Cryptography for Mobile security

Valtteri Niemi
University of Helsinki
Fall 2016
• The secret key of user i exists (and stays) only in two places:
  - in her own SIM card
  - in the Authentication Center
Trust model

• Each operator shares long term security association with its subscriber
  – Security association credentials stored in tamper-resistant identity module issued to subscriber (called the SIM or UICC)

• Operators may enter roaming agreements with other operators → a certain level of trust exists between the respective domains
Original design decisions for GSM security

• GSM aimed to be *as secure as the fixed networks* to which it would be connected
• *Active attacks* which involve impersonating a network element were intentionally *not* addressed
Authentication of user i

- Authentication Center chooses a random number RAND and computes

\[
\text{RAND} \rightarrow \text{K}_i \rightarrow \text{one-way function} \rightarrow \text{SRES} \rightarrow \text{Kc}
\]

- The triple (RAND, SRES, Kc) is sent to the MSC/VLR.
- MSC/VLR sends RAND to the phone.
- The one-way function of computing SRES/Kc is called A3/A8. These are operator-specific.
The SIM card computes

\[
\text{RAND} \quad K_i
\]

and sends the output SRES’ to the MSC/VLR.

- If SRES = SRES’, then the call is accepted.
Encryption of the call

• During the authentication a secret key is exchanged:
  \[ K_c = K'_c \]
  by which all calls/signalling are encrypted between the phone and the base station until the next authentication occurs.

• The encryption algorithm is called A5. The first two versions A5/1 and A5/2 were standardized but the specs are confidential and managed by GSM Association. The third version A5/3 is publicly available. All make use of 64-bit keys Kc.

• As a Rel-9 addition, there is also a 128-bit key algorithm A5/4.
  – Deployment of this is more difficult than in A5/3 case because longer keys require changes in many parts of the system
Structure of A5 stream cipher

Kc (64 bits) \rightarrow \text{core of A5} \rightarrow \text{pseudorandom bit stream (114)} \rightarrow \text{plain message (114)} \rightarrow \text{encrypted message (114)}
GSM security protocol

MS (SIM)  MSC/VLR  HLR
IMSI, Ki  (and BTS)  {{IMSI, Ki}}

IMSI / TMSI  IMSI

RAND  RAND, XRES, Kc

Kc

SRES

SRES = XRES ?

encrypted TMSI
Barkan–Biham A5/2 Attack (from 2003)

Exploited weaknesses in cryptographic algorithms:
  – A5/2 can be broken very fast

... and exploited also other legacy features in the GSM security system:
  – A5/2 was a mandatory feature in terminals
  – Call integrity based only on encryption
  – Same Kc is used in different algorithms
  – Attacker can force the victim MS to use the same Kc by RAND replay

An example attack: Decryption of strongly encrypted call
  – Catch a RAND and record a call encrypted with Kc and A5/3
  – Replay the RAND and tell the MS to use A5/2
  – Analyse Kc from the received encrypted uplink signal
  – Decrypt the recorded call with Kc
Countermeasure

- Withdrawal of A5/2 from all 3GPP terminals (starting from release 6)
GPRS security

- Similar to GSM security
- SGSN takes the role of MSC/VLR for authentication
- **Encryption** terminates also in SGSN
  - Embedded in Logical Link Layer (LLC)
  - Counter: frame number (22 bits) replaced by LLC counter (32 bits)
  - Algorithms:
    - GEA1 (confidential, weakest)
    - GEA2 (confidential)
    - GEA3 (publicly available)
    - GEA4 (Rel-9 addition; first to use 128-bit keys instead of 64-bit keys)
3G security
3G security background

• Leading *design principles* were:
  – Move useful 2G security features to 3G
  – Add countermeasures against real weaknesses in 2G

• Main *security characteristics* in GSM ( = 2G ):
  - User authentication & radio interface encryption
  - SIM used as security module
  - Operates without user assistance
  - Requires minimal trust in serving network

• Main *weaknesses* in GSM:
  - Active attacks are possible (false BS etc.)
  - Authentication data (e.g. cipher keys) sent in clear inside one network and between networks
  - Cipher keys too short (if 64 bits)
  - Secret algorithms do not create trust
Active attack

• A false element masquerades
  – as a base station towards terminal
  – as a terminal towards network

• Objectives of the attacker:
  – eavesdropping
  – stealing of connection
  – manipulating data
3G system architecture

based on GSM/GPRS architecture

Encryption & integrity
Execution of authentication
Transport of auth data
Mutual authentication

- There are three entities involved:
  - Home network HN (AuC)
  - Serving network SN (VLR/SGSN)
  - Mobile station MS (USIM)
- Executed whenever SN decides

- The idea: SN checks MS’s identity (as in GSM) and MS checks that SN has authorization from HN
- A master key $K$ is shared between MS and HN
- GSM-like challenge-response in user-to-network authentication
- Network proves its authorization by giving a token AUTN which is protected by $K$ and contains a sequence number SQN

- Each operator may use its own algorithms for authentication
- At the same time keys for ciphering and integrity checking are derived
- Ciphering and integrity checking are performed in MS and in RNC and these are independent of the authentication mechanism
Generation of security parameters

SN

IMSI

RAND, K, SQN

XRES, AUTN, CK, IK

HN

RAND, AUTN, XRES, CK, IK
3G Authentication & key agreement

checks whether SQN is big enough

checks RES = XRES?
3G ciphering mechanism

- Between UE and RNC
- Stream cipher like in GSM and GPRS
- Key length 128 bits
- Key lifetime could be limited.

- Begins with RNC sending “Security mode command”
- Layer:
  - RLC for non-transparent RLC mode
  - MAC for transparent RLC mode
- Both MSC/VLR and SGSN may give cipher keys to RNC. One key is used for each CN domain user data. The key for signaling data is changed whenever a new key is generated (which means key changes during active connections).
3G Ciphering algorithm

COUNT-C/32  DIRECTION/1
BEARER/8  LENGTH

CK/128

KEYSTREAM BLOCK

Plaintext MAC SDU or RLC PDU (data part)  +  Ciphered MAC SDU or RLC PDU (data part)
UEA1 (based on KASUMI block cipher)

\[
\text{COUNT} \ || \ \text{BEARER} \ || \ \text{DIRECTION} \ || \ 0...0
\]

KASUMI

\[
\text{BLKCTR} = 0
\]

KASUMI

\[
\text{BLKCTR} = 1
\]

KASUMI

\[
\text{BLKCTR} = 2
\]

KASUMI

\[
\text{BLKCTR} = n
\]

KASUMI

\[
CT[i] = PT[i] \ XOR \ KS[i]
\]
KASUMI
block cipher
S7 substitution box

int S7[128] = {
  54, 50, 62, 56, 22, 34, 94, 96, 38, 6, 63, 93, 2, 18, 123, 33,
  55, 113, 39, 114, 21, 67, 65, 12, 47, 73, 46, 27, 25, 111, 124, 81,
  53, 9, 121, 79, 52, 60, 58, 48, 101, 127, 40, 120, 104, 70, 71, 43,
  20, 122, 72, 61, 23, 109, 13, 100, 77, 1, 16, 7, 82, 10, 105, 98,
  117, 116, 76, 11, 89, 106, 0, 125, 118, 99, 86, 69, 30, 57, 126, 87,
  112, 51, 17, 5, 95, 14, 90, 84, 91, 8, 35, 103, 32, 97, 28, 66,
  102, 31, 26, 45, 75, 4, 85, 92, 37, 74, 80, 49, 68, 29, 115, 44,
  64, 107, 108, 24, 110, 83, 36, 78, 42, 19, 15, 41, 88, 119, 59, 3
};
Integrity protection

• Purpose: to authenticate *individual* RRC signaling messages

• Examples of *critical* messages:
  – from MS to RNC:
    - MS capabilities, including authentication, ciphering and integrity algorithm capabilities
    - Security control accept/reject message
    - Called party number in a mobile originated call
    - Periodic message authentication messages
    - Cell and URA updates
  – from RNC to MS:
    - Security mode command, including whether ciphering is enabled or not and the ciphering and integrity algorithms that are used
    - Periodic message authentication messages.

• **Almost all** RRC messages are integrity protected
For **UIA1**: the one-way function is based on **KASUMI** block cipher
Second set of algorithms based on SNOW3G

• These are called UEA2 and UIA2
• Added in 3GPP release 7 (in 2006)
• SNOW3G is a stream cipher
  – based on SNOW 2.0 (Nordic origin)
  – structure of UEA2 is straight-forward
SNOW 3G: structure
UIA2 based on SNOW 3G

Padded message $M$ goes through $f_M$ and then through a multiplication operation, resulting in OTP. OTP is then truncated to MAC.
Network domain security (based on IPsec)
Status on 3G security today

- 3G security resilient against security analyses
- No significant attacks known on cryptographic algorithms
- No false base station attacks seem possible
- 3G security seems still sufficient for 3G networks
Brief introduction to LTE (= 4G)
SAE / LTE: What and why?

SAE = System Architecture Evolution
LTE = Long Term Evolution (of radio networks)

• LTE offers higher data rates, up to 100 Mb/sec
  – Multi-antenna technologies
  – New transmission schema based on OFDM
  – Signaling/scheduling optimizations

• SAE offers optimized (flat) IP-based architecture
  – Two network nodes for user plane
  – Simplified protocol stack
  – Optimized inter-working with legacy cellular, incl. CDMA
  – Inter-working with non-3GPP accesses, incl. WiMAX
SAE / LTE: What and why?

SAE = System Architecture Evolution
LTE = Long Term Evolution (of radio networks)

• Technical terms:
  – E-UTRAN = Evolved UTRAN (LTE radio network)
  – EPC = Evolved Packet Core (SAE core network)
  – EPS = Evolved Packet System ( = RAN + EPC )
EPS architecture (non-roaming case)

From 3GPP TS 23.401
EPS architecture (one of the roaming variants)

From TS 23.401
E-UTRAN architecture

From 3GPP TS 36.300
Essential elements of EPS

From “LTE security”
From TS 23.402
Roaming case (one variant)

From TS 23.402
LTE Security
Implications of LTE/SAE architecture on security

- **Flat architecture:**
  - All radio access protocols terminate in one node: eNodeB
  - IP protocols also visible in eNB

- **Security implications due to**
  - Architectural design decisions
  - Interworking with legacy and non-3GPP networks
  - Allowing eNB placement in untrusted locations
  - New business environments with less trusted networks involved
  - Trying to keep security breaches as local as possible

- **As a result (when compared to UTRAN/GERAN):**
  - Extended Authentication and Key Agreement
  - More complex key hierarchy
  - More complex interworking security
  - Additional security for eNB (compared to NodeB/BTS/RNC)
Threats against EPS (1/2)

• Threats against user identity
• Other threats against privacy
• Threats of UE tracking:
  – e.g. tracking a user based on an IP address that could potentially be linked to an IMSI
• Threats related to handovers:
  – e.g. forcing a handover to a compromised base station by a powerful signal;
• Threats related to base stations and last-mile transport links:
  – e.g. injecting packets directly into the last-mile transport link or physical compromise of base stations in vulnerable locations;
• Threats related to multicast or broadcast signalling:
  – e.g. broadcasting false system information
• Threats related to denial of service:
  – e.g. by means of radio jamming or launching a distributed attack from many UEs
Threats against EPS (2/2)

• Threats of misusing network services:
  – e.g. flooding the network from inside the network by compromised elements or from outside
• Threats against the radio protocols:
  – e.g. faking or modifying the first radio connection establishment messages from UE
• Threats related to mobility management:
  – e.g. disclosure of sensitive data about users’ locations;
• Threats of manipulation of control plane data
• Threats of unauthorised access to the network
EPS security requirements (high-level)

- EPS shall provide a high level of security.
- Any security lapse in one access technology shall not compromise other accesses.
- EPS should provide protection against threats and attacks.
- EPS shall support authenticity of information between the terminal and the network.
- Appropriate traffic protection measures should be provided.
- EPS shall ensure that unauthorised users cannot establish communications through the system.
EPS security requirements (service-related)

• EPS shall allow a network to **hide** its internal structure from the terminal.
• Security **policies** shall be **under home operator control**.
• Security solutions should **not interfere with service delivery or handovers** in a way noticeable for end-users.
• EPS shall provide support for **lawful interception**.
• Rel-99 (or newer) **USIM is required** for authentication of the user towards EPS.
• USIM shall not be required for re-authentication in **handovers** (or other changes) between EPS and other 3GPP systems, unless requested by the operator.
• EPS shall support IMS **emergency calls**.
EPS security requirements (privacy-related)

- EPS shall provide several appropriate levels of user privacy for communication, location, and identity.
- Communication contents, origin, and destination shall be protected against disclosure to unauthorised parties.
- EPS shall be able to hide user identities from unauthorised parties.
- EPS shall be able to hide user location from unauthorised parties, including another party with which user is communicating.
EPS security features

- Confidentiality of the user and device identities
- Authentication between the UE and the network
- Confidentiality of user and signalling data
- Integrity of signalling data
- Visibility and configurability of security
- Platform Security of the eNodeB
- Lawful interception
- Emergency calls
- Interworking security
- Network domain security
- IMS security for voice over LTE
Major design decisions for EPS security (1/2)

- Permanent security association
  - Inherited from GSM and 3G
- Interfaces in UE and HSS/HLR
  - ME-USIM interface is fully standardized but HSS-AuC is not
- Reuse of 3G USIMs
- **No** reuse of 2G SIMs in EPS
- Delegated authentication
  - Inherited from GSM and 3G
- Reuse of 3G AKA
- Cryptographic network separation
- Serving network authentication
Major design decisions for EPS security (2/2)

• Termination point for encryption and integrity protection
  – Flat architecture required moving to base station site
• New key hierarchy in EPS
• Key separation in handovers
• Homogeneous security for heterogeneous access networks
• User identity confidentiality not protected against active attackers
• Other „NOT“ – decisions:
  – No integrity protection for user plane on radio interface
  – No (cryptographic) non-repudiation of charging
Identity confidentiality in EPS (1/2)

- Mechanism inherited from GSM and 3G
- User’s permanent identity (IMSI) is sent to the network only if network cannot identify the UE otherwise

From 33.401
Identity confidentiality in EPS (2/2)

- Network assigns a temporary identity for the UE
- It is sent to the UE in encrypted message
- In GSM/3G the temporary identity is
  - TMSI for CS domain
  - P-TMSI for PS domain
- In EPS the temporary identity is called GUTI (Globally Unique Temporary Identity)
Authentication and key agreement
Authentication and key agreement

- HSS generates authentication data and provides it to MME
- Challenge-response authentication and key agreement procedure between MME and UE
AKA protocol

Authentication data request
IMSI, SN identity, Network Type

Authentication data response
EPS-Authentication Vector (s)

User authentication request (RAND, AUTN, KSI_{ASME})

User authentication response (RES)

From TS 33.401
From “LTE security”
Generation of UMTS and EPS AV’s

From “LTE security”
Verification in USIM

Verify that SQN is in the correct range
Verify MAC = XMAC

From “LTE security”
Authentication failure types

• MAC code failure
  – XMAC differs from MAC

• Synchronization failure
  – SQN not in correct range
  – Re-synchronization is possible (next slide)

• Incorrect type of AV
  – Check a specific AMF separation bit (see later slide)

• Invalid authentication response
  – XRES differs from RES
Authentication re-synchronization parameter

\[ \text{AUTS} = \text{SQN}_\text{MS} \oplus \text{AK} \parallel \text{MAC-S} \]

From “LTE security”
LTE Data protection
Confidentiality and integrity of signalling

- RRC signalling between UE and E-UTRAN
- NAS signalling between UE and MME
- S1 interface signalling
  - protection is not UE-specific
  - optional to use
EPS signalling protection

From “LTE security”
User plane confidentiality

- S1-U protection is not UE-specific
  - (Enhanced) network domain security mechanisms (based on IPsec)
  - Optional to use
- Integrity is not protected for various reasons, e.g.:
  - performance
  - limited protection for application layer
EPS user plane protection

From “LTE security”
Ciphering mechanism

Extract from 3GPP TS 33.401
Integrity protection
Start of AS protection

UE

ASSecurityModeCommand
(integrity alg., ciphering alg., MAC-I)

ASSecurityModeComplete
(MAC-I)

ASSecurityModeReject

E-UTRAN
Cryptographic network separation (1/2)

**USIM / AuC**

\[ K \]

**UE / HSS**

\[ CK, IK \] [Network id]

**UE / MME**

\[ K_{NASenc} \] \[ K_{NASint} \]

**UE / eNB**

\[ K_{UPenc} \] \[ K_{RRCint} \] \[ K_{RRCenc} \]
Cryptographic network separation (2/2)

- Authentication vectors in EPS are specific to the serving network
  → AV’s usable in EPS cannot be used in GERAN or UTRAN
- AV’s usable for UTRAN/GERAN access cannot be used for E-UTRAN access
  - Solution by a “separation bit” in AMF field
- On the other hand, Rel-99 USIM is sufficient for EPS access
  → ME has to check the “separation bit” (when accessing E-UTRAN)
- As one consequence, “EAP-AKA’ “ was created in IETF
LTE crypto-algorithms
Crypto-algorithms

• Two sets of algorithms from Day One
  – If one breaks, we still have one standing
  – Should be as different from each other as possible
  – AES and SNOW 3G chosen as basis → ETSI SAGE has specified/chosen modes

• A third algorithm set was added for Release 11
  – The base algorithm ZUC is of Chinese origin and usable in China

• Rel-99 USIM is sufficient → master key 128 bits
  – All keys used for crypto-algorithms are 128 bits but included possibility to add 256-bit keys later (if needed)

• Deeper key hierarchy → (one-way) key derivation function needed
  – HMAC-SHA-256 chosen as basis
SNOW 3G

- The only algorithm that was inherited from 3G
- Discussed earlier
Structure of ZUC
Structure of EEA3
ZUC resistance verified against:

- Weak key attacks
- Guess-and-Determine Attacks
- BDD Attacks
- Inversion Attacks
- Linear Distinguishing Attacks
- Algebraic Attacks
- Chosen IV Attacks
- Time-Memory-Data Trade-Off Attacks
- Timing Attacks
Conclusions of ETSI SAGE evaluations of EEA3/EIA3

• “One stated objective for the design was that the new algorithms be substantially different from the first and second LTE algorithm sets, in such a way that an attack on any one algorithm set would be unlikely to lead to an attack on either of the others. In SAGE’s view this objective is not fully met – there are some architectural similarities between ZUC and SNOW 3G, and it is possible that a major advance in cryptanalysis might affect them both. However:
  – there are important differences too, so ZUC and SNOW 3G by no means “stand or fall together”;
  – and in any case the raison d’être of this new algorithm set is very different from that of the first two, so the objective is considerably less important than making the first and second algorithm sets different from each other.

• SAGE therefore does not consider this a barrier to acceptance of the new algorithms. Indeed, both of the paid evaluation teams noted that the ZUC design inherits some strong security properties from SNOW 3G, while adding further protection against as yet unknown attacks.”
Need for algorithm agility: example

Theory break of algo 2

Spec work for algo 3

Practical break of algo 2

Algo 3 implemented

Majority of terminal base supports algo 3
Need for algorithm agility: example

Theory break of algo 2

Practical break of algo 2

Dependent on one algo only

Spec work for algo 3

Algo 3 implemented

Majority of terminal base supports algo 3
Caveat: Security of algorithm capability negotiation

- Algorithm capabilities exchanged first without protection
- Re-exchanged and verified once integrity protection is turned on → all integrity algorithms should resist real-time attacks in the beginning of the connection

- If this is not the case anymore, broken algorithm has to be withdrawn completely from the system
  - In the same way as A5/2 is withdrawn from GSM
Handovers and interworking
Handovers without MME involvement (1/2)
Handovers without MME involvement (2/2)

- Handovers are possible directly between eNB’s for performance reasons
- If keys would be passed as such, all eNB’s in a “HO chain” would know all the keys → one compromised eNB would compromise all eNB’s in the “HO chain”
- Countermeasures:
  - One-way function used before key is passed (*Backward security*)
  - MME is involved after the HO for further key passes (**Forward security**, effective after two hops)
  - When MME involved already during the HO, Forward security is effective already after one hop
$K_{eNB}$ derivations

From TS 33.401
Interworking with UTRAN/GERAN (1/2)

• UE may be registered in both SGSN and MME simultaneously
  → when moving from one system (source) to the other (target) both
  native keys (created earlier in the target system) and
  mapped keys (converted from the keys in the source system) may exist
  – Note: native keys exist only for Rel-8 SGSN, not for legacy SGSN
Interworking with UTRAN/GERAN (2/2)

• Idle mode transition
  – From E-UTRAN to UTRAN: either *mapped* or *native* keys are used (depending on the identity used in Routing Area Update Request)
  – From UTRAN to E-UTRAN: *native* keys are used *but* an exceptional case exists also

• Handover
  – From E-UTRAN to UTRAN: *mapped* keys are used
  – From UTRAN to E-UTRAN: *mapped* keys are used *but* it is possible to activate the *native* keys after HO completed (using *key-change-on-the-fly* procedure)
Lawful interception
Lawful interception in 3GPP

LEA
3GMS

INTERCEPT REQUEST
3 GMS node

INTERCEPT REQUEST

NETWORK RELATED DATA

INTERCEPT REQUEST

TECHNICAL INTERCEPTION

HANDOVER INTERFACE
When LI is invoked: examples

• A **circuit switched call** is requested originated from, terminated to, or redirected by the target

• **Location** information related to the target facility is modified by the subscriber attaching or detaching from the network, or if there is a change in location

• An **SMS** transfer is requested - either originated from or terminated to the target

• A **data packet** is transmitted to or from a target
What is intercepted?

- **CC = Content of Communications**
  - Intercepted from media plane entities, e.g. in EPS: Serving Gateway

- **IRI = Intercept Related Information**
  - E.g. in the case of Attach:
    - *Observed MSISDN*
    - *Observed IMSI*
    - *Observed ME Id*
    - *Event Type*
    - *Event Time*
    - *Event Date*
    - *Network Element Identifier*
    - *Location Information*
    - *Failed attach reason*
    - *Etc.*
Relay Node architecture

(From TS 36.300)
Relay Node architecture (cont’d)

- RN appears as regular eNB towards UE
- In some aspects, RN acts like UE towards network
- Goal is to extend coverage and throughput
Relay node security

- Security between RN and network based on UICC and AKA
- Secure channel between the UICC and the RN, established based on
  - Pre-shared keys or
  - Certificates
- RN meets platform security requirements similar to those of Home eNB
- User plane integrity is provided between RN and DeNB (unlike between “normal” UE and “normal” eNB)
  - Key hierarchy extended because of this (see next slide)
Relay node security (cont’d)

USIM / AuC

K

CK, IK

UE / HSS

K_{ASME}

UE / MME

K_{NASenc} \quad K_{NASint}

UE / eNB

K_{UPint} \quad K_{UPenc} \quad K_{RRCint} \quad K_{RRCenc}

K_{eNB / NH}
Security aspects typically not standardized

• Product implementations
  – Secure SW development
  – HW security
  – Security testing and audits

• Organizational aspects
  – Organization of security in a corporation
  – Security awareness
  – CERT

• Operational aspects
  – Anti-virus, vulnerability scanning
  – Firewalls
  – Intrusion detection and prevention
  – Fraud management systems
Some future challenges

- Machine-to-machine communications
- Internet of Things / Internet-connected smart objects
- Sensor networks
- Device-to-device communications
- Privacy enhancements
- Impacts of Cloud computing
LTE security: Summary
Summary

– New architecture and business environment require enhancements to 3G security
– Radio interface user plane security terminates in base station site
– Cryptographic separation of keys
– Security mechanisms extended to support Relay Nodes
– New architectures create challenges with Lawful interception
More information

www.3gpp.org
Perspectives to 5G
5G targets (according to METIS)

- 1000 x higher mobile data volume per area
- 10 to 100 x higher number of connected devices
- 10 to 100 x higher typical user data rate
- 10 x longer battery life for low power machine communications
- 5 x reduced End-to-End latency
5G architecture (according to METIS)
5G key technologies

• Cloud computing
• Software-defined networking
• Network function virtualization
• (Direct) device-to-device communications
• Machine-to-machine communications
Some 5G security challenges

• Isolation of functions in virtualized environment
• All issues with SDN and Cloud Computing
• Potential lack of infra support in device-to-device communications
• Potential lack of human intervention in machine-to-machine communications
A privacy challenge: Identity confidentiality (1/2)

- 4G mechanism was inherited from GSM and 3G
  - User’s permanent identity (IMSI) is sent to the network only if network cannot identify the UE otherwise

From 33.401
Identity confidentiality (2/2)

• Network assigns a temporary identity for the UE
• It is sent to the UE in encrypted message
• In GSM/3G the temporary identity is
  – TMSI for CS domain
  – P-TMSI for PS domain
• In EPS the temporary identity is called GUTI (Globally Unique Temporary Identity)

**CHALLENGE:** Is this still good enough for 5G also?
If not - how to find an efficient solution to protect user identity?
Cryptoalgorithms 1/2

• It cannot be excluded that quantum computers could appear during the lifetime of 5G
• Therefore 256-bit keys are a safe bet
• On the other hand, if they do not appear, 128-bit keys are enough
• → start with 128-bit keys but with built-in upgradability?
Cryptoalgorithms 2/2

• In the heterogeneous environment, many algorithms will be needed
  – Legacy networks
  – Several new technologies with cryptofunctions in low layers

• Algorithm agility needs to be guaranteed