Interviewer: Can you tell me a little bit about yourself and your background in cybersecurity?

Researcher: I do research on cryptographic protocols—protocols that use cryptographic primitives to ensure certain security guarantees. I've been doing that for 15 years, focusing on protocols for privacy-preserving computation, consensus, and blockchain consensus.

Interviewer: How does cryptography play a role in modern cyber warfare, and what are the key challenges in securing national infrastructure?

Researcher: Cryptography is needed for essentially every kind of communication over insecure networks, which are all the networks we have. You need proper cryptographic protocols to ensure that communication among institutions, both governmental and private, remains confidential and retains integrity. It's a key component of any secure communication solution.

Interviewer: How would you describe the current state of cybersecurity in Denmark based on cryptographic knowledge?

Researcher: I'm not sure I can answer this properly as I do theoretical research. I don't know how the intelligence community or the government is dealing with this. In general, Denmark is a highly digitalized country, so most public services use information systems that demand protection. There is a good data protection authority established in Denmark. But in terms of cyber warfare, I have no idea what is being done—I don't work with intelligence.

Interviewer: What are the most effective cryptographic techniques for defending against state-sponsored cyber attacks? What is the best way to secure information?

Researcher: It depends on exactly what you're trying to do with that information—whether you're sending it from point A to point B, computing on that information, or ensuring no one changes publicly available information. We have a number of standardized protocols for secure communication, and the best idea is always to stick to the standards and not come up with your own schemes.

Interviewer: What are the biggest cybersecurity risks posed by small information leaks, and how can they be exploited in cyber warfare?

Researcher: Any information leakage can be exploited by adversaries and bad actors. It depends on exactly what they managed to leak. If they manage to leak secret keys used to encrypt information, that's bad because the adversary can then read the information you're trying to securely transfer or store.

Interviewer: How can secure multi-party computation be optimized for scalability and large-scale applications like blockchains?

Researcher: Secure multiparty computation can be used to compute any arbitrary function on private inputs. The way to make it more efficient and scalable is to construct specific-purpose protocols for specific functions that are more efficient than protocols that can compute every

single function. You would construct specific-purpose protocols that give you better performance for the functions you want to compute at large scale.

Interviewer: What are the trade-offs between decentralization, security, and efficiency in privacy-preserving blockchain applications?

Researcher: Unfortunately, there aren't many deployed privacy-preserving blockchain applications. There are a few projects like Zcash, Monero, and Concordium. The trade-off is that privacy-preserving transactions require more space and computation than standard transactions with no privacy, because you need heavier tools to achieve these privacy guarantees.

Interviewer: What is the best way to store passwords and encrypt them securely?

Researcher: 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. This is better than trying to store any local database of passwords that you created yourself. That's the good practice at this point.

Interviewer: Can you explain how quantum computing threats influence the design of future cryptographic protocols?

Researcher: Quantum computers, if we are able to construct one that is large enough and stable enough, would be able to run algorithms that solve some of the computationally hard problems that underpin our most widely used cryptographic algorithms. This would break our most widely used cryptographic primitives and protocols.

It's important to note that we are still many orders of magnitude away from constructing such a computer. Current quantum computers have a very small number of qubits and are very unstable, so they wouldn't be able to run these algorithms. The solution is constructing new cryptographic primitives and protocols based on problems that are still hard even for quantum computers.

Interviewer: Can you give an example?

Researcher: For example, the LWE problem, which is defined on a mathematical structure called a lattice. You can use it to construct digital signatures, encryption, key exchange protocols, and so on that would still be secure against quantum attacks, to the best of our knowledge.

Interviewer: How do quantum computing advancements impact the security assumptions of classical cryptographic protocols?

Researcher: As I mentioned, quantum computers that are large enough and stable enough would be able to run algorithms that can solve problems underpinning the security of our most widely used cryptographic primitives.

Interviewer: How do quantum-safe cryptographic protocols compare in terms of performance and scalability for real-world applications?

Researcher: The current post-quantum secure primitives and protocols do have overhead compared to widely deployed schemes. They require larger signatures, larger ciphertexts, and more computation. But they are already at a level that could be deployed in the real world—they're not so much slower or bigger that they would be impossible to use.

Interviewer: What would be the potential risks of quantum computers being developed, and how could they affect Denmark's digital infrastructure, such as MitID for logging into government websites?

Researcher: If a quantum computer that is large and stable enough is developed, it's not going to affect just MitID—it's going to affect everything. Every communication over the internet requires cryptographic primitives and protocols that could be broken by a large enough quantum computer if we continue using our current constructions. That's why there's a lot of effort right now in constructing post-quantum secure cryptographic primitives that are not affected by quantum computers.

Interviewer: What are the key challenges in designing post-quantum cryptographic algorithms that balance security and efficiency?

Researcher: The biggest challenge is not actually designing them—they already exist. The key challenge is transitioning to those algorithms, standardizing them, and deploying them in real-world applications while moving away from algorithms that could be broken by quantum computers.

Interviewer: What role does lattice-based cryptography play in mitigating threats posed by quantum computers?

Researcher: Lattice-based cryptography is based on problems that cannot be easily solved by quantum computers. So you can construct cryptographic primitives that could not be easily broken by a large enough quantum computer.

Interviewer: What would you suggest for large firms that need to secure information and defend against potential quantum computer attacks?

Researcher: As usual, the best approach is to implement standardized protocols and primitives. The NIST Institute has created a standard for post-quantum secure cryptography, and using primitives from that standard is the best way to go.

Interviewer: What strategies can governments and critical infrastructure entities adopt to future-proof their cryptographic security against quantum threats?

Researcher: They need a migration plan. They need to start planning now how to migrate their systems to use post-quantum secure algorithms.

Interviewer: Can you give an example?

Researcher: For the TLS protocol that everyone uses for all communication over the internet, it would make sense to start by migrating web servers, browsers, and clients used within large organizations to use post-quantum secure cipher suites. This would ensure that information exchanged via the TLS protocol is secure against quantum computers.

Interviewer: If there is a quantum attack, what can an organization do to recover?

Researcher: There's no difference between a quantum attack or any other kind of attack. If an attack happens and information is leaked or modified, it doesn't matter if it was quantum or not—an attack is a problem regardless of how attackers succeeded.

The risk of quantum computers is that if a large enough one is built, it could break primitives we currently believe to be secure. But if a primitive is broken, regardless of whether it's by a quantum or classical attack, any organization using it needs to migrate to a new primitive that is secure against existing attacks, whether classical or quantum.

Interviewer: What would be the first step to recover from any kind of cyber attack where information is leaked?

Researcher: If the information has already been leaked, there's not much you can do—the information is leaked. You need to find the vector the attacker used and fix it. By law, you have to notify the data subjects and data owners that their information has been leaked, but the information is already out there.

Interviewer: For example, in Danish healthcare systems, there are CPR numbers. What would be a better way to encode them to prevent leaks?

Researcher: It depends on whether you're talking about sending CPR numbers over the internet or storing them on a server. For communication, use the TLS protocol for every communication over the internet and any insecure network. For storing information on servers, use standard hard disk encryption techniques so that someone with physical access cannot extract data from the hard disk.

Interviewer: How would you assess the risk of potential information breaches in healthcare institutions in Denmark?

Researcher: I cannot assess that because I don't know what measures they are using, what systems they have, or what their procedures are. Similarly, I don't know what the IT department at ITU is doing—it's a completely different department that runs the IT infrastructure. I don't know what systems they use, what procedures are in place, or what security policies exist.

Interviewer: What would you say about cryptography's role in modern society?

Researcher: It's fundamental for guaranteeing basic civil rights to privacy, data sovereignty, and control over your data in a society where all data is spread across multiple distributed systems and sent over insecure networks. Without cryptography, we would not be able to do that.

Interviewer: What role does it play in information security?

Researcher: It plays a central role. You cannot have any information security without cryptography.

Interviewer: What risks exist even when public information is encrypted?

Researcher: Even if something is encrypted, you still need proper key management because if the key leaks, then information can be accessed. That's one of the main risks.

Interviewer: How would cryptography affect national security infrastructure?

Researcher: It is already used in national security infrastructure. You use cryptography every time you want to send data over the internet without it being corrupted or intercepted. It's essential—you cannot have secure communication without cryptography.

Interviewer: What is the best way to encrypt communication?

Researcher: You need a protocol that ensures both confidentiality and integrity guarantees are achieved. Like I said, the best way is using standards like the TLS protocol.