Written submission from Crypto Quantique (SEM0061)

Introduction

Who are Crypto Quantique?

Crypto Quantique has created the world's most secure end-to-end IoT security platform. At its heart is the world's first quantum-driven semiconductor hardware IP, called QDID, that generates multiple, unique, unforgeable cryptographic keys for devices manufactured using standard CMOS processes. The keys do not need to be stored and can be used independently by multiple applications on demand. When combined with cryptographic APIs from the company's universal IoT security platform, QuarkLink, the solution creates a secure bridge between silicon, device, software, and solutions provider.

The company, which is based in London, UK, was co-founded by Dr. Shahram Mossayebi (CEO), an expert in cryptosystems, and Dr. Patrick Camilleri (VP Research & Innovation), a semiconductor designer with significant experience in complex parallel computer systems.

Why are we submitting evidence?

The IoT Industry where we operate is heavily fragmented which means there are numerous companies implementing many technologies in a single industry. The arrival of legislation brings about minimal viable standards for these implementations. In this way companies can not cut corners and either refuse to implement basic security standards or leave it to someone else in the supply chain to figure out.

Written evidence

What is the current and future anticipated demand for common products built with semiconductor materials (e.g. computer chips) both in the UK and globally

1. The semiconductor industry is facing one of the largest chip shortages in living memory. Experts predict the chip shortage will continue into 2023 and possibly beyond. Semiconductors are largely manufactured in areas where COVID lockdowns have been particularly tough, like Taiwan, China, and South Korea. This is led to widespread shortages all along the supply chain, and governments like the US and Germany are considering expanding production ability in the future to diversify supply and decrease the reliance on global production.
2. Due to this many industries have had massive delays in consumer, military, and enterprise products. Along with this, more chips than ever are demanded even basic electronics, which are now including basic connectivity. With the emergence of web 3.0 technologies (Web 3.0 is an idea for a new iteration of the World Wide Web based on blockchain technology) which will require more computing power, leading to device upgrades and more strain on the semiconductor supply chain.

What is the UK's semiconductor supply chain and is this secure? If not, how can this be improved? What specific strengths does the UK have to contribute to regional or global semiconductor supply chains? How competitive is the UK within the global context of the semiconductor industry?

3. The UK has a very strong education system, with some of the best university institutions in the world. The emergence of computer science as a career in the last 30 years has caused these institutions to invest heavily in technology education. However, there is currently no production capacity in the UK for commercial-grade equipment. The UK only produces research-based hardware for these universities, and everything else is imported from other countries such as Taiwan.
4. These are just a few examples of legislative and standards efforts currently underway.
5. The European Union's Cybersecurity Act was adopted on 21st March 2019. California implemented a bill on 1st January 2020 to protect the privacy of personal information being shared through connected devices. Then, in February 2020, the Korea Internet and Security Agency published guidelines for how to IoT ecosystems need to meet the requirements of the country's Personal Information Protection Act (PIPA).
6. The UK has been consulting on how to introduce cybersecurity laws to protect smart devices and IoT infrastructure for the past couple of years. In April 2021 it announced its plans to legislate, based on feedback from the consultation. Under the planned legislation, customers must be informed, at the point of sale, for how long a smart device will receive security software updates. Manufacturers will also be banned from shipping products with default passwords and will have to provide a public point of contact to make it simpler for anyone to report a vulnerability. An enforcement body will be established and given the power necessary to investigate allegations of non-compliance and ensure compliance.
7. This work is part of a wider, longer-term push by the UK government to improve cyber security, which goes back to the launch of a National Cyber Security Strategy in 2016. Among the stated goals of that Strategy were to ensure that the majority of online products and services were 'secure by default' by 2021.

Are there opportunities for strengthening different parts of the current UK semiconductor industry? What are the potential weaknesses and strengths of the UK semiconductor industry to meet future requirements of electronic device manufacturing?

8. At the moment, there is no fabrication process technology available for commercial output in the UK. These machines and infrastructure require a huge amount of investment, running into multiple billions to get off the ground. They require specific buy-in from companies with the knowledge already. There are quite a number of barriers to entry on fabrication production, of which, cost and economies of scale are two large barriers.

In which industries does the UK not have an end-to-end semiconductor supply chain? Are there any opportunities for these supply chain gaps to be filled within the UK?

9. The UK currently has no end-to-end semiconductor supply chain in any industry other than some very minor research facilities in Universities. There are companies that provide services for parts of the supply chain but nothing connects those companies. One big opportunity would be to produce silicon or fabricate chips in the UK in the long term.

How can the Government strengthen semiconductor research and innovation? Are there any current areas of weakness in the present Government strategy to semiconductor innovation? Is there effective communication between the various stakeholders within the UK's semiconductor ecosystem?

10. The government could provide infrastructure and incentives for commercial enablement. At the moment any UK-based firm that wishes to produce silicon needs to use external fabrication facilities, that can ignore requests due to the size and location of UK-based companies and prioritise local companies instead.
11. The recent flurry of serious cyberattacks has made it clear that cybersecurity is fundamental to national security, not a 'nice-to-have' solution to a minor technical issue that is poorly understood by politicians. The introduction of billions of low-cost IoT devices to the internet has only increased the security challenge. Governments, international standards bodies, industry groups and more are now moving quickly to make IoT implementations more trustworthy. This is being addressed through the development of checklists, guidelines, standards, business processes, certification schemes, and legislation.
12. All this activity helps to build the sense that IoT networks will soon be much more trustable. What is missing from these approaches is a strong way of knowing that the devices that populate an IoT ecosystem are genuine and still under the control of the people who introduced them to the Internet. This can only be achieved through hardware, by embedding a unique and immutable identifier within a chip in every device whose presence can be used to verify the device's unique identity and set up the secure communications needed to protect it from being suborned. Until this is widely done, IoT security will remain a patchwork rather than whole cloth.

Does the UK have the required skills, talent and diversity to be able to boost its current semiconductor industry and to respond to future disruption?

13. The UK has the design skills for semiconductor, with Arm in Cambridge and many design houses across the UK. However like mentioned above the lack fabrication and foundry facilities is a major blocker to future ability to respond to disruption

What are the potential national security concerns or vulnerabilities in our semiconductor industry? How should the UK collaborate with the United States and European Union? What are the ramifications on other industries and the wider economy within the UK?

14. The semiconductor industry is heavily influenced in both direction and production by Asian countries. China and India are now key players in the technology ecosystem and either country becoming more hostile towards western countries would be extremely concerning. TSMC is one of the largest and best producers of semiconductor chips in the world, and is based out of Taiwan. Taiwan would be seen as a risk both economically and politically due to influence from China.
15. The UK should ally closely with the EU and USA to ensure they are in a strong position to counter any technological influence from emerging countries who might want to influence global supplies.

Is the Government currently providing the clarity and direction required to enable growth and security in the semiconductor industry? Are the right governmental organisations involved with ensuring effective development of our current semiconductor industry to thrive in the future?

16. The government has not had much direction in the technology sector, which has led to an overall lack of investment in hardware production facilities. The UK has been reliant on global markets for bleeding-edge technology. The government would need to speed heavily to catch up on this.
17. The second hurdle is education. You cannot achieve strong IoT security through software alone or trying to stitch it onto an enterprise IT network. The foundations of IoT security are hardware security. The common practice of injecting random numbers into the silicon chips that power IoT devices to create device identities and the cryptographic keys needed to connect to them is expensive and fraught with security loopholes. In many cases, companies are ceding control of their security to third parties, and they remain unaware of how vulnerable the injected identities and keys are to cyberattacks when they are stored in device memories. The only viable solution is to have the chips that power IoT devices generate their own unique, immutable, and unforgeable identifies within their silicon fabric. Several technologies have been developed in recent years to enable this and their adoption is gathering pace. We need a continuous effort to educate the industry about what's available and how to choose between the various options.
18. Third, we need to automate the process of managing IoT security. This has three elements. Provisioning, which means configuring devices to meet their intended purpose, onboarding – connecting them to services and applications on computer servers, and ongoing lifetime management, which can include firmware updates and revocation of devices if they are compromised or not longer needed.
19. IoT security, particularly cryptography, is complicated, but system users just don't have the time to learn about the intricacies. How people interact with IoT security must be made simple and accessible. After all, how many car drivers would there be today if everyone had to understand how internal combustion engines work before they were allowed behind the wheel? In recent years, there has been great progress in this area too, and there are several providers of software that automates some aspects of IoT security management, and even a few that can deliver on end-to-end security, from device-to-cloud.
20. Building trust, contributing to impartial IoT security education, and simplifying security processes through automation, will together democratise IoT security. Without these things, the promised benefits of the digital transformation of industry will remain beyond the grasp of many, and fear and uncertainty will remain.