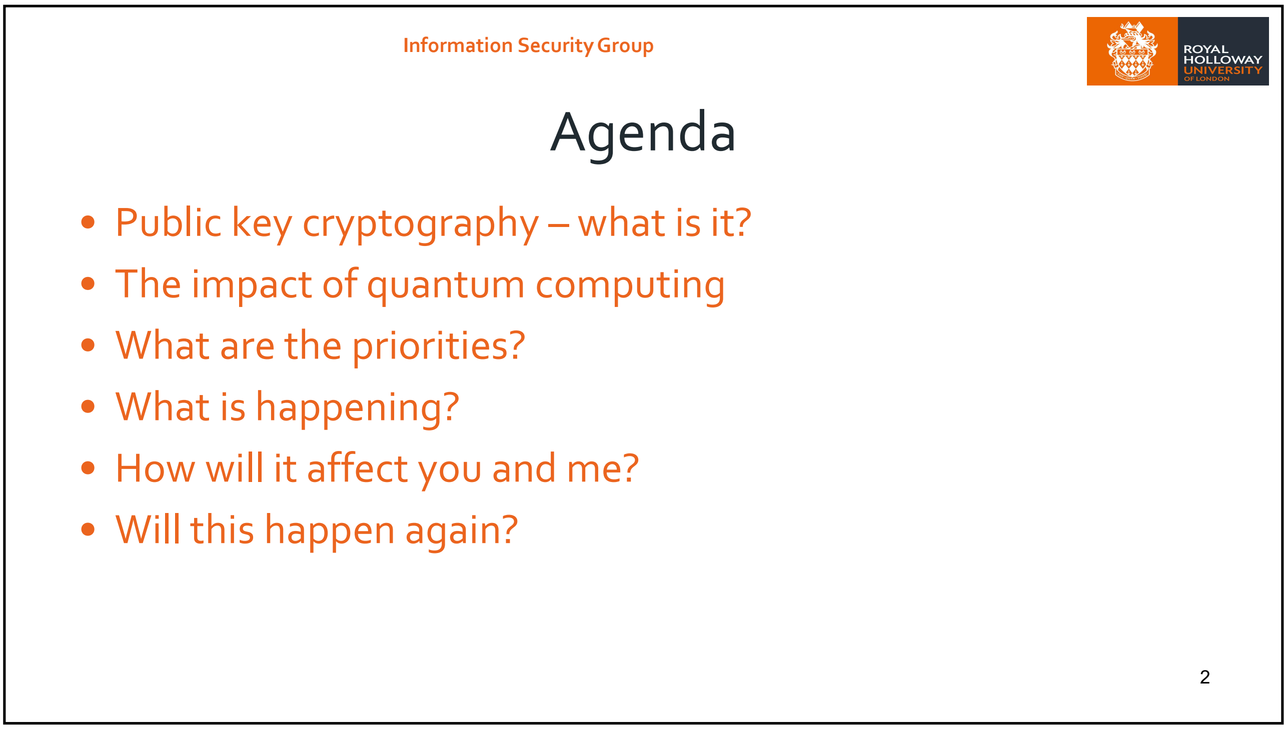
computing
conference 2024

Out with the old: The cryptographic revolution caused by the threat of quantum computing

Chris Mitchell
Royal Holloway, University of London

1



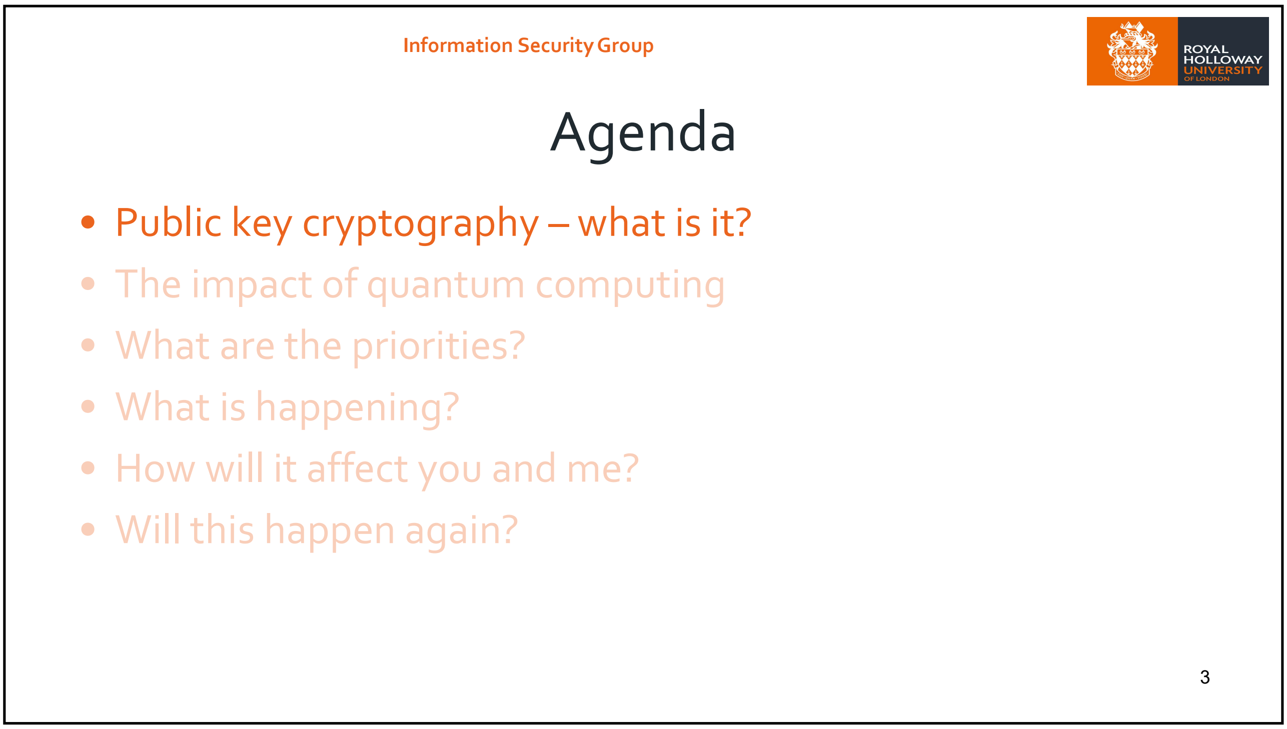
Information Security Group

Agenda

- Public key cryptography – what is it?
- The impact of quantum computing
- What are the priorities?
- What is happening?
- How will it affect you and me?
- Will this happen again?

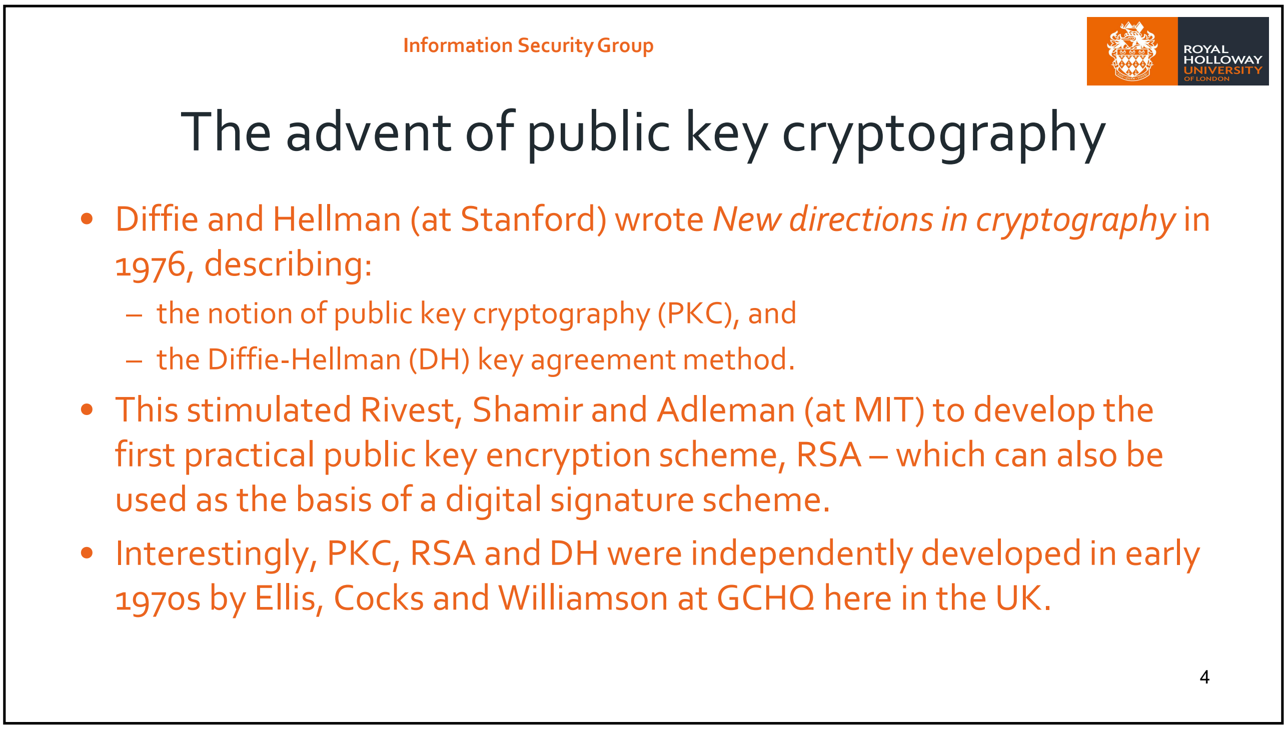
2

2



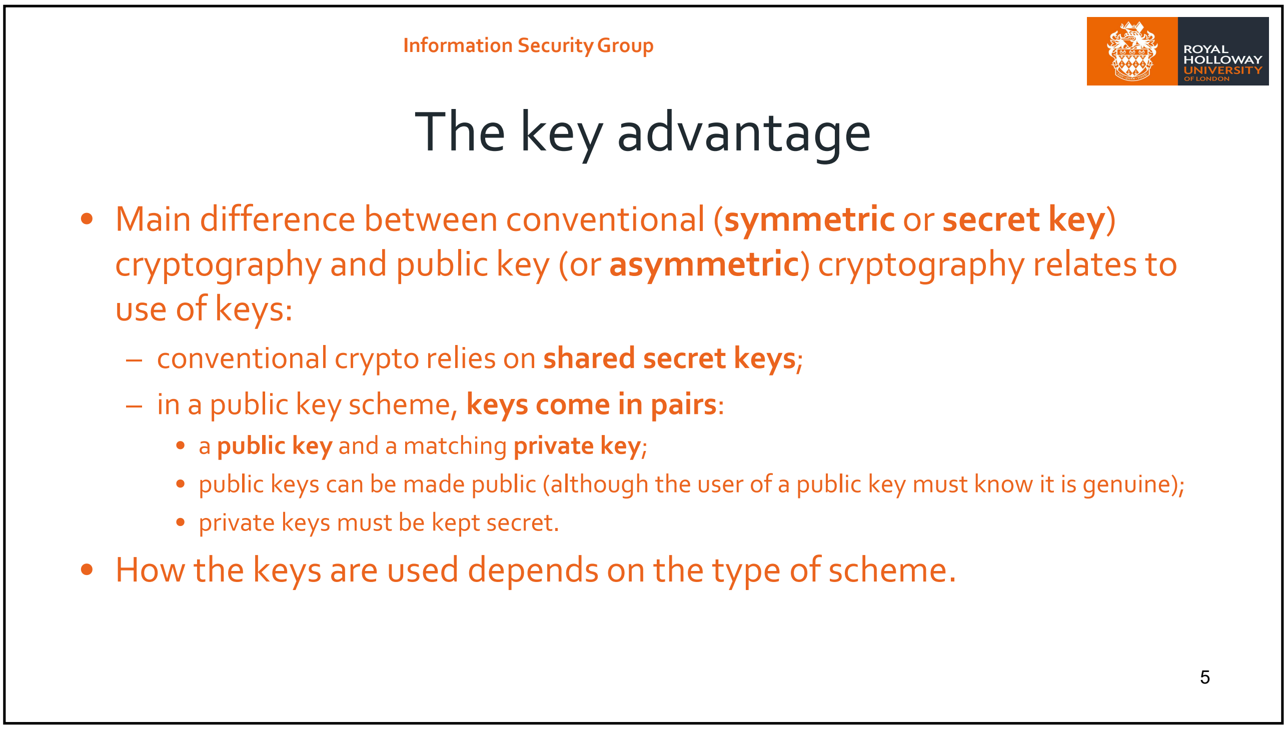
Agenda

- Public key cryptography – what is it?
- The impact of quantum computing
- What are the priorities?
- What is happening?
- How will it affect you and me?
- Will this happen again?



The advent of public key cryptography

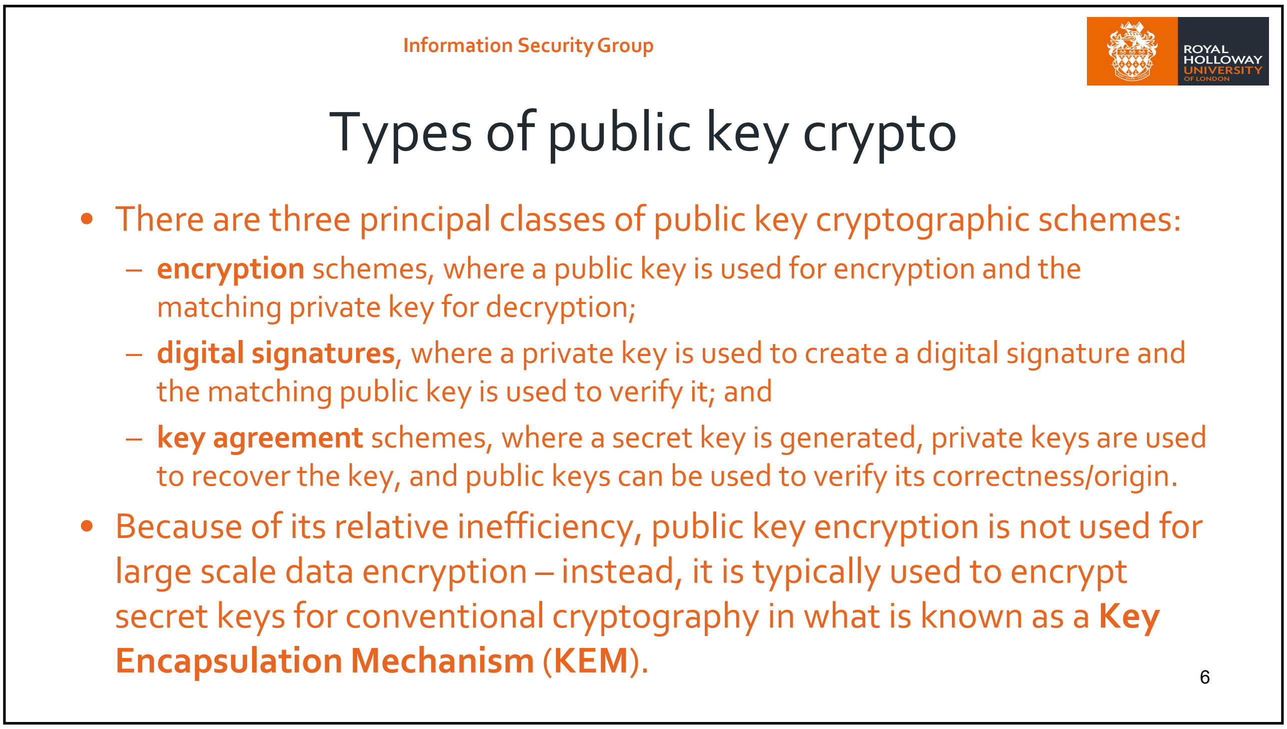
- Diffie and Hellman (at Stanford) wrote *New directions in cryptography* in 1976, describing:
  - the notion of public key cryptography (PKC), and
  - the Diffie-Hellman (DH) key agreement method.
- This stimulated Rivest, Shamir and Adleman (at MIT) to develop the first practical public key encryption scheme, RSA – which can also be used as the basis of a digital signature scheme.
- Interestingly, PKC, RSA and DH were independently developed in early 1970s by Ellis, Cocks and Williamson at GCHQ here in the UK.



The key advantage

- Main difference between conventional (**symmetric** or **secret key**) cryptography and public key (or **asymmetric**) cryptography relates to use of keys:
  - conventional crypto relies on **shared secret keys**;
  - in a public key scheme, **keys come in pairs**:
    - a **public key** and a matching **private key**;
    - public keys can be made public (although the user of a public key must know it is genuine);
    - private keys must be kept secret.
- How the keys are used depends on the type of scheme.

5



Types of public key crypto

- There are three principal classes of public key cryptographic schemes:
  - **encryption** schemes, where a public key is used for encryption and the matching private key for decryption;
  - **digital signatures**, where a private key is used to create a digital signature and the matching public key is used to verify it; and
  - **key agreement** schemes, where a secret key is generated, private keys are used to recover the key, and public keys can be used to verify its correctness/origin.
- Because of its relative inefficiency, public key encryption is not used for large scale data encryption – instead, it is typically used to encrypt secret keys for conventional cryptography in what is known as a **Key Encapsulation Mechanism** (**KEM**).

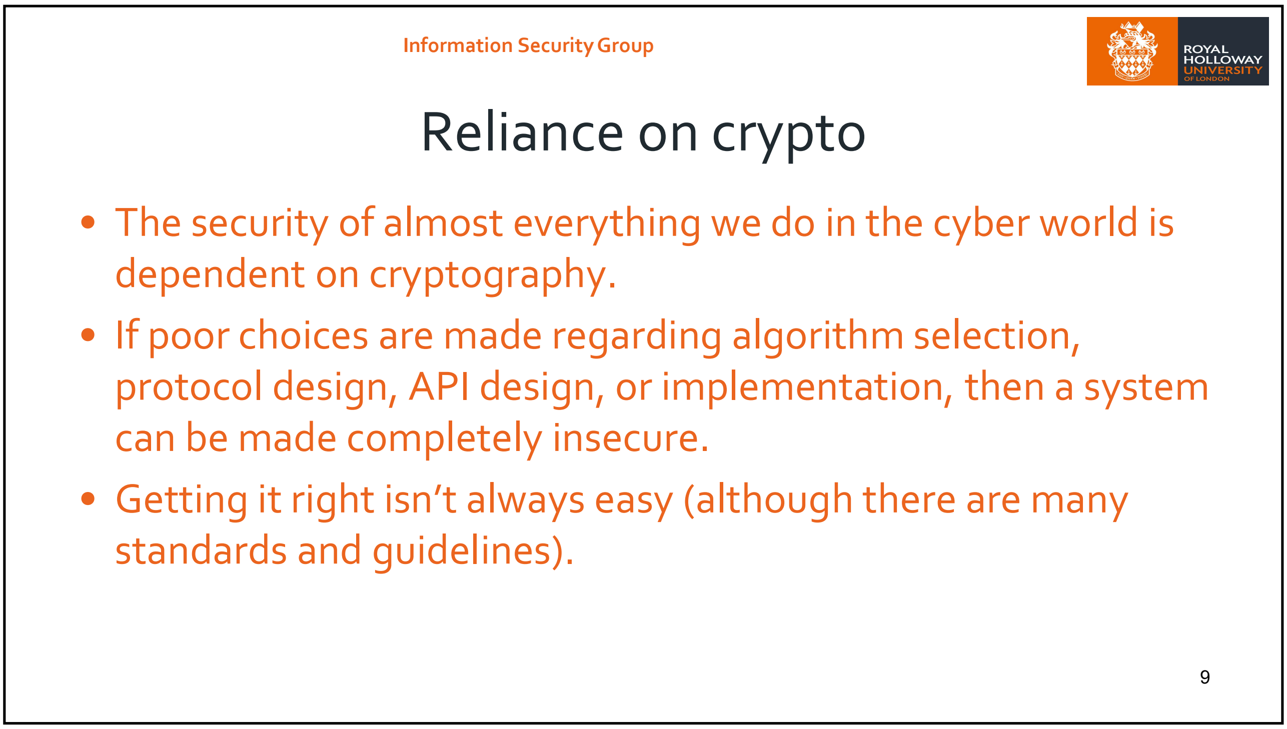
6

Today’s algorithms

- Over the past 30 years, two classes of public key cryptosystem have dominated:
  - **RSA** – used for encryption (e.g. RSA-KEM) and digital signatures;
  - **discrete logarithm-based schemes** – used in a wide variety of ways (e.g. DSA, ECDSA, ECIES-KEM, key agreement).
- Security of RSA rests on the **difficulty of factoring large integers**.
- Security of discrete log schemes relies on **difficulty of computing logarithms** in the chosen group (typically either a multiplicative group over a finite field or the group of points on an elliptic curve).

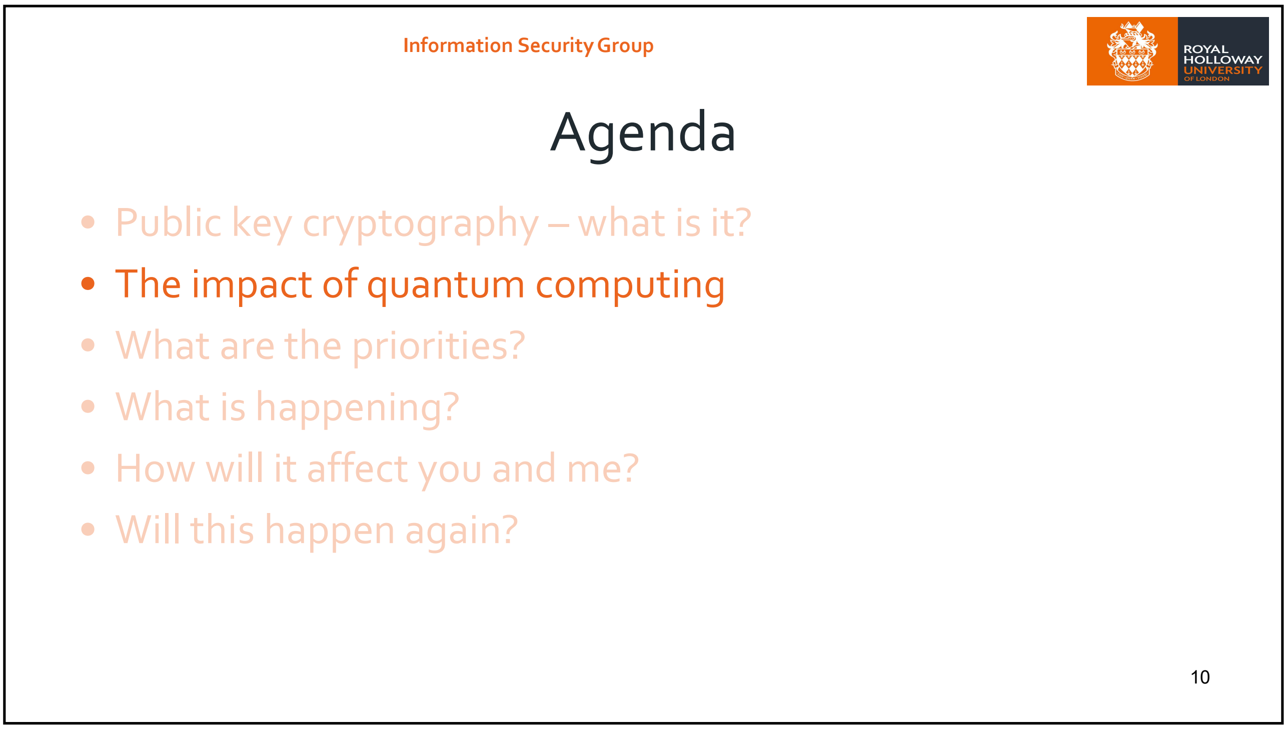
Pervasiveness of cryptography

- Today, cryptography is being used in almost every activity when using a payment card/app, phone, tablet, PC or Internet service.
- Examples include:
  - TLS almost universally used to protect browser-server interactions;
  - transparent full disk encryption and many other crypto services in modern OSs;
  - crypto-enabled proofs of identity including passports, identity tokens, etc.;
  - card payment security;
  - digitally signed software updates for many types of device; …
- All these applications involve public key (asymmetric) cryptography.



Reliance on crypto

- The security of almost everything we do in the cyber world is dependent on cryptography.
- If poor choices are made regarding algorithm selection, protocol design, API design, or implementation, then a system can be made completely insecure.
- Getting it right isn't always easy (although there are many standards and guidelines).

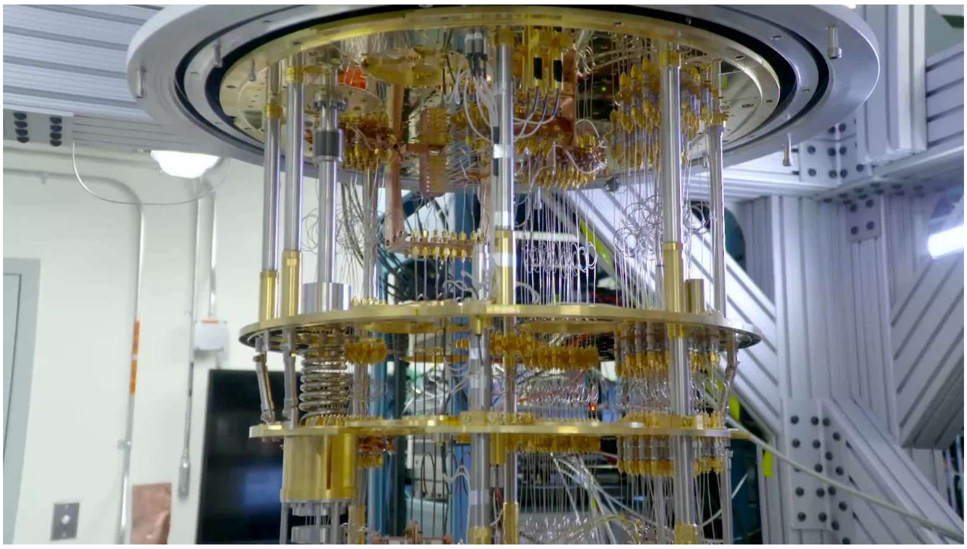


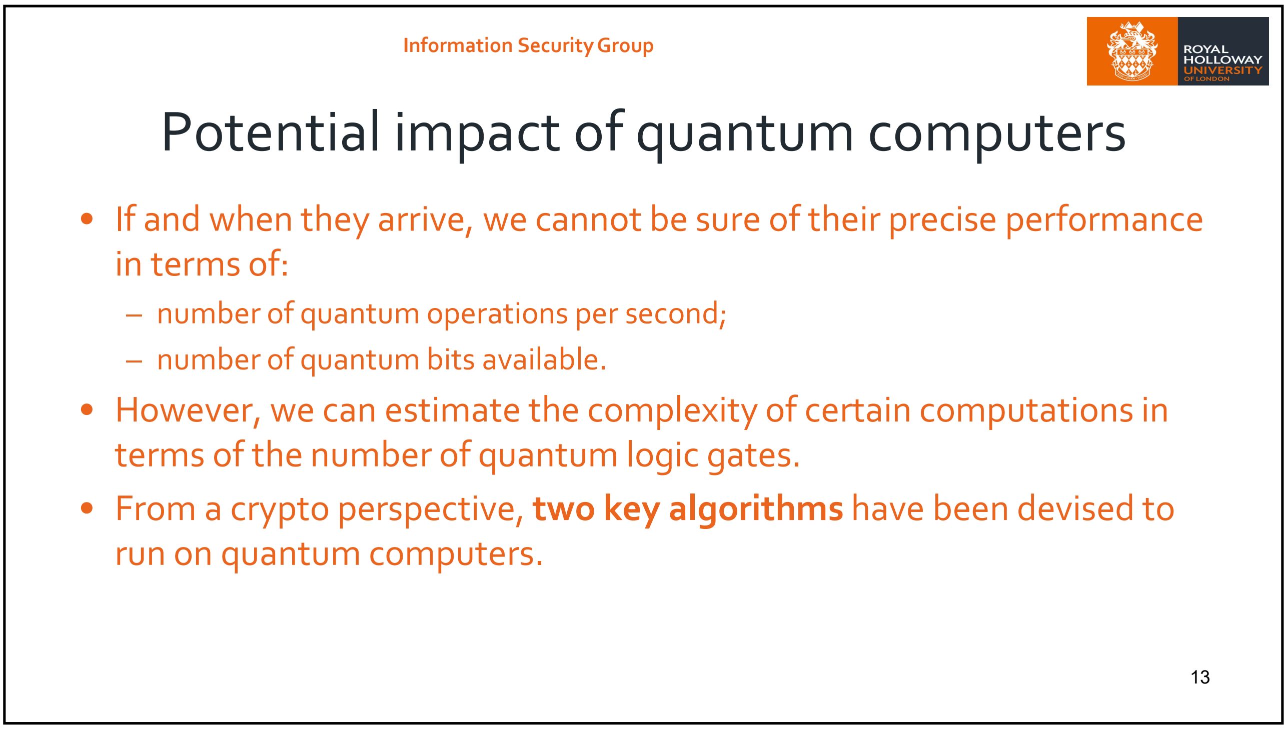
Agenda

- Public key cryptography – what is it?
- The impact of quantum computing
- What are the priorities?
- What is happening?
- How will it affect you and me?
- Will this happen again?

Quantum computers

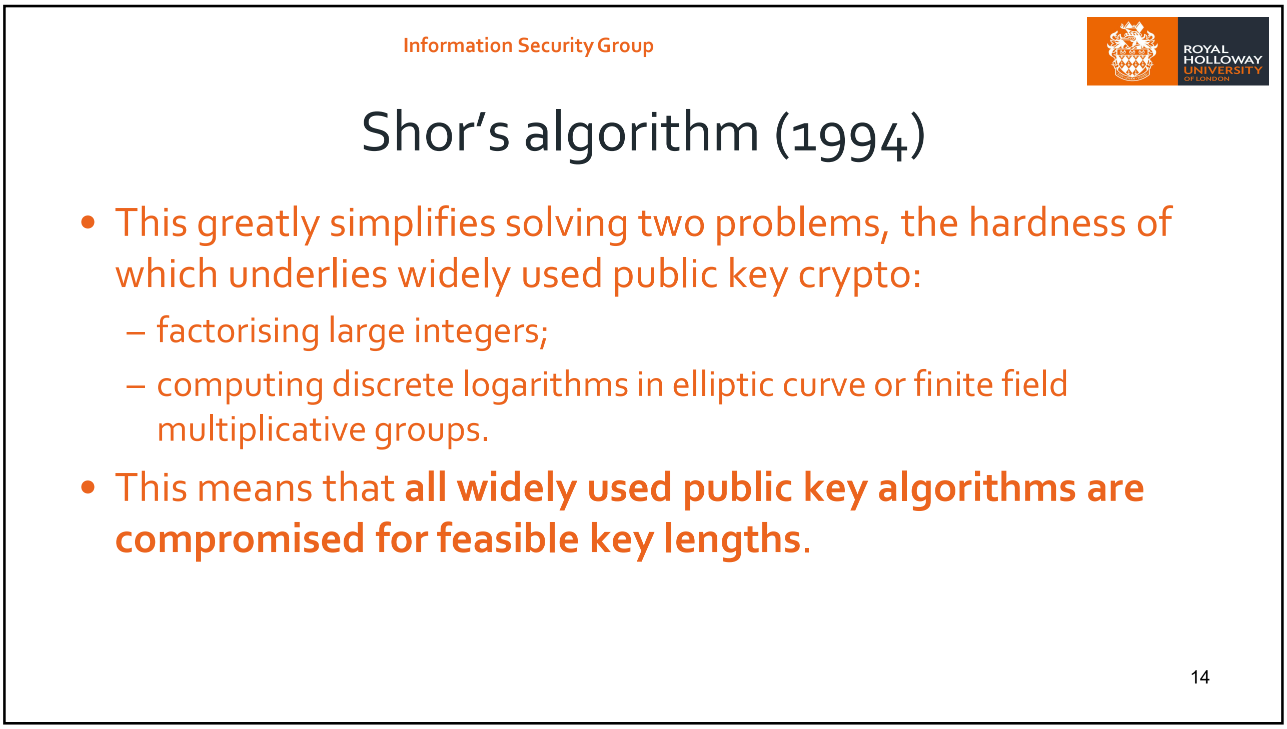
- In recent years there has been much discussion of the impact of quantum computing on cryptography.
- There is still no universal agreement that large-scale, general purpose, quantum computers will ever be built – see, for example, Dyakonov's March 2019 IEEE Spectrum article – but huge efforts continue.
- Year on year, progress is being made, with systems incorporating larger numbers of **qubits** (quantum bits, the basic unit of information in a quantum computer) – the current record is around 1000 qubits.
- Should such computers become available, they will have a major impact on the security of today's cryptography.





Potential impact of quantum computers

- If and when they arrive, we cannot be sure of their precise performance in terms of:
  - number of quantum operations per second;
  - number of quantum bits available.
- However, we can estimate the complexity of certain computations in terms of the number of quantum logic gates.
- From a crypto perspective, **two key algorithms** have been devised to run on quantum computers.



Shor's algorithm (1994)

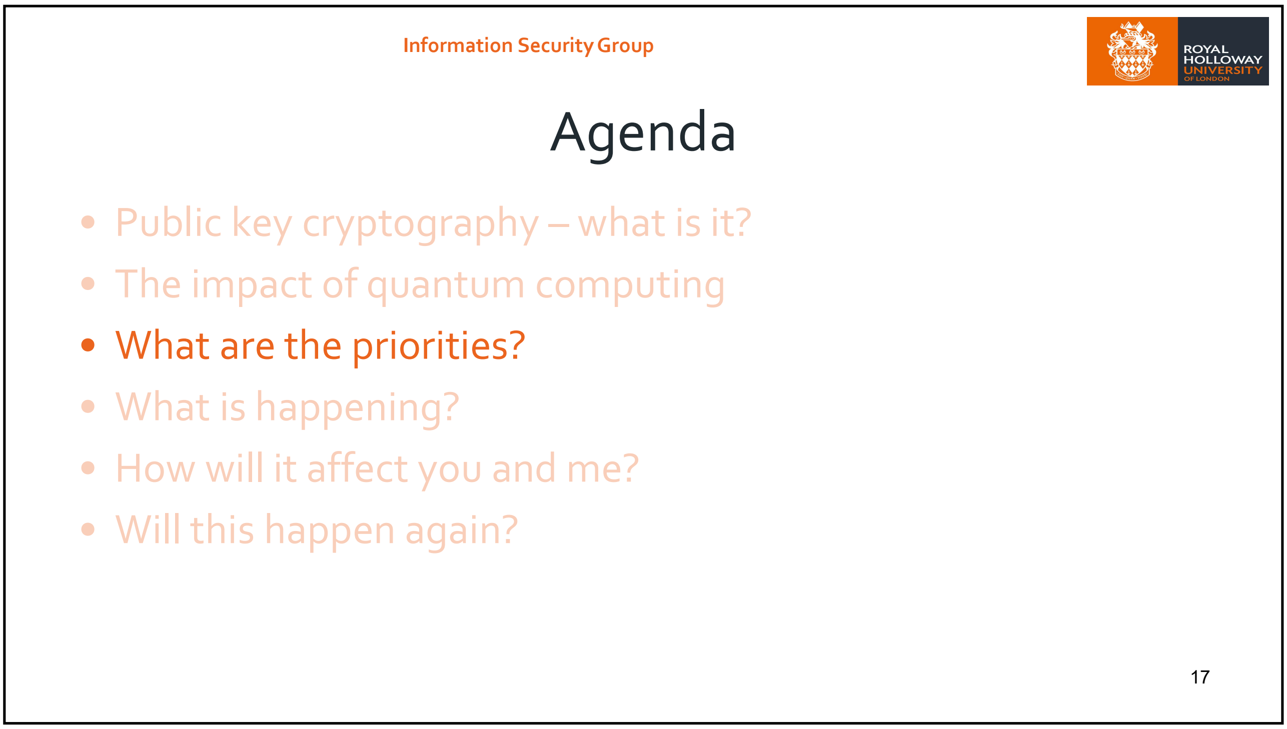
- This greatly simplifies solving two problems, the hardness of which underlies widely used public key crypto:
  - factorising large integers;
  - computing discrete logarithms in elliptic curve or finite field multiplicative groups.
- This means that **all widely used public key algorithms are compromised for feasible key lengths**.

Grover’s algorithm (1997)

- Suppose function *f* has |Domain(*f*)|=2^k.
- Reduces complexity of searching for solutions *x* to ***f*(*x*)=*y*, for known *y***, from 2^k function evaluations to $O(2^{k/2})$ function evaluations.
- A brute force key search (with known plaintext) involves solving such an equation.
- This effectively reduces key length for symmetric algorithms by half.
- Actually, not so simple since function evaluation for AES involves lots of quantum computation.

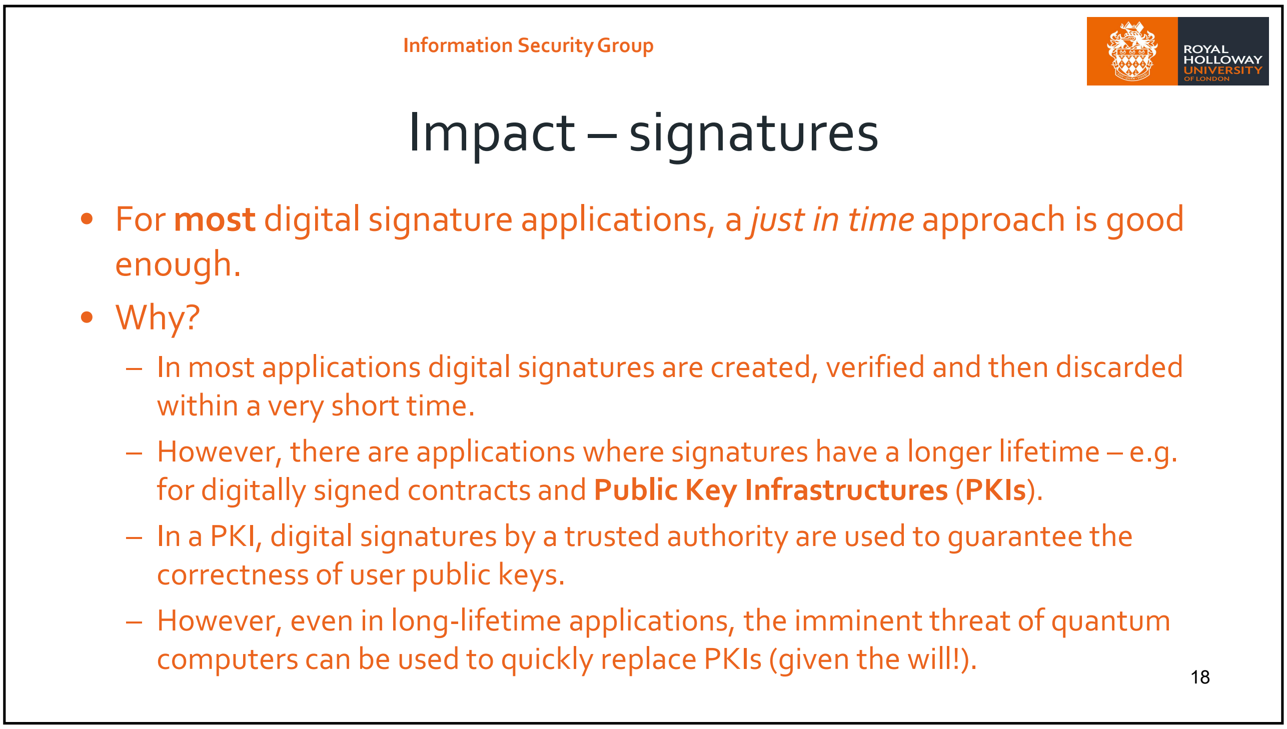
Replacing today’s crypto

- For symmetric crypto, moving from 128-bit keys to 256-bit keys is more than adequate; indeed, 128-bit key schemes look set to remain secure for the foreseeable future – so no panic here!
- **However, for public key crypto we need new algorithms.**
- This is causing a complete revolution in the way we use cryptography, given how pervasive public key crypto has become.



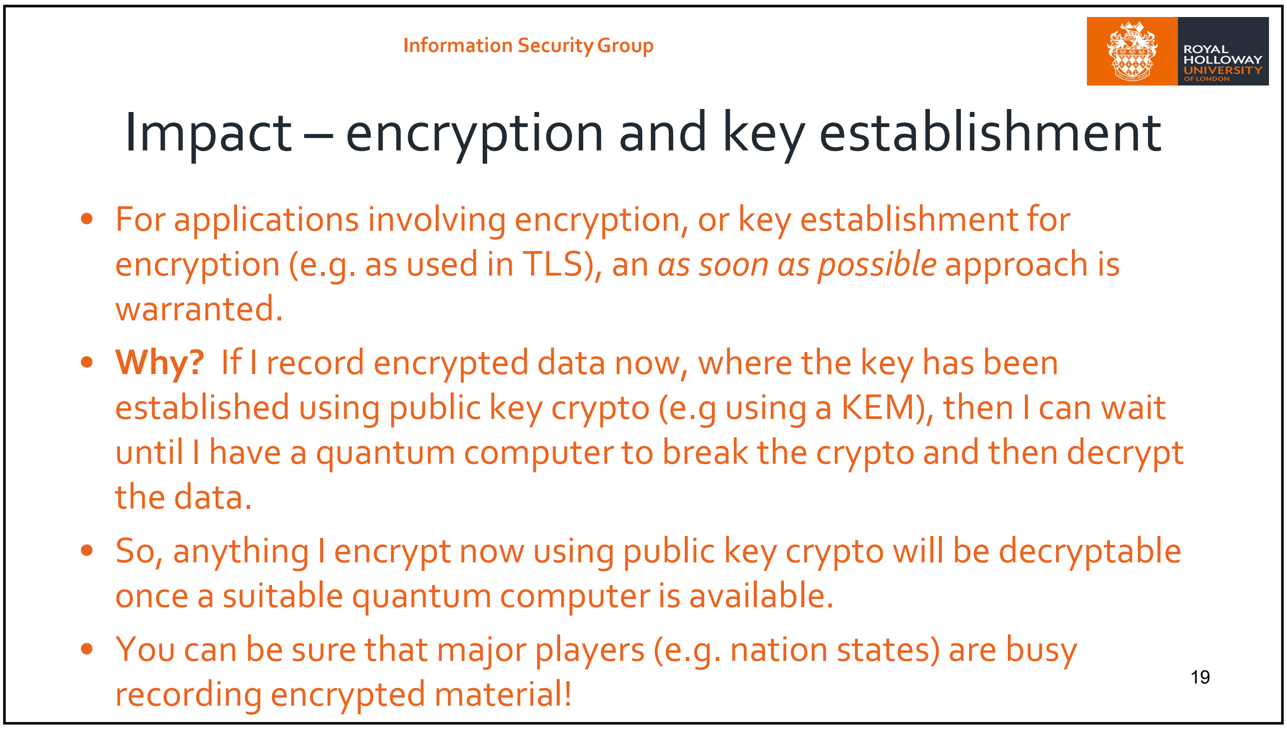
Agenda

- Public key cryptography – what is it?
- The impact of quantum computing
- What are the priorities?
- What is happening?
- How will it affect you and me?
- Will this happen again?



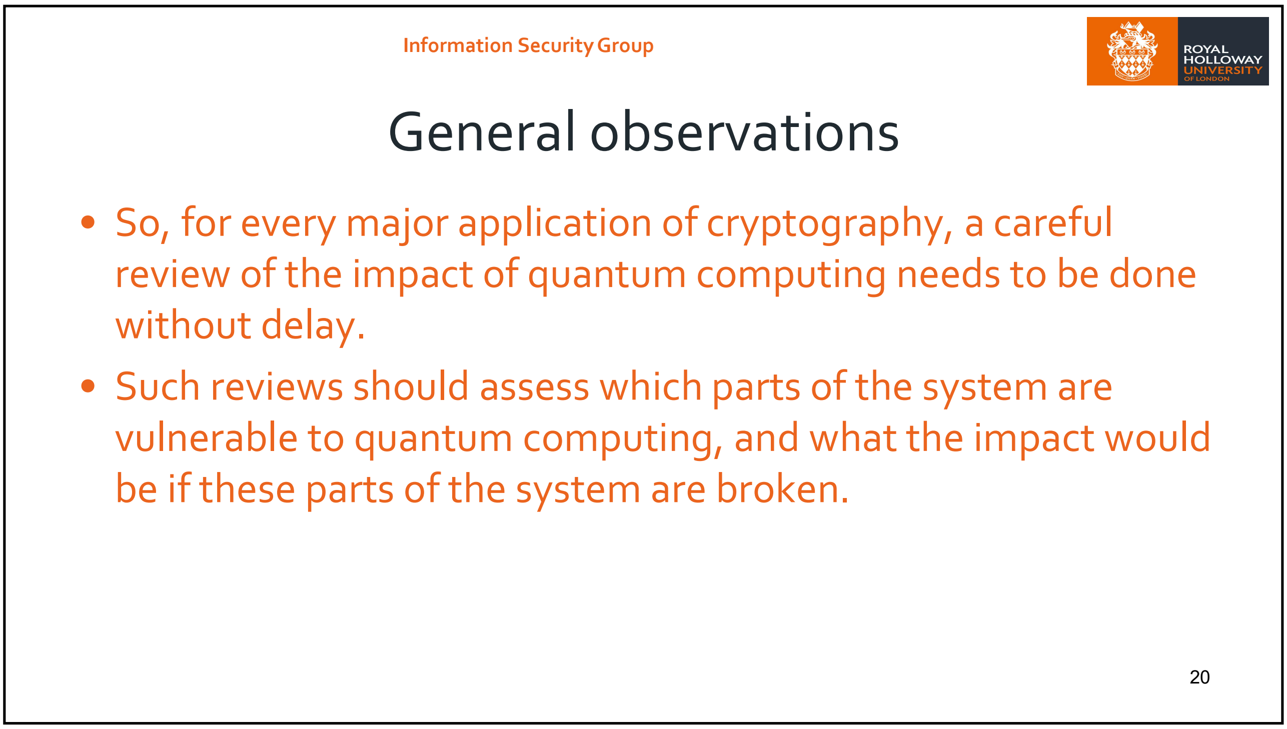
Impact – signatures

- For **most** digital signature applications, a *just in time* approach is good enough.
- Why?
  - In most applications digital signatures are created, verified and then discarded within a very short time.
  - However, there are applications where signatures have a longer lifetime – e.g. for digitally signed contracts and **Public Key Infrastructures** (**PKIs**).
  - In a PKI, digital signatures by a trusted authority are used to guarantee the correctness of user public keys.
  - However, even in long-lifetime applications, the imminent threat of quantum computers can be used to quickly replace PKIs (given the will!).



Impact – encryption and key establishment

- For applications involving encryption, or key establishment for encryption (e.g. as used in TLS), an *as soon as possible* approach is warranted.
- **Why?** If I record encrypted data now, where the key has been established using public key crypto (e.g using a KEM), then I can wait until I have a quantum computer to break the crypto and then decrypt the data.
- So, anything I encrypt now using public key crypto will be decryptable once a suitable quantum computer is available.
- You can be sure that major players (e.g. nation states) are busy recording encrypted material!



General observations

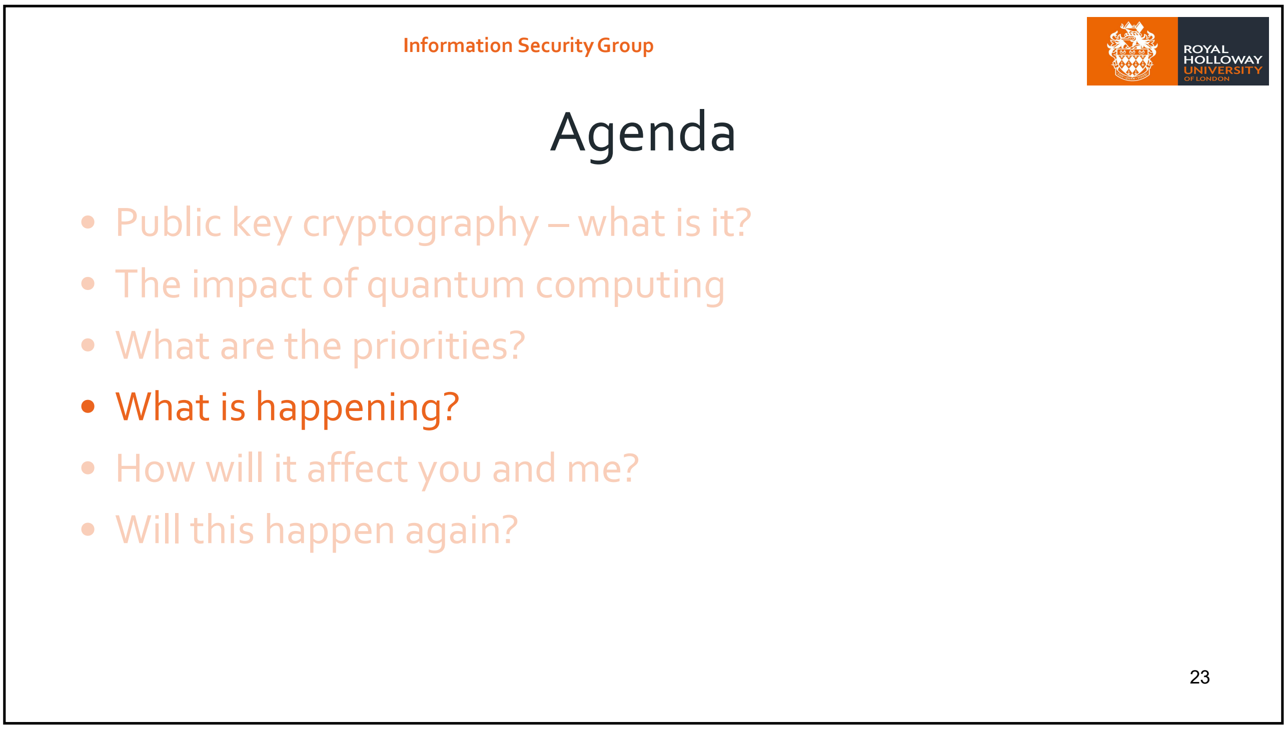
- So, for every major application of cryptography, a careful review of the impact of quantum computing needs to be done without delay.
- Such reviews should assess which parts of the system are vulnerable to quantum computing, and what the impact would be if these parts of the system are broken.

Reviews needed

- Reviews should consider how long it will take:
  - to replace crypto used in each part of the system;
  - to update the specifications;
  - to produce replacement implementations; and
  - to replace all existing deployed implementations.
- The total time could be very considerable, e.g., credit and debit cards have a typical lifetime of three-five years, so replacing all such cards could take a decade or more (and this doesn't even consider the time required to replace the supporting infrastructure).

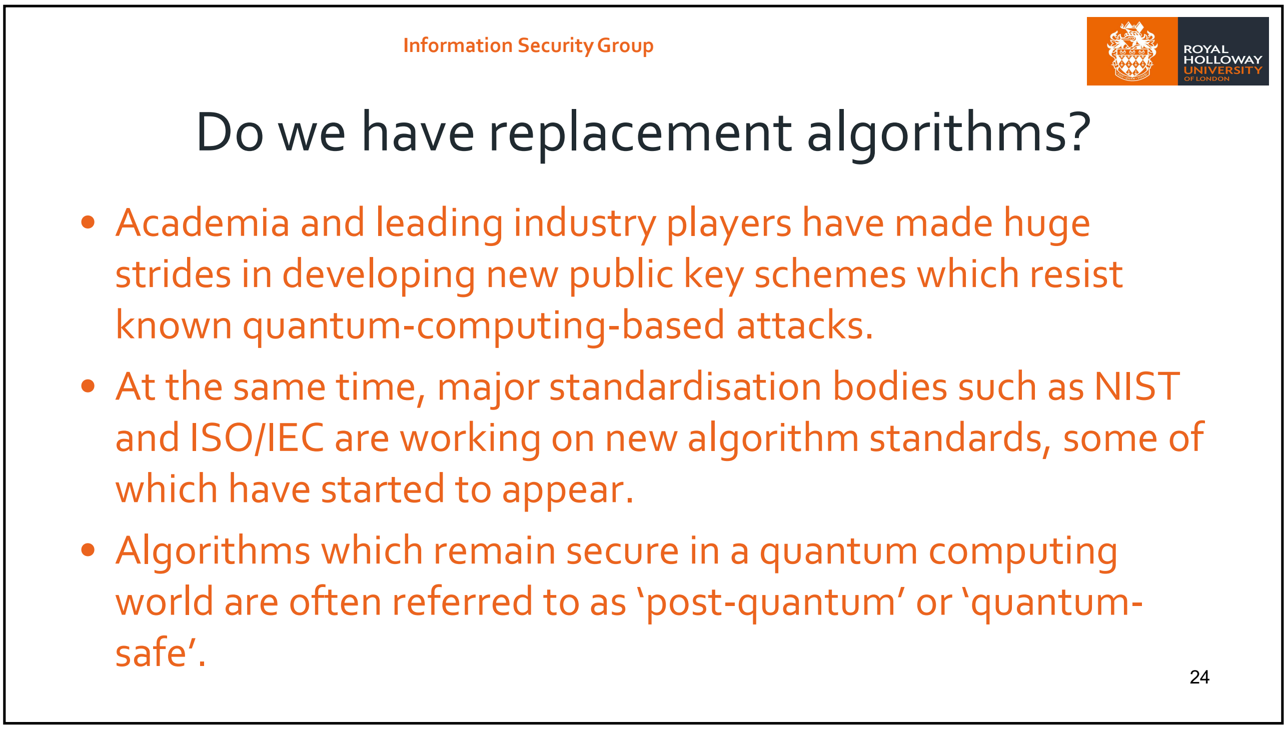
Where are we?

- It seems safe to assume that such reviews have been conducted for most high-value systems, e.g. in banking and telecommunications.
- However, I am much less confident about the situation for smaller companies, particularly in less affluent nations.
- I don’t see a major government-inspired push to start replacing vulnerable systems …



Agenda

- Public key cryptography – what is it?
- The impact of quantum computing
- What are the priorities?
- What is happening?
- How will it affect you and me?
- Will this happen again?



Do we have replacement algorithms?

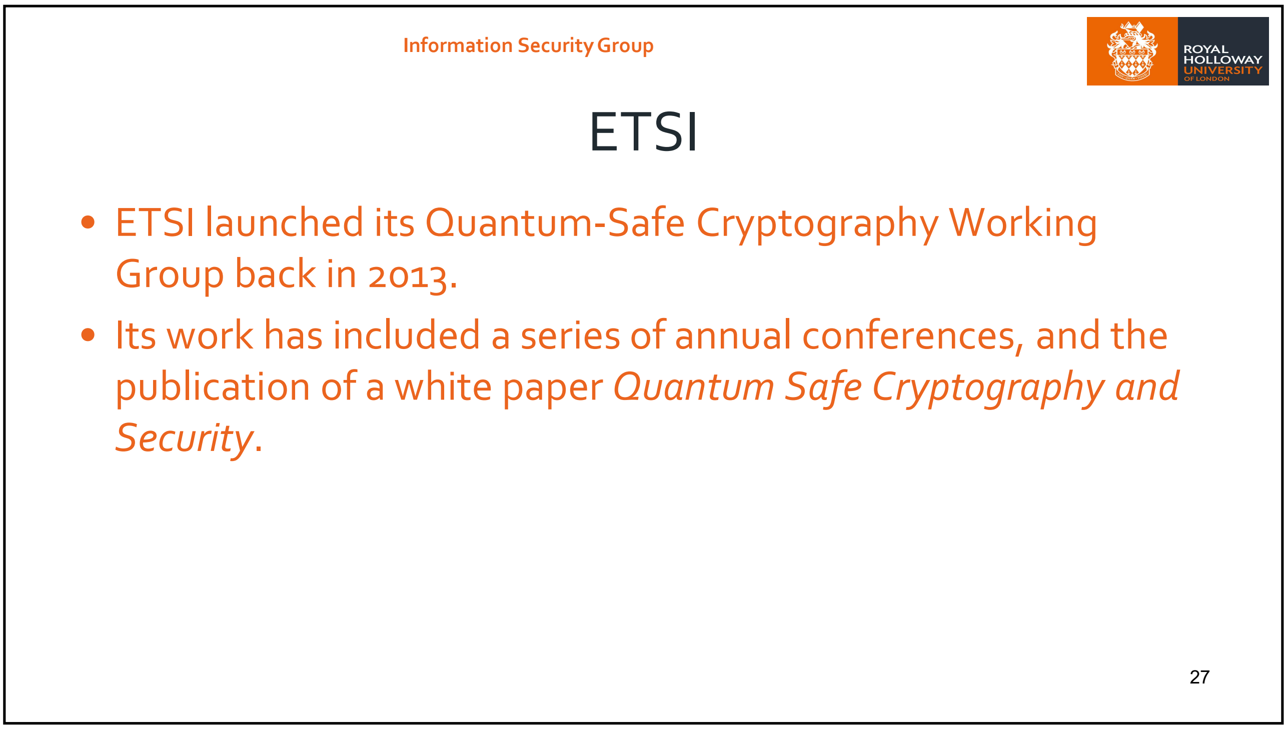
- Academia and leading industry players have made huge strides in developing new public key schemes which resist known quantum-computing-based attacks.
- At the same time, major standardisation bodies such as NIST and ISO/IEC are working on new algorithm standards, some of which have started to appear.
- Algorithms which remain secure in a quantum computing world are often referred to as 'post-quantum' or 'quantum-safe'.

The NIST competition

- The NIST *Post-Quantum Cryptography Standardization* competition was announced in 2016.
- Following a series of conferences and a huge number of inputs, three draft standards have recently been published:
  - Draft FIPS 203 contains three variants of **ML-KEM**, a KEM based on a scheme known as CRYSTALS-KYBER;
  - Draft FIPS 204 contains **ML-DSA**, a signature algorithm based on a scheme known as CRYSTALS-DILITHIUM;
  - Draft FIPS 205 contains **SLH-DSA**, another signature algorithm – this time based on a scheme known as SPHINCS+.

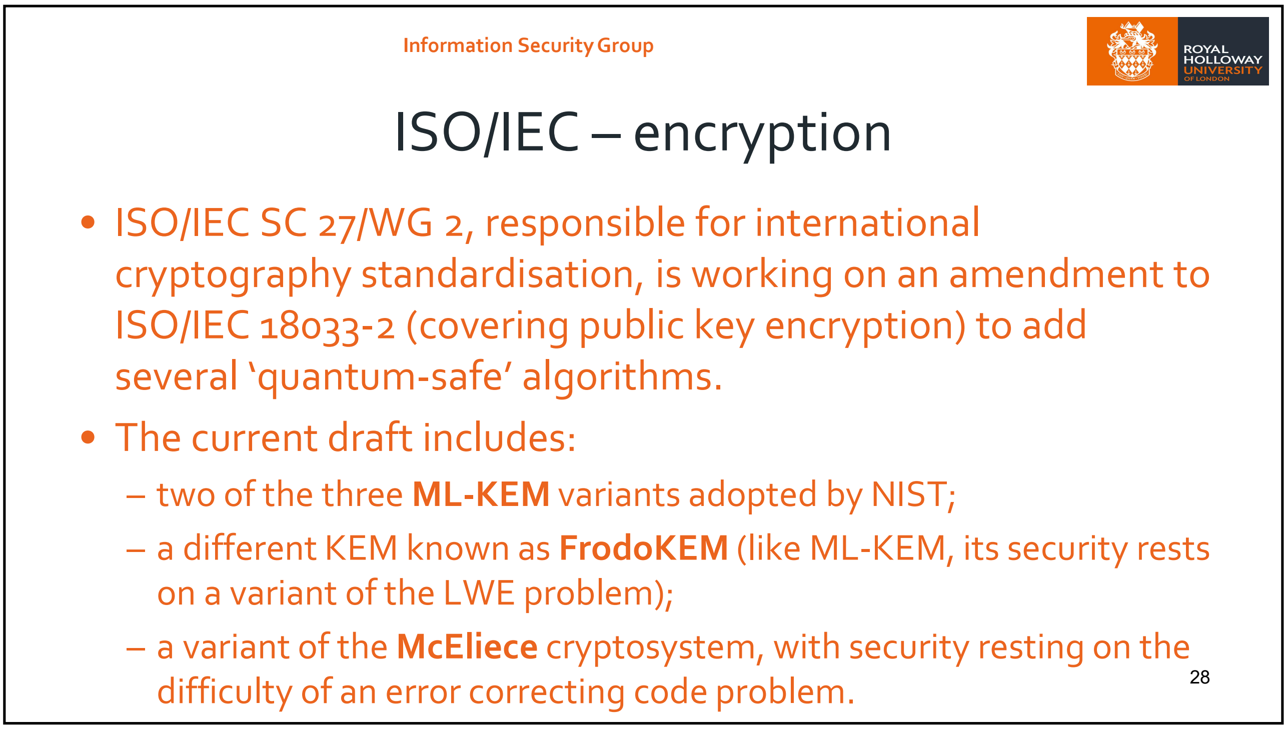
NIST candidates – security

- The hard computational problem on which the security of ML-KEM and ML-DSA is based is the **Module Learning With Errors (LWE)** problem.
  - LWE aims to hide a secret by introducing noise;
  - the problem involves deducing a linear *n*-ary function from given evaluations of the function, some of which may be erroneous;
  - LWE believed to be computationally hard even for a quantum computer.
- SLH-DSA is very different: based on a cryptographic hash-function – its security rests on the security of the chosen hash-function.



ETSI

- ETSI launched its Quantum-Safe Cryptography Working Group back in 2013.
- Its work has included a series of annual conferences, and the publication of a white paper *Quantum Safe Cryptography and Security*.



ISO/IEC – encryption

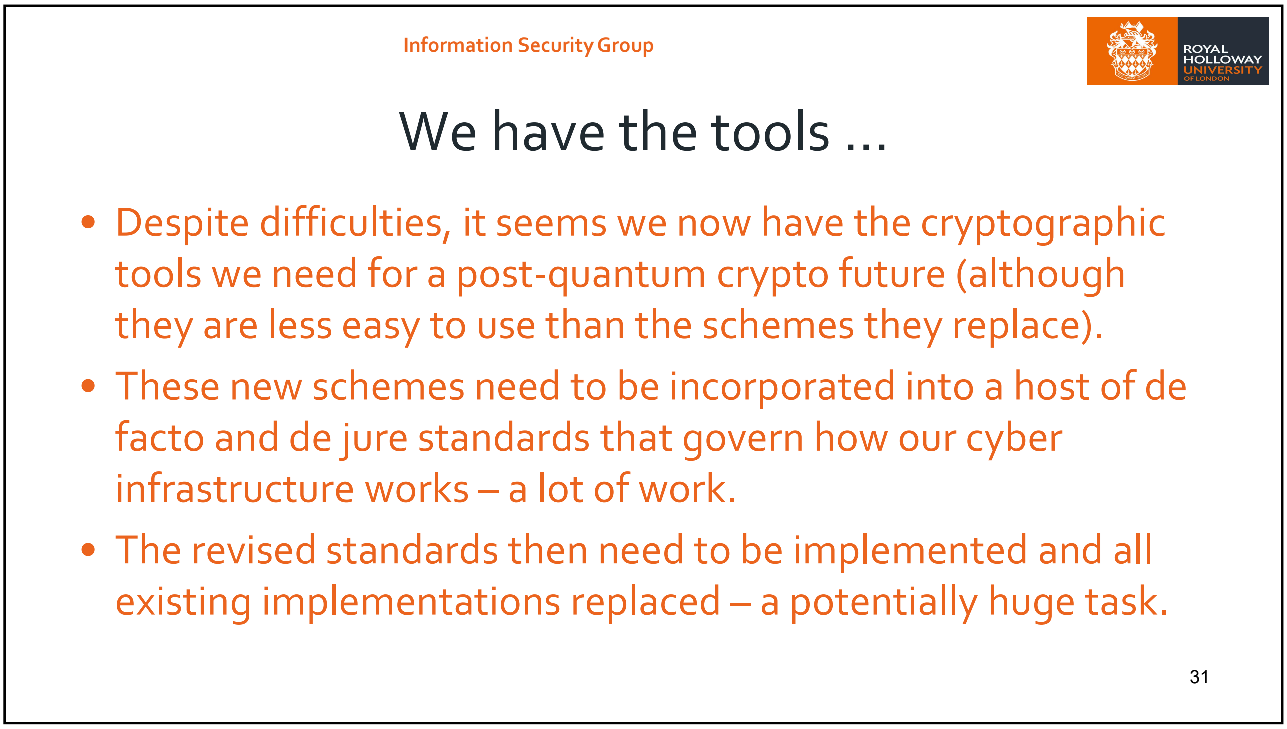
- ISO/IEC SC 27/WG 2, responsible for international cryptography standardisation, is working on an amendment to ISO/IEC 18033-2 (covering public key encryption) to add several 'quantum-safe' algorithms.
- The current draft includes:
  - two of the three **ML-KEM** variants adopted by NIST;
  - a different KEM known as **FrodoKEM** (like ML-KEM, its security rests on a variant of the LWE problem);
  - a variant of the **McEliece** cryptosystem, with security resting on the difficulty of an error correcting code problem.

ISO/IEC controversies

- Including any of the ML-KEM variants in ISO/IEC 18033-2 caused much discussion, given they are **slightly tweaked versions** of CRYSTALS-KYBER.
- This is at least partly because of a suspicion that NIST might have included some kind of backdoor weakness.
- The other two ISO/IEC adopted algorithms are less efficient:
  - FrodoKEM is more conservative in its design choices;
  - McEliece is a long-standing algorithm – over 50 years – and is believed secure although it uses very large keys.

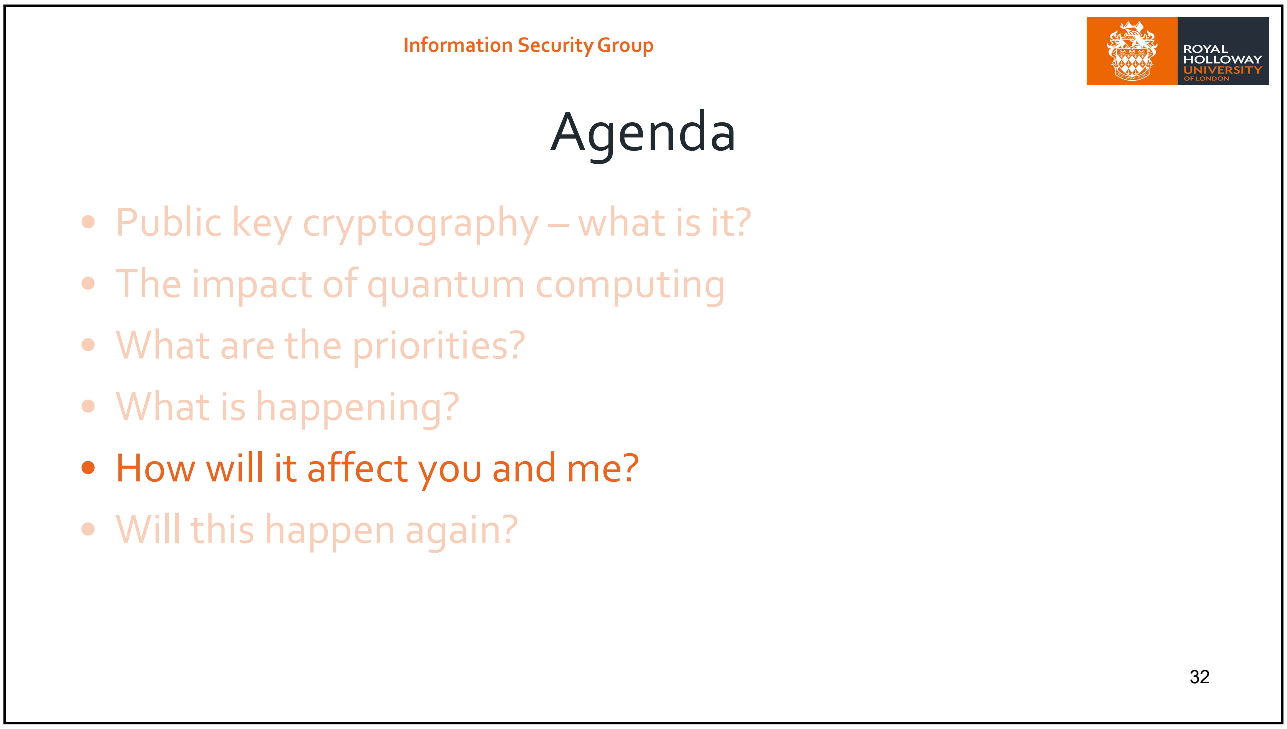
ISO/IEC – digital signatures

- ISO/IEC 14888-4 – now nearing publication – contains several hash-function-based post-quantum signature schemes, although they are distinct from SDLH-DSA.
- It is likely that ISO/IEC will also eventually adopt the NIST–specified signature schemes, although standardising signatures is less urgent.



We have the tools …

- Despite difficulties, it seems we now have the cryptographic tools we need for a post-quantum crypto future (although they are less easy to use than the schemes they replace).
- These new schemes need to be incorporated into a host of de facto and de jure standards that govern how our cyber infrastructure works – a lot of work.
- The revised standards then need to be implemented and all existing implementations replaced – a potentially huge task.



Agenda

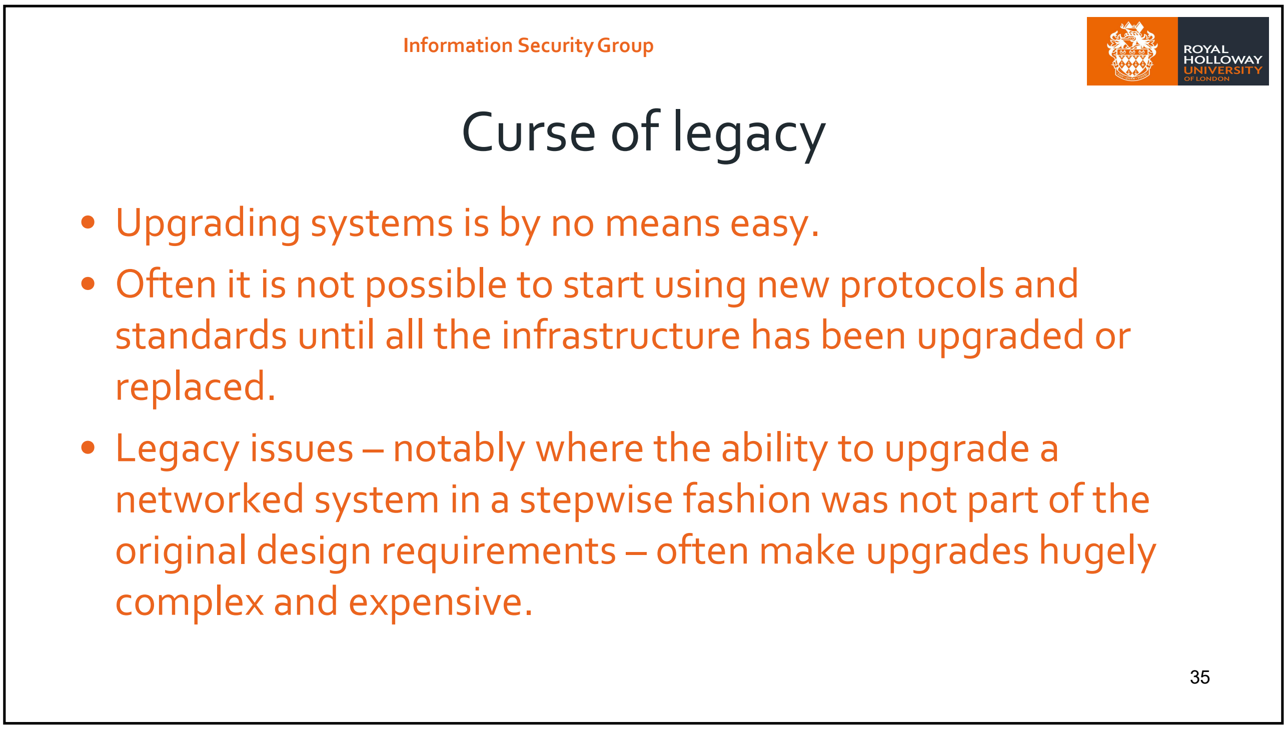
- Public key cryptography – what is it?
- The impact of quantum computing
- What are the priorities?
- What is happening?
- How will it affect you and me?
- Will this happen again?

Are we ready for the quantum apocalypse?

- Of course not.
- For example, there are no 'quantum-secure' TLS ciphersuites available by default in Windows 10.
- But there is hope that we will *mostly* be ready in time.
- The crypto standards we need will be in place within the next couple of years, and we can then expect to see the algorithms being rolled out across the global IT infrastructure.

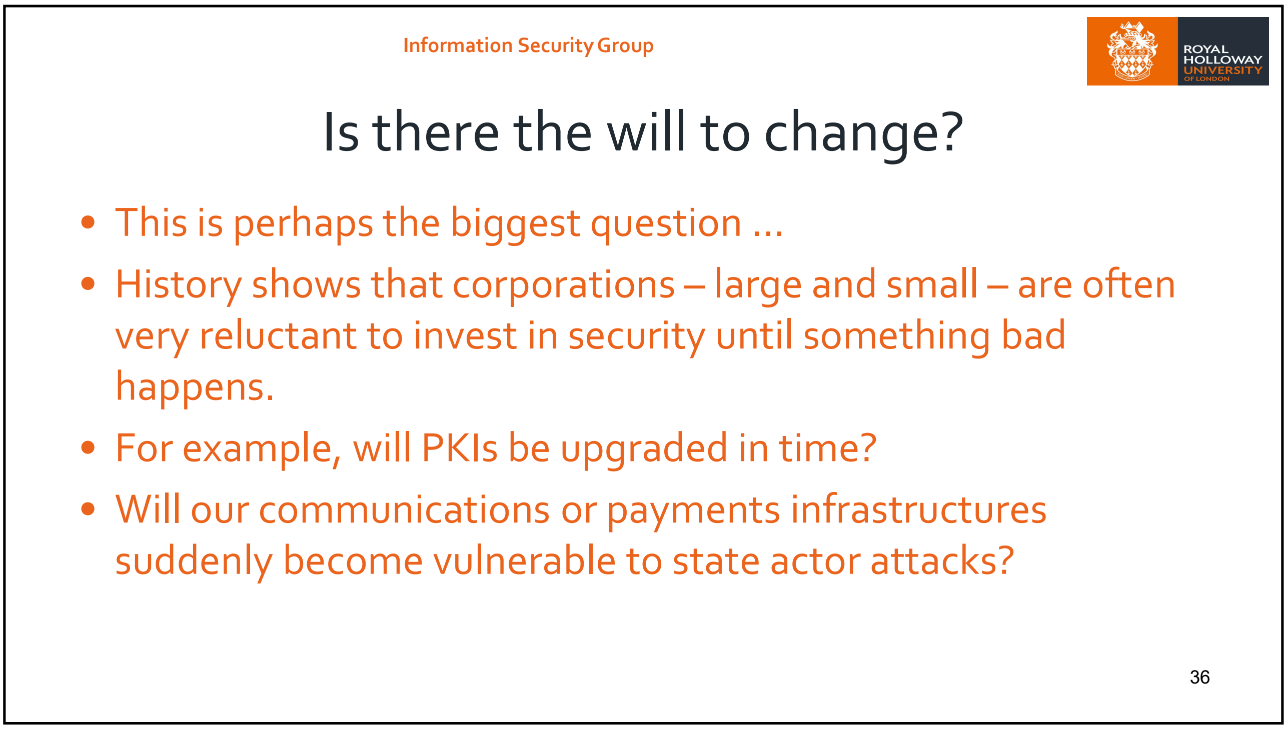
How much notice will we have?

- It is impossible to know how long we have until sufficiently capable quantum computers are available.
- My guess would be at least five years, but who knows?
- The threat of hostile nation state actors and organised crime is clear.
- National states will have early access to powerful quantum computers – you can be sure there is a lot of government research going on behind the scenes.
- An early advantage could be critical.



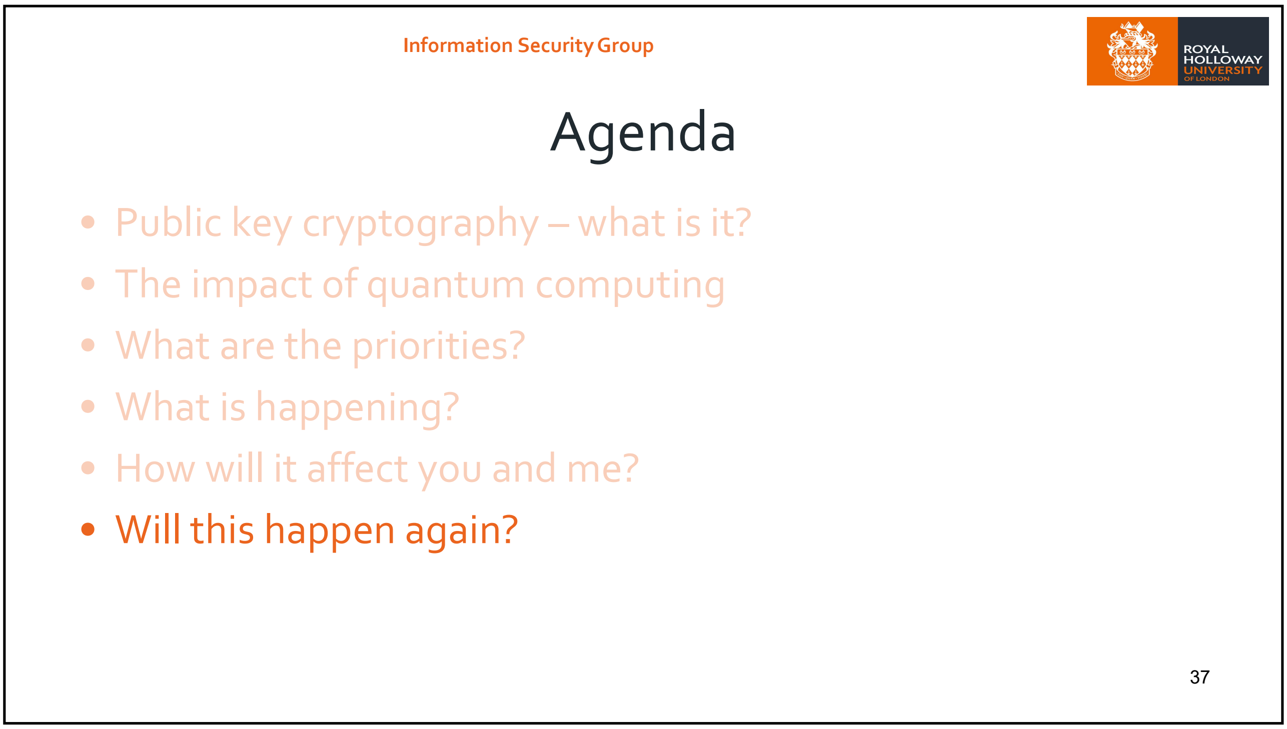
Curse of legacy

- Upgrading systems is by no means easy.
- Often it is not possible to start using new protocols and standards until all the infrastructure has been upgraded or replaced.
- Legacy issues – notably where the ability to upgrade a networked system in a stepwise fashion was not part of the original design requirements – often make upgrades hugely complex and expensive.



Is there the will to change?

- This is perhaps the biggest question …
- History shows that corporations – large and small – are often very reluctant to invest in security until something bad happens.
- For example, will PKIs be upgraded in time?
- Will our communications or payments infrastructures suddenly become vulnerable to state actor attacks?



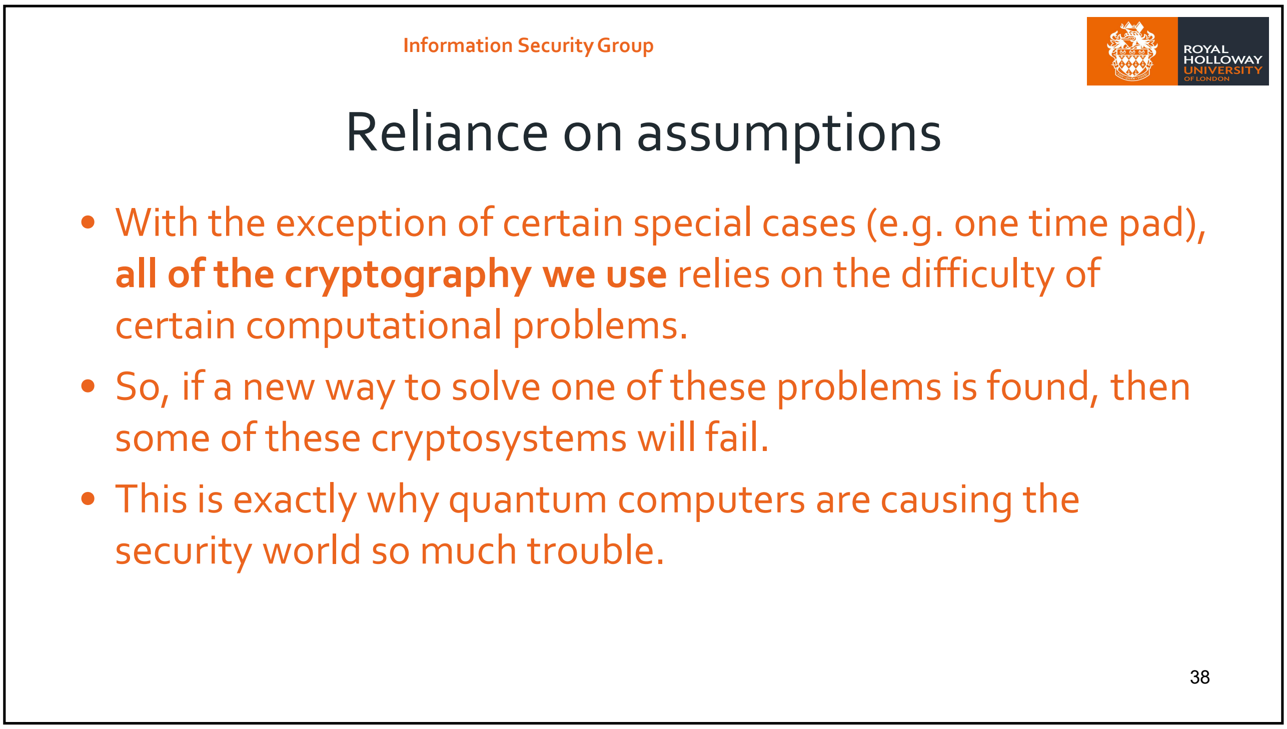
Information Security Group

Agenda

- Public key cryptography – what is it?
- The impact of quantum computing
- What are the priorities?
- What is happening?
- How will it affect you and me?
- Will this happen again?

37

37



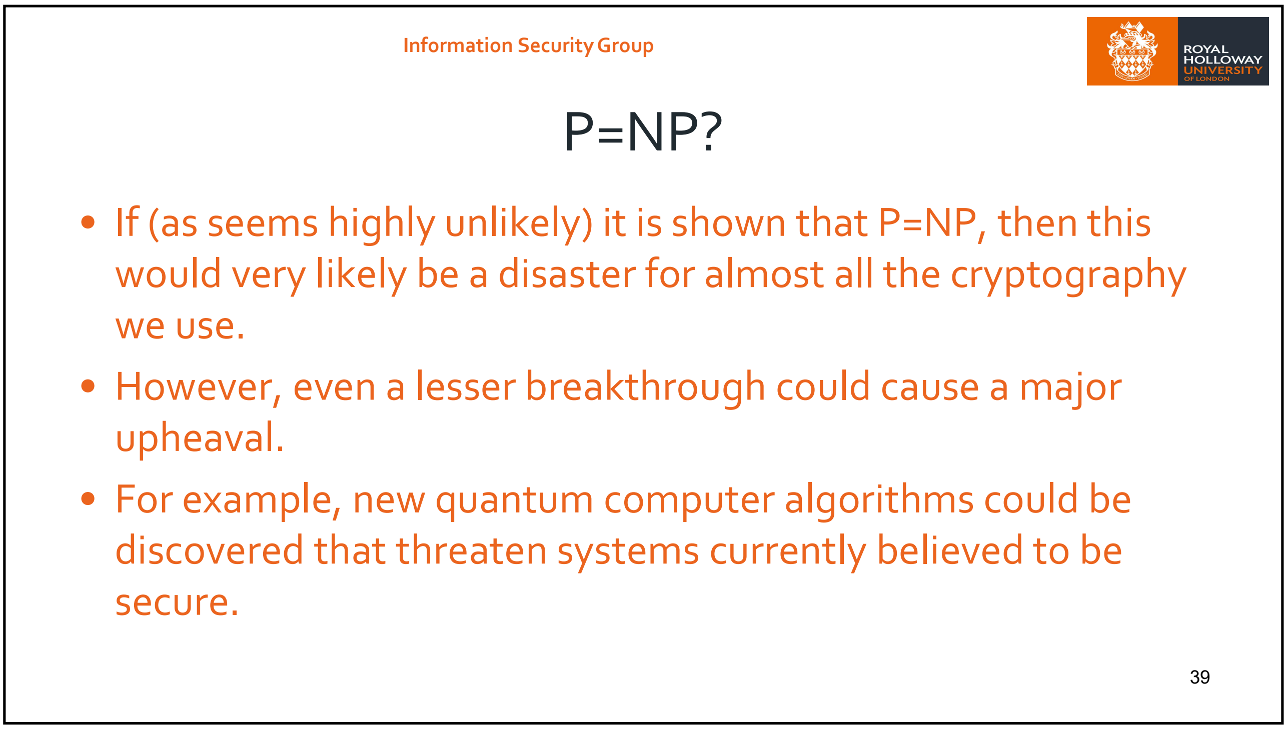
Information Security Group

Reliance on assumptions

- With the exception of certain special cases (e.g. one time pad), **all of the cryptography we use** relies on the difficulty of certain computational problems.
- So, if a new way to solve one of these problems is found, then some of these cryptosystems will fail.
- This is exactly why quantum computers are causing the security world so much trouble.

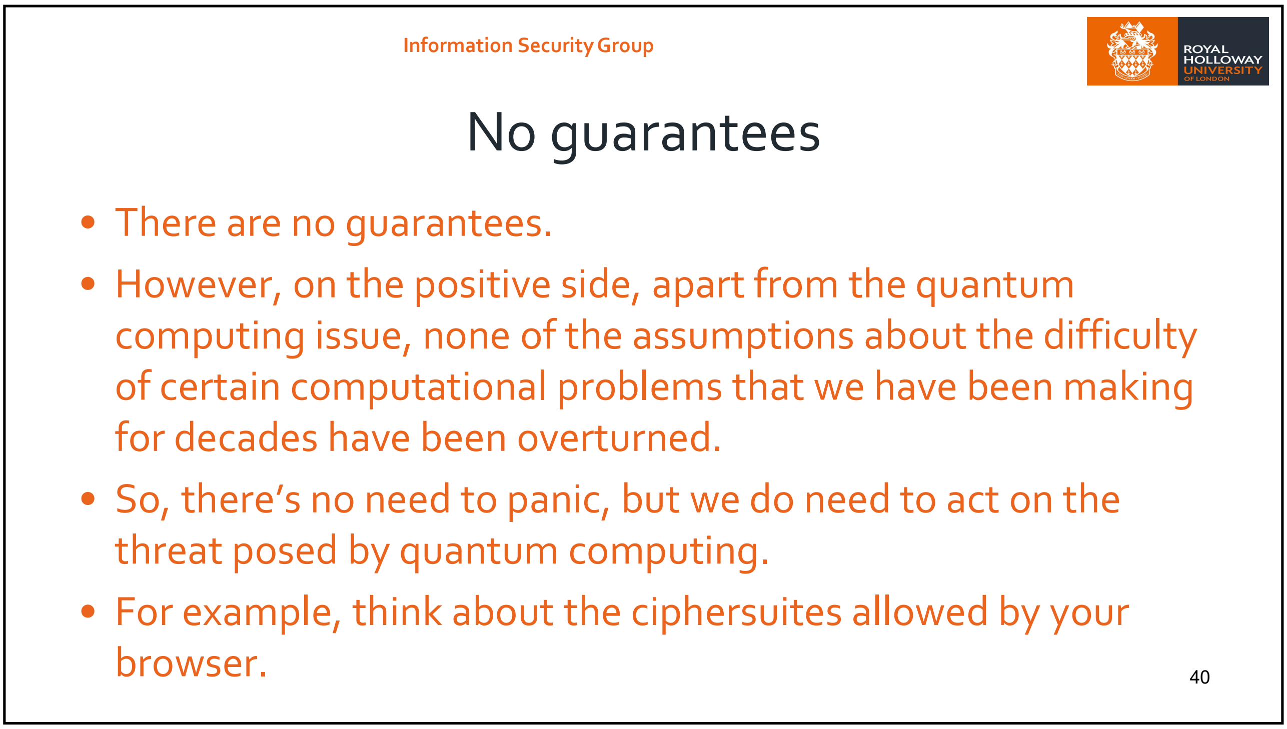
38

38



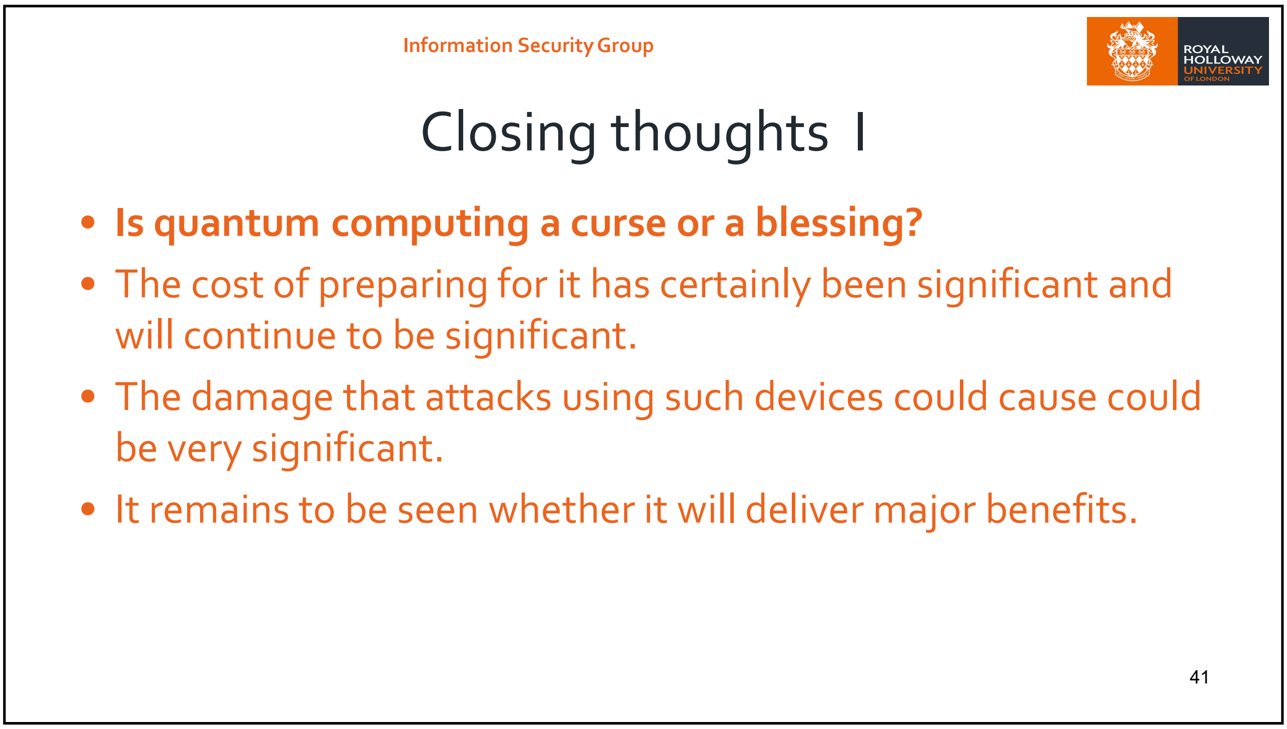
P=NP?

- If (as seems highly unlikely) it is shown that P=NP, then this would very likely be a disaster for almost all the cryptography we use.
- However, even a lesser breakthrough could cause a major upheaval.
- For example, new quantum computer algorithms could be discovered that threaten systems currently believed to be secure.



No guarantees

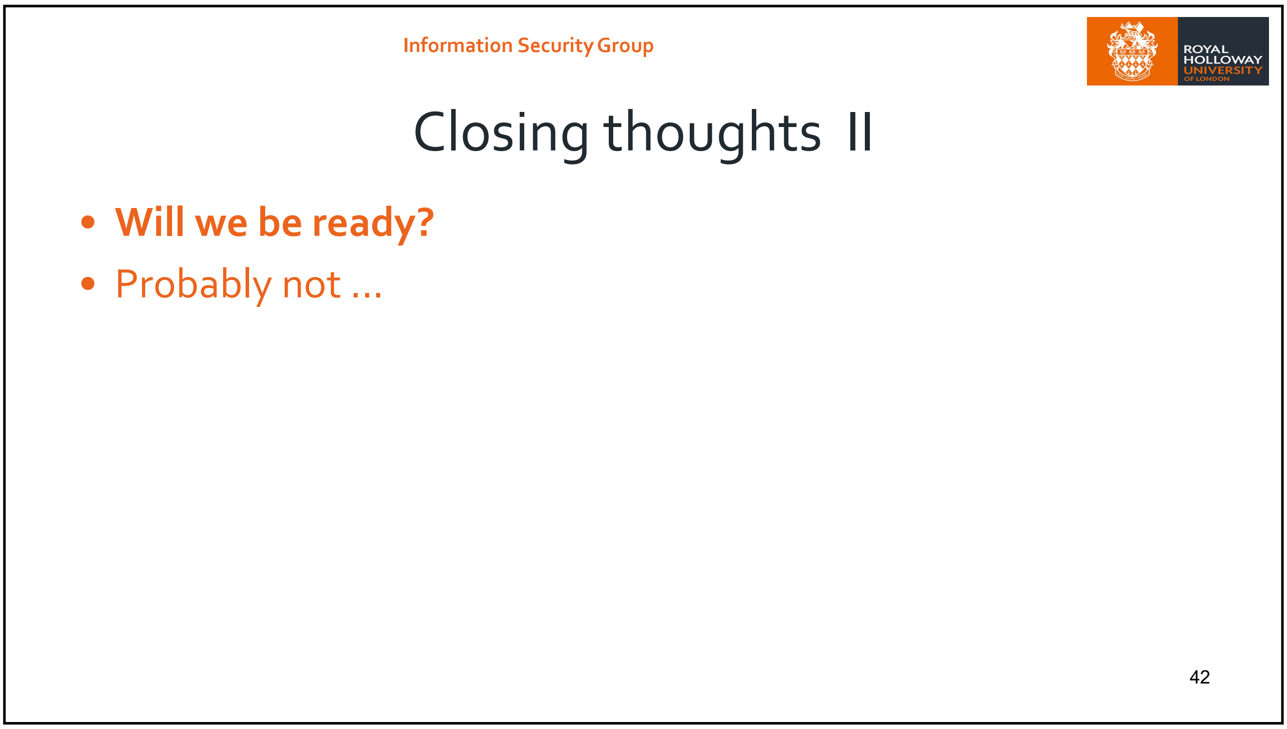
- There are no guarantees.
- However, on the positive side, apart from the quantum computing issue, none of the assumptions about the difficulty of certain computational problems that we have been making for decades have been overturned.
- So, there’s no need to panic, but we do need to act on the threat posed by quantum computing.
- For example, think about the ciphersuites allowed by your browser.



Information Security Group

Closing thoughts I

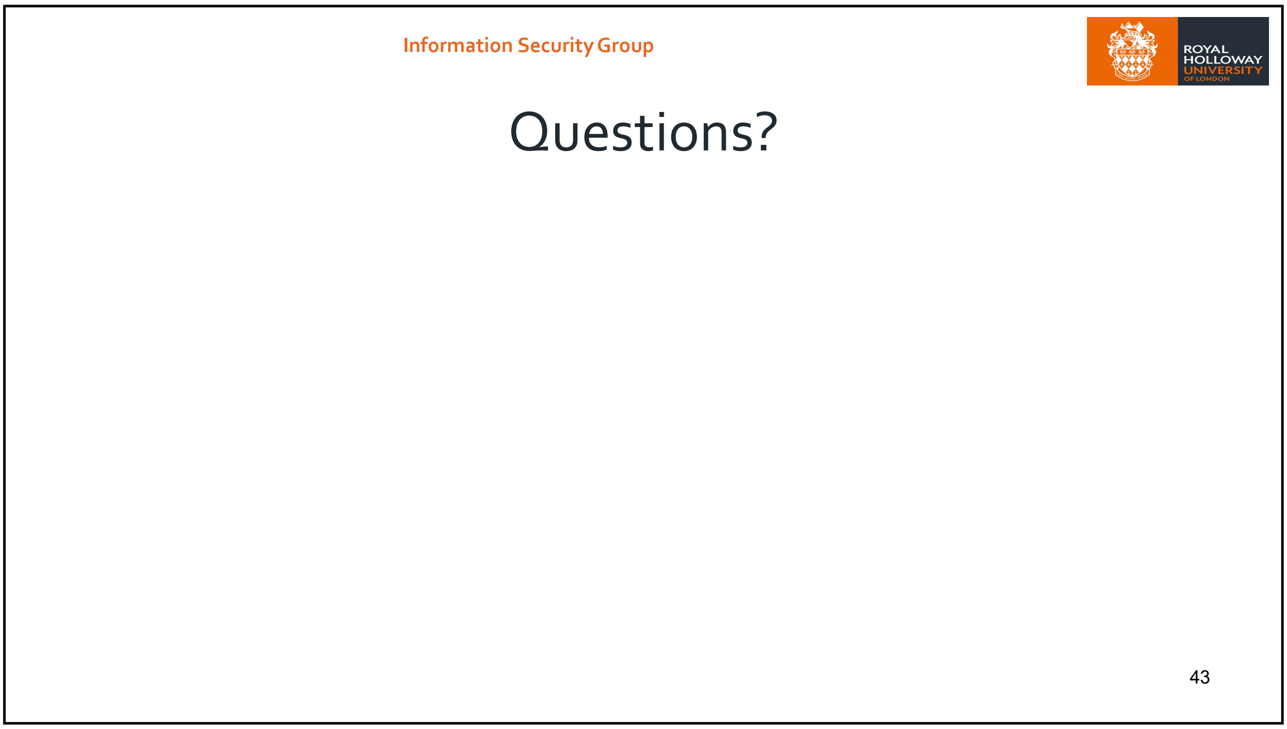
- **Is quantum computing a curse or a blessing?**
- The cost of preparing for it has certainly been significant and will continue to be significant.
- The damage that attacks using such devices could cause could be very significant.
- It remains to be seen whether it will deliver major benefits.



Information Security Group

Closing thoughts II

- **Will we be ready?**
- Probably not …



Questions?