Quantum computing – What will be the real impact on 5G security?

Chris Mitchell
me@chrismitchell.net
www.chrismitchell.net

1

1

Information Security Group

Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

2

2

Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

Quantum computers

- In recent years there has been much discussion of the impact of quantum computing on cryptography.
- There is no general 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.
- Should such computers ever become available, they will have a major impact on the security of today's cryptography.

Mobile security

- Security of mobile telecommunications has relied on cryptography since GSM, designed in the 1980s and first deployed in 1991.
- GSM is often referred to as **2G** for the **2nd generation** of mobile telecommunications.
- 5G is the latest generation, standardised by 3GPP, and 5G systems are now being deployed globally.
- Mobile comms are very widely used worldwide, and 5G looks set to become even more significant.
- So the security of 5G is hugely important.

Quantum and 5G

- These observations have motivated this talk, which examines the impact of quantum computing on 5G security.
- As I will describe, key parts of the system as currently specified are vulnerable should a quantum computer become available.
- This detailed analysis had led to the proposal of a phased upgrade to 5G security, with a smooth and simple migration path.

Information Security Group

General observations

- This review of priorities in 5G security evolution is just one amongst many needed.
- 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.

7

7

Information Security Group

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).

8

8

Information Security Group

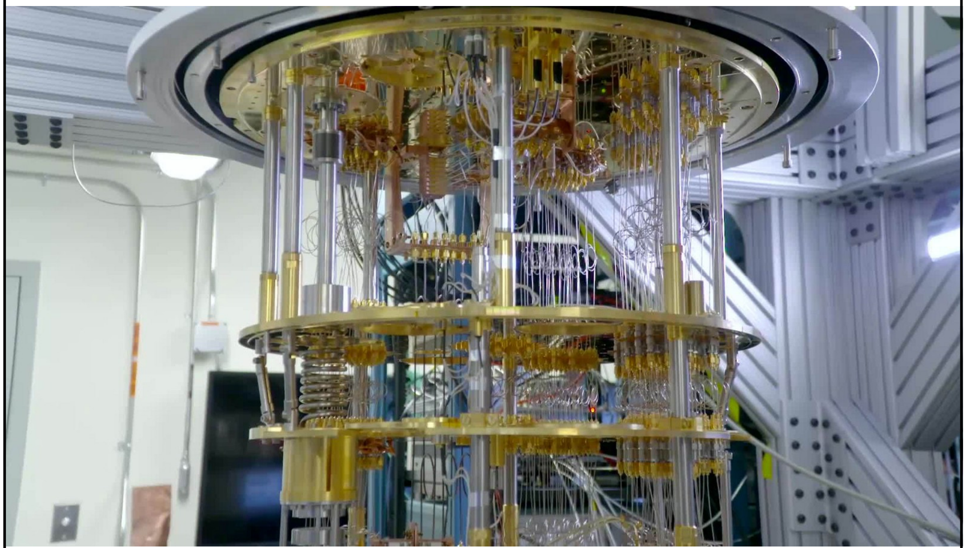
Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

9

9

Information Security Group



10

10

Potential impact

- If and when they arrive, we cannot be sure of the 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 crypto perspective, there are two key algorithms that have been devised to run on quantum computers.

11

Shor's algorithm (1994)

- Greatly simplifies solving two problems, the hardness of which underlies all currently used asymmetric crypto:
  - factorising large integers;
  - computing discrete logarithms in elliptic curve or finite field multiplicative groups.
- Means that all currently used asymmetric algorithms are compromised for feasible key lengths.

12

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.

Impacts

- For message authentication and digital signature applications a *just in time* approach is good enough.
- For applications involving encryption, or key establishment for encryption (e.g. TLS), an *as soon as possible* approach is warranted.

Replacing today's crypto

- For symmetric crypto, moving from 128-bit keys to 256-bit keys is more than adequate.
- For asymmetric crypto need new algorithms.
- Fortunately, NIST, ETSI, ISO/IEC and other standards bodies are working on it …
- The NIST *Post-Quantum Cryptography Standardization* competition is moving ahead – Round 2 candidates announced in January 2019.

Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

Information Security Group

Principal actors

- The main players in 5G security are:
  - User Equipment (**UE**), made up of a Mobile Equipment (**ME**) and a **USIM** (chip card);
  - USIM issued by the **home network/issuing network**, which has an Authentication credential Repository and Processing Function (**ARPF**);
  - USIM and ARPF share a **128-bit secret key *K***;
  - UE gets service from a **visited network**, which has a Security Anchor Function (**SEAF**).

17

17

Information Security Group

Main security objectives

- 5G security is an evolution of 4G security, itself an evolution of 2G and 3G security.
- Like its predecessors, 5G security has three main aims, in decreasing order of importance:
  - *fraud prevention* (through USIM-network authentication);
  - *voice, data and signalling protection* between UE and visited network (using encryption and MACs);
  - *user identity privacy* against radio path eavesdroppers (through temporary identifiers).

18

18

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

5G new features

- Three major differences between 4G and 5G:
  - *flexibility in authentication method* – USIM can authenticate to the serving network using either 5G AKA or the Internet EAP-AKA';
  - *robust mobile identity confidentiality* – using asymmetric encryption to supplement temporary IDs;
  - *data integrity protection* – all transmitted voice and data is integrity protected, not just signalling messages as in 4G.

19

19

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Security architecture

- Can divide the functioning of 5G crypto-based security into four main parts:
  - Authentication and Key Agreement (AKA);
  - Key derivation;
  - Session security;
  - Mobile identity confidentiality.
- Next summarise each of these (we only cover 5G AKA and not EAP-AKA').

20

20

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Authentication and Key Agreement (AKA)

- 5G AKA is an evolution of AKA in 2G, 3G and 4G – it is the foundation of 5G security.
- The home network ARPF generates **Authentication Vectors** (**AVs**) for its USIMs which are sent to the appropriate visited networks and used in 5G AKA protocol.
- AVs are computed using long-term key *K*.
- Avoids the need for the key *K* to ever leave the home network's ARPF or the USIM.

21

21

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Authentication Vectors I

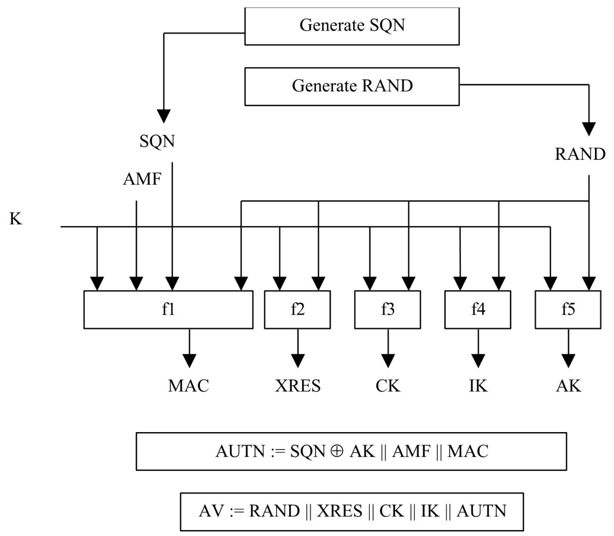
5G AVs are computed in three stages.

1. Generate a 3G AV: **(RAND, XRES, CK, IK, AUTN)**
   – RAND is authentication challenge (network to USIM);
   – XRES is expected response (for authentication of USIM);
   – CK and IK are keys;
   – AUTN (authentication token) contains:
      - a 64-bit encrypted sequence number SQN (= SQN⊕AK);
      - a 48-bit MAC (for authentication of network to USIM).
   – All 128-bit values.
   – Computed using functions *f*1 – *f*5 (home-network-specific, although set of functions provided in 3GPP specifctions).

22

22

Authentication Vectors II



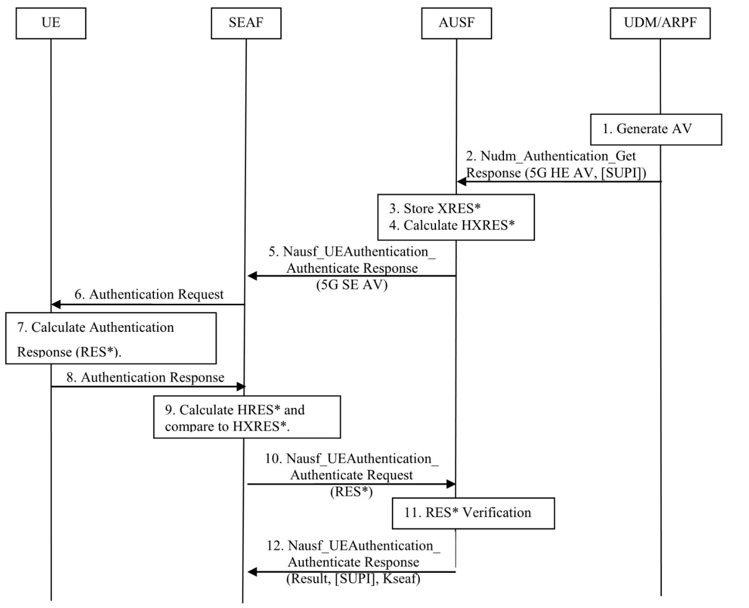
Authentication Vectors III

2. Derive a 5G HE AV **(RAND, AUTN, XRES*, K_{AUSF})** from the 3G AV:
   - XRES* = *f*(XRES, RAND, CK, IK, servingnetworkID);
   - K_{AUSF} = *f*(CK, IK, AUTN, servingnetworkID).
3. Compute a 5G AV **(RAND, AUTN, HXRES*, K_{SEAF})** from the 5G HE AV:
   - HXRES* = *f*(XRES*, RAND);
   - K_{SEAF} = *f*(K_{AUSF}, servingnetworkID).

- Step 2 is computed by the home network **outside the ARPF**.
- Step 3 is computed by the **serving network**, not the home network.

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON



25

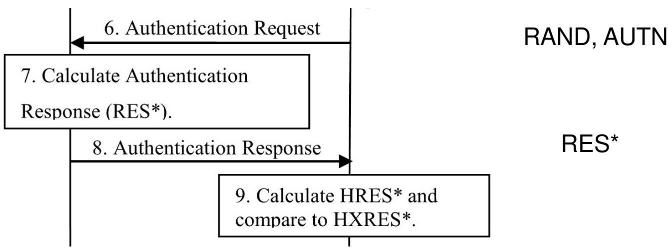
25

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

AKA protocol I

- In the diagram:
  - steps 1-5: computation and transfer of the 5G AV, and
  - steps 6-12: use of the AV in the AKA protocol.



26

26

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

AKA protocol II

- The RAND and AUTN are passed to the **USIM** by the ME.
- The **USIM** essentially does the same job as done by the ARPF to compute the 3G AV.
- The SQN is decrypted and checked and the MAC is checked.
- If the checks work out, the **USIM** sends the ME the 3G-style RES, CK and IK.
- This is converted to the 5G RES* by the **ME** which is sent to the serving network. The **ME** also computes K_{SEAF}.
- The **serving network** converts RES* to HRES*, which is compared to the HXRES* value in the 5G AV.

27

27

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

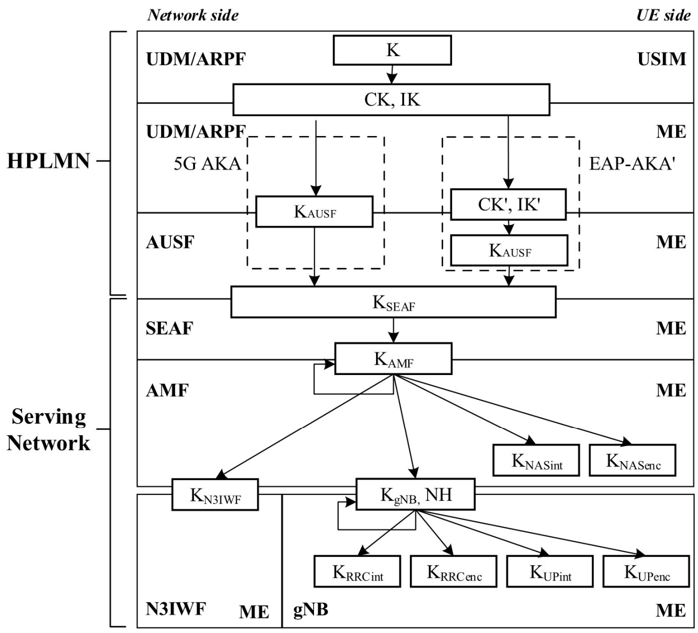
Key derivation

- A wide range of 128-bit operational keys are derived from the **anchor key** K_{SEAF}.
- These are all derived in pairs – one for encryption and one for MACing.
- Different keys are derived for (a) data/voice transfer, and (b) various types of signalling.
- These key derivations take place in the ME and the serving network.
- Key derivations use standardised functions.

28

28

Information Security Group



29

29

Information Security Group

Session security

- Data, voice and signalling sent between the UE and the visiting network are all encrypted and MAC-protected using 128-bit keys derived from K_{SEAF}.
- Unlike the USIM/ARPF functions *f*1 – *f*5, these algorithms are standardised (there are multiple options).
- [*Essentially, everything that goes on outside the USIM needs to be standardised.*]

30

30

Backward compatibility

- It is important to note that:
  - the home network ARPF only outputs 3G AVs;
  - the USIM is only required to do 3G-style computations;
  - the 3G-style values of RES, CK and IK output by the USIM are used by the ME to derive 5G keys and the 5G authentication response.
- So a 3G USIM will work in a 4G or 5G handset.

Mobile identity encryption I

- As in previous generation networks, the primary method for identity confidentiality is the use of temporary identifiers (GUTIs).
- New GUTIs sent to the UE via an encrypted channel.
- However, *occasionally* the permanent identifier (SUPI) must be sent across the network.
- If so, it is asymmetrically encrypted using a randomised scheme of the home network's choice (although ECIES is provided as a possible scheme).
- The encrypted SUPI is sent to the home network which decrypts it and returns a cleartext value.

Mobile identity encryption II

- The encryption of the SUPI can be done either in the USIM or in the ME, at the choice of the USIM.
- Obviously, in the latter case then the standardised scheme must be employed and the USIM must provide the public key to be used.

Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

Keys and key derivation

- Foundation of all security (apart from mobile identity confidentiality) is a 128-bit key *K*.
- That is, all operational keys, as well as the authentication response RES* sent over the radio path, are a function of *K* and public data.
- Here 'public data' includes the RAND value, which is sent across the radio path in cleartext.

Proprietary functions

- Functions *f*1 – *f*5 are network-proprietary (possibly secret).
- This offers little additional security for two reasons:
  - candidate functions are standardised, and so at least some networks will use these public functions;
  - the functions must be built into every USIM, and hence could be obtained via reverse-engineering.

AKA

- Suppose a malicious party with a quantum computer has intercepted a matching pair of RAND and RES*.
- RES* (128 bits) is a (fixed, semi-public) function solely of RAND and *K* (128 bits).
- Grover's algorithm means that $O(2^{64})$ work is required to deduce *K*.

Session security

- A somewhat similar Grover-algorithm-based attack could be based on intercepted ciphertext.
- However, such an attack would require known plaintext and also knowledge of RAND.
- That is, such attacks are more difficult than those based on the AKA messages.
- Note that MACs are computed on plaintext prior to encryption, and hence so do not help.

Information Security Group

Attack impact

- Note that these attacks will only yield the long term key *K* for a single USIM, allowing cloning of this USIM and deriving of operational keys.
- That is, $O(2^{64})$ quantum operations will be needed to break a single USIM.
- 2^{64} computations is still a lot on a modern conventional computer, which have been developed over 70 years.
- Of course, if operator derives USIM keys from a 128-bit master key then all bets are off …

39

39

Information Security Group

When is a solution needed?

- Observe that USIMs potentially have a long lifetime.
- Unfortunately the attack can be performed using recorded RAND-RES* pairs, and so the problem should be fixed *as soon as possible*.
- Of course, switching USIMs is not so hard, but networks may wish to avoid encouraging users to switch USIMs lest they also switch network.

40

40

Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

41

41

Public key availability

- Mobile identity (SUPI) encryption can be performed in the ME, and in this case the ME needs to be given the public key by the USIM.
- That is any USIM must output the home network public key 'on demand'.
- So the public key is in the public domain.
- Even if the USIM does the SUPI encryption, the long-term public key will be in every USIM and so is prone to reverse-engineering attack.

42

42

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Shor's algorithm

- An opponent armed with a quantum computer can use Shor's algorithm to derive the home network private key from the public key.
- This will then re-enable *IMSI-catcher* attacks, where a fake network can ask a UE to reveal its permanent identity.
- This will apply to all UEs for that network.

43

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

When is a solution needed?

- In principle this could be fixed *just in time* by replacing the asymmetric algorithm.
- This is because learning where a user was in the past is not so sensitive.
- You can't do IMSI-catching retrospectively.
- However, upgrading the algorithm without changing the USIM is likely to be tricky, so making the change as soon as possible would be highly desirable.

44

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

45

45

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

A way forward

- Because of the way the system is designed, it seems possible to develop a three-phase approach to a post-quantum-secure 5G.
- This should allow a simple and smooth migration.
- Painful real-world experience says that a simple migration path is absolutely critical in practice.

46

46

Information Security Group

Phase 1: Long-term secret key

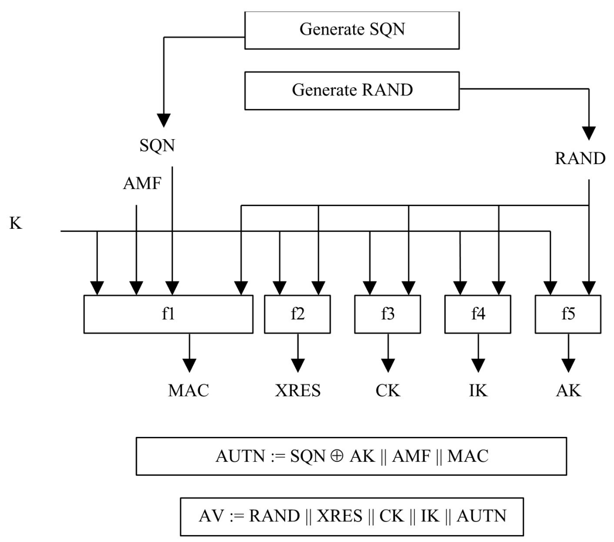
- Observe that the long-term secret key *K* never leaves the USIM or issuing network ARPF.
- The key *K* is only ever used as shown in the diagram.
- That is, it is only ever used as input to the functions *f*1 – *f*5.

47

47

Information Security Group

Use of the secret key *K*



48

48

Information Security Group

Implications of 256-bit key K

- Note that *f*1 – *f*5 are operator-specific.
- So a USIM equipped with a **256-bit key could be deployed with existing handsets and infrastructure today** – as long as the issuing network's ARPF is updated appropriately.
- Of course, new functions *f*1 - *f*5 will be needed, and the standards updated to allow this.

49

49

Information Security Group

What needs to be changed?

- Just a few simple changes are needed:
  - update the standards (probably only 3GPP TS 33.105) to permit longer keys;
  - update the standards to give requirements for *f*1 – *f*5 in case of a 256-bit key *K*;
  - update the standards to provide a new set of 'example' functions *f*1 – *f*5;
  - encourage operators and manufacturers to switch.

50

50

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

How does it affect security?

- A 256-bit key will be post-quantum-secure (assuming functions designed with care).
- This prevents cloning of USIMs.
- Only remaining attack would be to discover derived 128-bit operational keys.
- Impact of such an attack would be small relative to the high per-key attack cost, since such keys are changed every few hours.

51

51

Information Security Group

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Phase 2: Asymmetric encryption

- Asymmetric encryption/decryption only ever in the USIM, (optionally) the ME, and the home network.
- So, pending the availability of upgraded handsets, an operator **could switch to a post-quantum-secure scheme today**, assuming:
  - the availability of appropriate USIMs capable of performing the new encryption algorithm; and
  - necessary changes to the issuing network.
- Once a new encryption algorithm is standardised and implemented in handsets, the USIM can delegate encryption to the ME.

52

52

What needs to be changed?

- The following changes will be needed:
  - selection of a post-quantum-secure asymmetric encryption algorithm, presumably once standards for such algorithms are available (e.g. from NIST);
  - inclusion of the scheme in the relevant standards;
  - at some point, the inclusion of this algorithm in handsets will need to be mandated;
  - encourage operators to adopt the scheme.

How does it affect security?

- Changing the algorithm will prevent compromise of the encrypted SUPI.
- This will restore mobile identity confidentiality to the status it has today.
- Sadly it is not 100% robust, as active error-message-based attacks are possible to link two appearances of the same UE.

Phase 3: Key derivation and use

- Currently, all operational keys (ultimately derived from CK and IK) are 128 bits long.
- Post-quantum-security will require changing all keys to 256 bits and upgrading all algorithms to use 256-bit keys.
- Fortunately:
  - all keys are derived from the combination of CK and IK (total of 256 bits), and
  - 256 bit keys are already derived at each stage (although only 128 of the 256 are actually used).

What needs to be changed?

- The following changes will be needed:
  - selection of appropriate 256-bit-key encryption and MAC functions;
  - inclusion of the new functions in the relevant standards;
  - mandating manufacturers and operators to implement these functions;
  - switching all these functions on – e.g. in 6G.
- No new USIMs needed (assuming already upgraded in Phase 1)!

How does it affect security?

- If:
  - all keys are 256 bits long, and
  - are derived from 256-bit keys (or equivalent);
  - key derivation functions are well-selected;
- then no quantum computer based attacks using Grover's algorithm will be possible.

Agenda

- Introduction
- Quantum computing
- 5G security
- Impact I – symmetric crypto
- Impact II – asymmetric crypto
- A phased solution
- Conclusions

Information Security Group

Summary of findings

- Have proposed a three-phase series of evolutionary changes to enable a post-quantum secure mobile network.
- The most significant changes will simultaneously make the 3G, 4G and 5G long-term secret key post-quantum secure.

59

59

Information Security Group

Summary of recommendations

- A three-phase sequence of upgrades is proposed:
  1. Switch to 256-bit USIM keys for all new USIMs **asap** – affects only USIMs and the ARPF (old USIMs will continue to work) – fixes 3G, 4G, 5G;
  2. Upgrade to post-quantum-secure asymmetric encryption – affects only USIMs, handsets and home networks – **when algorithms available**;
  3. **In long term** upgrade all symmetric algorithm keys to 256 bits – affects everything apart from USIMs and the ARPF.

60

60

Good news

- Slightly bizarrely, 3GPP TS 33.501 (5G security architecture) already allows both 128-bit and 256-bit keys *K*, so moves are already afoot to switch.
- However, 3GPP TS 33.105, which specifies how *K* is used and also the requirements on *f*1 – *f*5, specifies only a 128-bit key.
- 256-bit key candidates for *f*1 – *f*5 have also been devised – called **TUAK** (see 3GPP TS 35.201).
- So Phase 1 is almost done, except for making the final changes to the standards and encouraging operators to get moving …

61

61

Other news

- The functions used for key derivation (mainly based on SHA-256) have already been specified in such a way that moving to 256-bit keys throughout should be straightforward.
- Of course, network infrastructures and handsets will need to be upgraded to support algorithms using longer keys before the solution can be enabled.
- This seems a long way off.

62

62

More information

- A preprint covering most of the material in this talk was recently posted to arXiv:
  - Chris Mitchell, *The impact of quantum computing on real-world security: A 5G case study*. arXiv:1911.07583v1 [cs.CR] 18 Nov 2019.
- All 3GPP specifications are available from the 3GPP website: http://www.3gpp.org