Wireless Cellular Network Security: Part 7

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi, "*LTE Security*", John Wiley and sons, 2nd edition, 2013.

Key Hierarchy

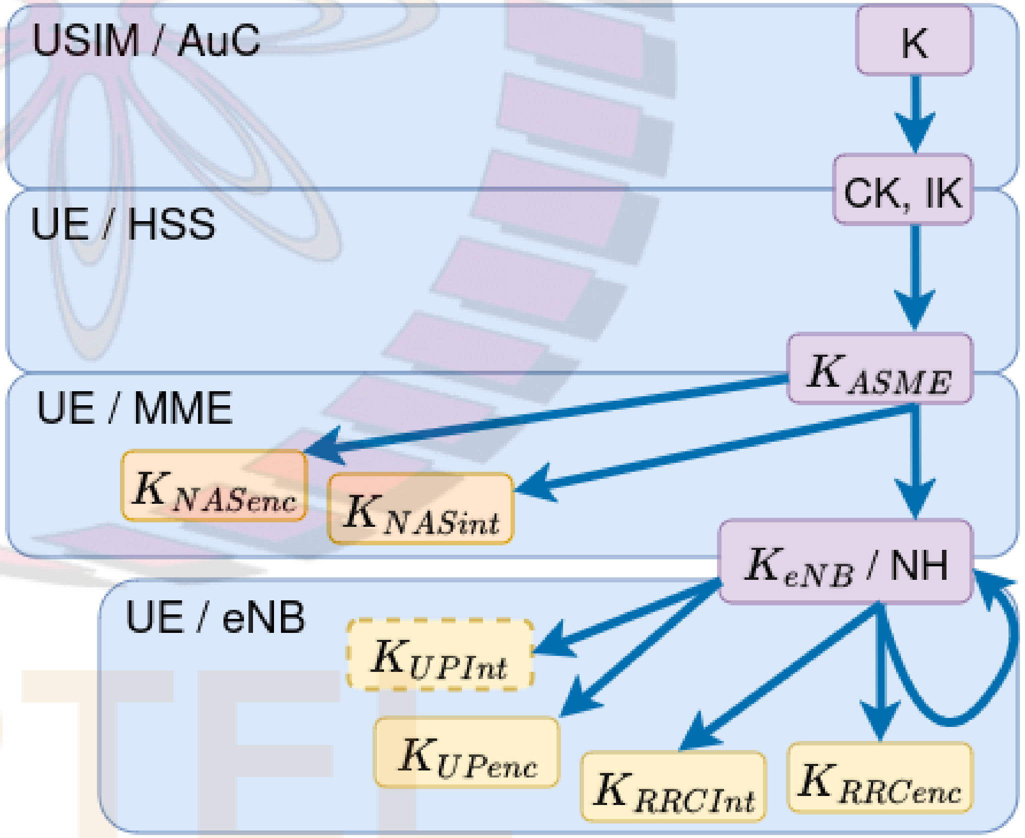
- All cryptographic keys that are needed for various security mechanisms are derived from the intermediate key K_{ASME}
  - ❑ can be viewed as a 'local master key' for the subscriber, in contrast to the permanent master key K
- On the network side, the intermediate local master key K_{ASME} is stored in MME, while permanent master key K is stored in AuC
- Advantages of using an intermediate key:
  - ❑ Enables cryptographic key separation, which implies that each key is usable in one specific situation (or context) only
    - o knowing a key that is used in one context does not help in trying to guess what key is being used in another context
  - ❑ Also improves the system in terms of providing key freshness
    - o i.e., it is possible to more often renew the keys used in security mechanisms, e.g., in ciphering
    - o we do not have to run EPS AKA each time we want to renew keys used for protecting the radio interface, so we do not have to involve the home network to obtain fresh keys
- Disadvantage of using intermediate keys:
  - ❑ added complexity: there are more types of keys in the system, all of which need to be computed, stored, protected, kept in sync, etc.
- Thus, we have a security versus complexity trade-off situation:
  - ❑ for EPS, the security benefits of using an intermediate key outweigh the added complexity, whereas the reverse was true at the design phase of 3G security

Key Hierarchy (contd.)

- After the idea of using the intermediate key K_{ASME} was introduced in the design of EPS security, it was natural to take a further step:
  - ❑another intermediate key K_{eNB} was added that is stored in the eNB
- Addition of K_{eNB} makes it possible to renew keys for protection of radio access without involving the MME

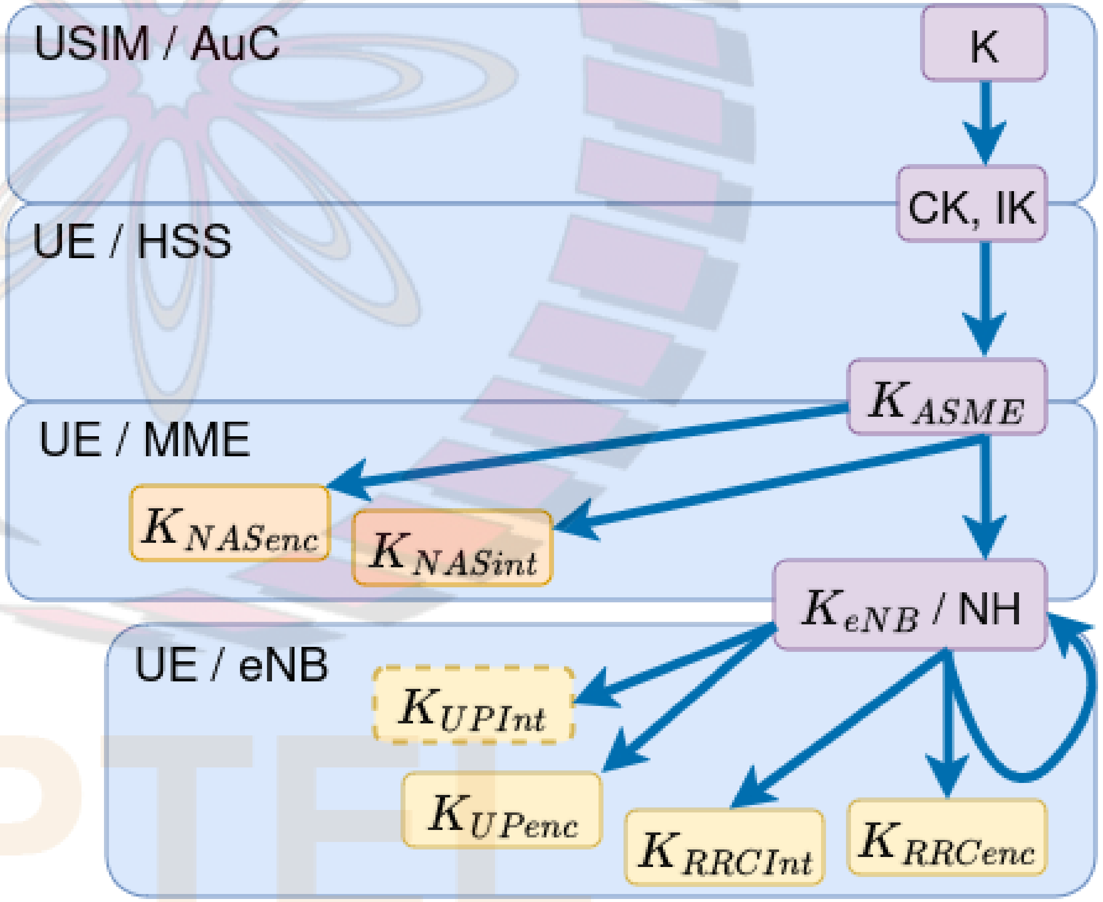
Key Hierarchy (contd.)

- Fig. shows the whole key hierarchy of EPS
  - ❑ UMTS key hierarchy is a small subset of this and consists of K, CK, and IK only
  - ❑ arrow between two keys means that one key (the one to which the arrow points) is derived from the other
    - o In all cases, there are also additional input parameters that are needed in the derivation
    - o None of the additional parameters is assumed to be secret information
- For all cases except K_{eNB}/ Next Hop (NH), each key is always derived from another key at a higher layer in the hierarchy
- The special case where there is an arrow from K_{eNB}/ NH to itself is in context of certain handover situations between eNBs where MME is not involved
  - ❑ NH is a transitional, intermediate key generated during handovers
  - ❑ details omitted



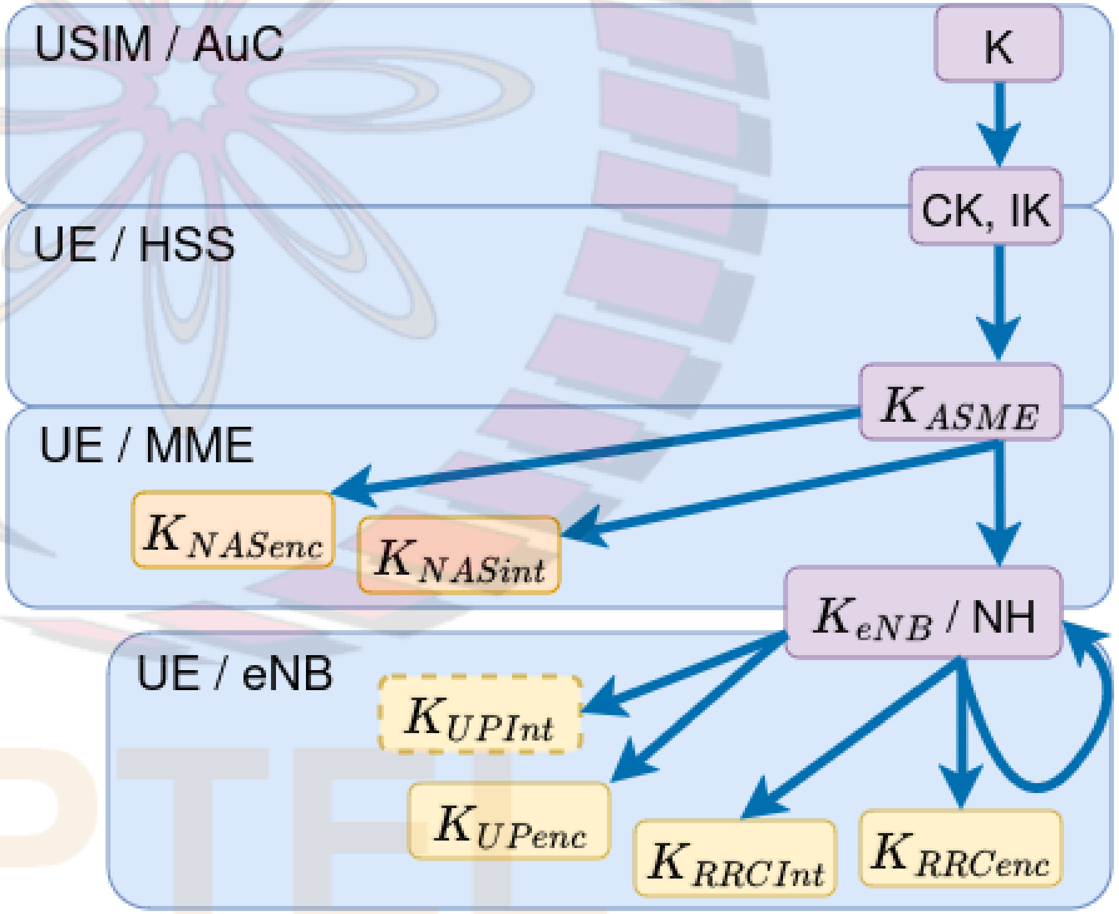
Key Hierarchy (contd.)

- Important property of key derivation:
  - ❑ starting from keys in lower layers of the key hierarchy, it is impossible in practice to compute keys in the higher layers
- The topmost key derivation from K to CK and IK happens:
  - ❑ on the user side, inside the USIM and, on the network side, inside the AuC
- K_{ASME} is independently derived in UE and MME from CK, IK and other inputs, as discussed earlier
- K_{eNB} is derived from K_{ASME} and an additional input, which is a counter parameter
  - ❑ This additional parameter is needed to ensure that each new K_{eNB} derived from K_{ASME} differs from the ones derived earlier
  - ❑ Purpose of K_{eNB} is to be a local master key in an eNB



Key Hierarchy (contd.)

- K_{NASenc} (respectively, K_{NASint}) is a key used to encrypt (respectively, protect the integrity of) NAS signalling traffic
  - ❑ derived from K_{ASME} and two additional parameters
- K_{RRCenc} (respectively, K_{RRCint}) is a key used to encrypt (respectively, protect the integrity of) RRC signalling traffic
  - ❑ derived from K_{eNB} and two additional parameters
- K_{UPenc} is a key used to encrypt user plane (UP) traffic
  - ❑ derived from K_{eNB} and two additional parameters
- K_{UPenc} is a key used to protect the integrity of a certain type of UP traffic
  - ❑ details omitted



Cryptographic Key Separation

- One purpose of the complex key hierarchy is to provide key separation
  - i.e., each key is used in a single unique context for cryptographic protection of either user traffic or signalling traffic
- Also, because all keys used for such protection are leaves in the hierarchy, it is infeasible to derive a key used in one protection context from another key (or set of keys) used in other contexts
  - The intention is that attackers cannot find out any keys used in one context from keys used in any other context
- However, note that cryptographic key separation does not help if there is a leakage of higher layer keys, e.g., because somebody has been able to get access to keys stored in MME

Key Renewal

- Another benefit of the complex key hierarchy is that keys can be renewed without affecting all other keys
- When one key is changed, only the keys that are dependent on it have to be changed; the others may remain the same
- E.g., K_{eNB} can be re-derived without changing K_{ASME} in the process
- As a consequence of changing K_{eNB}, all keys derived from K_{eNB} (e.g., K_{RRCenc} and K_{RRCint}) are changed as well
- Reasons why renewing keys is useful:
  - recall: it is good cryptographic practice to periodically change keys: an attacker who is trying to guess the key needs to start all over again when key is changed
  - another reason follows from a generic security principle: we should minimize the need to distribute the same secret to many entities
    - in the case of K_{eNB}, it is renewed whenever it is derived for a new eNB, thus preventing two eNBs from using the same key

Protection for Signalling and User Data

Security Algorithm Negotiation

- Before the communication can be protected, UE and network need to agree on what security algorithms to use
- EPS supports multiple algorithms and includes two mandatory sets of security algorithms:
  - 128-EEA1 and 128-EIA1 based on the stream cipher SNOW 3G, and 128-EEA2 and 128-EIA2 based on Advanced Encryption Standard (AES), which all implementations of UEs, eNBs and MMEs need to support
- A third set of security algorithms is optional for implementation
  - 128-EEA3 and 128-EIA3 based on the stream cipher ZUC
- EPS can be extended to support more algorithms in the future
- Algorithms are negotiated separately between UE and eNBs (AS level) and between UE and core network, i.e., MME (NAS level)
- The network selects the algorithms based on the UE security capabilities and the configured list of allowed security algorithms for the network entities (eNBs and MMEs)
- The UE provides its security capabilities to the network during the attachment procedure

Security Algorithm Negotiation (contd.)

- Security capabilities that UE provided to network are repeated in integrity-protected response message from network
- Reason:
  - to protect against bidding down attacks, where the attacker modifies the message carrying the UE security capabilities from the UE to the network
  - if UE detects a mismatch between the security capabilities it sent to the network and the ones it received from the network, the UE cancels the attach procedure
- MME is responsible for selecting the NAS-level algorithms, and the eNB is responsible for selecting the AS-level algorithms, including the user plane algorithm
- Operator configures MMEs with a list of allowed algorithms for NAS signalling in priority order:
  - one list for the integrity algorithms and one for the ciphering algorithms
- During the security setup, MME chooses one NAS ciphering and one NAS integrity algorithm based on the configured lists and signals the decision to UE

Security Algorithm Negotiation (contd.)

- Similar to MME configuration, each eNB is also configured with a list of allowed algorithms in priority order:
  - one list for integrity protection algorithms and another for ciphering algorithms
- Thus, the eNB decides what algorithms are used with the UE for AS signalling protection and for AS user plane data protection
- MME sends K_{eNB} key to eNB, from which the actual protection keys are derived

NAS Signalling, AS Signalling, and User Data Protection

- NAS and AS signalling messages are encrypted, and provided with message integrity and replay protection
- User plane data is encrypted, but no message integrity or replay protection provided
- Relevant keys from the key hierarchy discussed earlier used for above purposes
- We omit the details