Speech draft

> Suggested guideline: Executive Summary; Problem and Motivation (ending with your novel contributions), Solution and Results/Conclusion.
>
> 8 mins

Slide1: Hello everyone, my name is Bingbing Liang, I am so proud of making a presentation with Xingjian Wang, and XinJing Guo to show our group study.

Today, We'll discuss how integrating Quantum Key Distribution and Grover's algorithm into IoT architectures which can enhance security and data processing efficiency. Let's start.

Slide2: As the number of smart devices increases, securing them against hackers becomes more challenging. The advent of quantum computing necessitates the development of new security measures to protect our IoT networks against both existing and emerging threats.

Slide3: To meet this challenge, we turn to quantum computing. Quantum Key Distribution offers a secure communication channel that's theoretically impervious to eavesdropping, based on the fundamental principles of quantum mechanics.

Slide4: Meanwhile, Grover's algorithm provides a quantum leap in data processing efficiency, reducing the time required to search through vast datasets. Together, these quantum technologies can enhance both the security and efficiency of IoT systems.

Slide 5: We present a new Architecture that uses these quantum computing tricks to keep IoT devices safe and speedy. Let's take a closer look at the architecture of our Framework.

Starting at the bottom in pink, we have our IoT devices—let's call them Devices A, B, and C. These are the everyday gadgets like sensors or smart appliances in homes and businesses. They continuously generate data, which is the foundation of our IoT network.

Now, let's follow the data as it travels up. Normally, this data could be vulnerable to hackers. That's where our quantum tech steps in. The data first goes through what we call **QKD Network Nodes**—you can see them here. These nodes use Quantum Key Distribution to turn regular data into encrypted data. This is like turning a postcard into a sealed letter that only the right person can open.

Once encrypted, the data heads to the Quantum Processing Units, shown in red. Think of these as super-smart computers that can do complex math problems super fast. Here, Grover's algorithm comes into play, making sense of the data at speeds traditional computers can only dream of.

After the data is processed, it's like we've found the needle in the haystack quickly and without tipping off any onlookers. This processed data is then sent to the **Cloud Center**, the green bar at the top. Here, it's stored securely and can be used to make smart decisions, like adjusting your smart home's temperature or managing a city's traffic lights.

And it's a two-way street. The Cloud Center can send commands back to the IoT devices. Again, these commands are protected by quantum keys, ensuring that our devices act only on secure, verified instructions.

Slide 6: Due to the quantum hardware still needing long time to go, we keep representing the Hybrid Quantum-Classical Computing Architecture. Imagine we've got a team that includes both a superhero and a wise old master. They work together to make sure our smart devices at home and work talk to each other without any bad guys listening and do their jobs super fast.

On the right, we have our smart devices, like sensors and switches, which gather info and do things like turning on lights.

In the middle, is where the superhero steps in. This is the QKD Node, where our data gets a super suit, making it invisible to anyone trying to sneak a peek. It's then rushed through our super-fast quantum computer, which is like the superhero's brain, figuring things out really quickly and storing them safely in the quantum database.

Over on the left, is where our wise old master does his work. He takes the super-processed data and adds his knowledge, keeping it safe in the regular database we've always used.

At the top, the application server is like the control tower, sending out orders to the smart devices based on the super-quick thinking of our superhero and the wisdom of the old master.

And all of this is connected to the cloud, that big space on the internet where we can get extra info and help from outside.

So, what we have here is a dream team of the old and the new, making sure our smart devices are safe and super quick.

Slide 7:

Integrating quantum technology into everyday devices is challenging. We're focusing on three main areas: making the necessary infrastructure affordable, enabling seamless communication between quantum and traditional devices, and developing scalable quantum algorithms. Each step is crucial for bringing this advanced technology into our daily lives, and we're making progress every day.

Slide 8:

This roadmap shows us where we're going and how each step leads to the next, bringing us closer to a future where quantum computing is a part of everyday life, making our devices more amazing than we ever thought possible.

Slide 9:

To sum up, we've taken a big step by mixing quantum computing with IoT to make devices safer and faster. We used two quantum tricks, QKD and Grover's algorithm, to create a super-strong shield against hackers and speed up data handling. It's not just an idea for the future—it's something that can change how we protect our smart devices right now.

Slide10:

Thank you for listening.