacks. To the best of our knowledge.

00:10:10  
*Speaker 1:* So can you name me the trade offs that exist between the decentralization, security and efficiency in privacy preserving blockchain applications?

00:10:23  
*Speaker 2:* Oh, unfortunately, there aren't that many deployed privacy preserving blockchain applications. Right. There's a few, um, uh, projects like Zero Cache, uh, and, um, Monero and, um. What else? Well, Concordia was also running with a shitload of transactions. The the trade off that you get is that doing transactions that are privacy preserving takes more space and more computation. And doing standard transactions with no privacy. Uh, just because you need heavier tools in order to achieve this privacy guarantees.

00:11:11  
*Speaker 1:* So how do quantum computing advancements impact the security assumptions of classical cryptographic protocols?

00:11:20  
*Speaker 2:* Uh, that's what I already told you, that, uh, quantum computers that are large enough and stable enough would be able to run an algorithm that can solve problems that underpin the security of the most widely used cryptographic primitives.

00:11:39  
*Speaker 1:* So how do the quantum safe cryptographic protocols compare in terms of performance and scalability for real world applications?

00:11:49  
*Speaker 2:* The current, as we call them, post-quantum secure, um, primitives and protocols. They do have a overhead in relation to the widely deployed schemes that we use right now. They require larger signatures, larger ciphertext and so on and more computation. But they are already at a level that you could deploy them in the real world. It's not that much slower or bigger that would make it impossible to use.

00:12:28  
*Speaker 1:* So can you make an example of, for example, like the. I would say potential risks of quantum computer being developed and, for example, how can they affect the digital structure of Denmark? Since we use the method to log in into the governmental website, what.

00:12:56  
*Speaker 2:* If a quantum computer that is large and stable enough is developed? It's not going to affect just meet ID, it's going to affect everything, because every communication over the internet requires cryptographic primitives and protocols that can be broken by a large enough quantum computer if we deploy them with our current, uh, deployed constructions. So that's why there's a lot of effort right now in constructing post-quantum secure cryptographic primitives that are not affected by a quantum computer.

00:13:30  
*Speaker 1:* So what will be the key challenges in design is a post-quantum cryptographic algorithm that balances security and efficiency.

00:13:41  
*Speaker 2:* Well, the biggest challenge is not actually designing them. They already exist. We have already designed them. The key challenge is doing the transition to those, uh, algorithms, uh, standardizing them and deploying them in real world applications. Uh, and, and getting away from the, the algorithms that could be broken by a quantum computer.

00:14:07  
*Speaker 1:* So what role does the lattice based cryptography play in mitigating the threats posed by the quantum computers?

00:14:16  
*Speaker 2:* A lattice based cryptography is based on problems that cannot be easily solved by a quantum computer. So they can you can construct cryptographic primitives that could not be easily broken by a large enough quantum computer.

00:14:32  
*Speaker 1:* So what would you suggest to implement in, uh, for example, like in the large firm that has to secure information and has to defend from the quantum computer attack. So what will be the best way to secure data?

00:14:53  
*Speaker 2:* As usual, the best is to implement standardized protocols and primitives. So the Nest uh Institute has created now a standard for post-quantum secure cryptography. And that's the best way to go using primitives from that, from that standard.

00:15:13  
*Speaker 1:* So what strategies can government and critical infrastructure entities adopt to future proof, say, cryptographic security against quantum threats?

00:15:26  
*Speaker 2:* Oh, they need a migration plan. They need to start playing. Uh, how planning now. How to, uh, migrate their systems to use polls to post-quantum secure algorithms?

00:15:41  
*Speaker 1:* Can you make an example?

00:15:45  
*Speaker 2:* Of, uh, you or what? I don't I don't understand, uh, an example of, uh, of migration to post-quantum secure primitives.

00:15:56  
*Speaker 1:* Yeah. For example, what would you suggest.

00:15:58  
*Speaker 2:* Uh, for, uh, say, the TLS protocol that everyone uses for all communication over the internet? Um, it would make sense to start by migrating, uh, web servers and, uh, the browsers and clients used within this large or organizations to use post-quantum secure cipher suites in the TLS protocol so that the information exchange via the TLS protocol is secure against one of computers.

00:16:37  
*Speaker 1:* So let's say that there is a quantum threat. What such organisation is it you can do to recover from it?

00:16:51  
*Speaker 2:* Recover from what?

00:16:53  
*Speaker 1:* From quantum attack.

00:16:56  
*Speaker 2:* Oh, uh, there is no difference between a quantum attack or any other kind of attack. If an attack happens and information is leaked or information is modified, it doesn't matter if it was quantum or not. And attack is a problem, regardless of how the attackers succeeded in performing the attack. Uh, so there is nothing special about quantum attacks or the the, the risk of, um, quantum computers is that they if a large enough quantum computers built, then it would be able to break the primitives that we believe to be secure right now. But if a primitive is broken, regardless of it's by a quantum attack or classical attack, and its security guarantees are, um, no longer, uh, valid, then uh, or whatever organization that is using it needs again to migrate to a new primitive that is secure against, uh, the current existing attacks, be they classical or quantum.

00:18:03  
*Speaker 1:* So what would you suggest would be the first step to recover from the any kind of cyber attack? And, uh, for example, there was a cyber attack and the information is leaked. So how can we secure that the actor will not get the access to it? So how can organization.

00:18:24  
*Speaker 2:* If the information has been leaked already. There's nothing else you can do. The information is leaked. How are you going to prevent. Prevent someone from accessing information if it's already leaked? The only thing you can do is find the vector that this attacker used and fix it. But the information has been leaked. There's not much you can do. I mean, by law, you have to notify the the data subjects and data owners related to that information, that their information has been leaked. Um, but there's nothing you can do. The information is already leaked.

00:18:58  
*Speaker 1:* But for example, in Danish health care systems, there is a CPR numbers. Yeah. And they're relatively easy to I would say to know which way would you suggest will be better to. To encode them to prevent them from leaking.

00:19:24  
*Speaker 2:* Oh, well, you should just. It depends on what you're talking about. I mean, you're talking about sending CPR numbers over the internet, or you're talking about storing CPR numbers on a server. I'm not sure. What do you mean?

00:19:40  
*Speaker 1:* Basically, I'm talking about the storing them on the server and the communication between the hospitals. They send it over the email sometimes some of the doctors. So how can we preserve this information?

00:19:56  
*Speaker 2:* Just stick to the standards. Use the TLS protocol for every communication over the internet and over any insecure network. And then you're fine. And for storing the information on the on the server, then, uh, use standard, uh, hard disk encryption techniques so that someone who gets physical access cannot just extract this all from the hardest.

00:20:27  
*Speaker 1:* So how would you assess the risk of potential information breach in the health care institutions in Denmark right now?

00:20:40  
*Speaker 2:* I cannot assess that because I don't know what measures they are using. I don't know what systems they are using. I don't know what their procedures are, so I cannot assess that.

00:20:54  
*Speaker 1:* Can you say something about it using.

00:20:57  
*Speaker 2:* I also don't know what the IT department at Ai2 is doing. We don't work with them. I mean, we, they, they, you know, it's a different it's a completely different department that runs the I.T infrastructure in ITU. I don't know what they are running. I don't know what systems they use, what procedures are in place, what security policies are in place. So I cannot assess that.

00:21:25  
*Speaker 1:* So what would you say about the cryptography role in the modern society?

00:21:33  
*Speaker 2:* Well, it's fundamental for guaranteeing basic civil rights to privacy and to, um, data sovereignty and and to make sure that you can actually, uh, control your data in a society where all data is just spread around multiple distributed systems and sent around, over and secure networks without cryptography would not be able to do that.

00:22:00  
*Speaker 1:* So what does it so which role does it play in the information security?

00:22:09  
*Speaker 2:* Well, it plays a central role. You cannot have any information security without cryptography.

00:22:17  
*Speaker 1:* So basically. What risks can be posed if the public information is being encrypted, and which risk can the owner's information have?

00:22:37  
*Speaker 2:* Well, even if something is encrypted, you still need to have proper key management because if the key leaks, then information can be accessed. So that's one of the main risks.

00:22:51  
*Speaker 1:* How would the cryptography affect the national infrastructure, the national security infrastructure.

00:23:03  
*Speaker 2:* Uh, how it would affect the national security infrastructure.

00:23:06  
*Speaker 1:* Yeah.

00:23:08  
*Speaker 2:* Uh, well, it is already used in the national security infrastructure, right? It's you use cryptography every time you want to send any data over the internet without the data being corrupted or intercepted. So I trust that it's already being used. That's essential. Like I said, you cannot get secure communication without cryptography.

00:23:32  
*Speaker 1:* What is the best way to encrypt the communication?

00:23:38  
*Speaker 2:* Uh, so you need a protocol that makes sure that both confidentiality and integrity guarantees are achieved. Like I said, the best way is using standards using the TLS protocol.

00:23:54  
*Speaker 1:* Okay. I don't really have any more questions since okay.

00:23:59  
*Speaker 2:* So always for the the forum. So sign it and send it to you.

00:24:04  
*Speaker 1:* Okay. Great. Yeah. Thank you so much.

00:24:06  
*Speaker 2:* You're welcome. Bye bye.

00:24:08  
*Speaker 1:* Yeah. Have a nice day.

00:24:09  
*Speaker 2:* You too.