LTE Security

Encryption and Integrity Protection in LTE

LTE Security: Key Concepts

Authentication

- The LTE Network verifies the UE's identity by challenging the UT use the keys and report a result.
- The network checks the result against the expected result

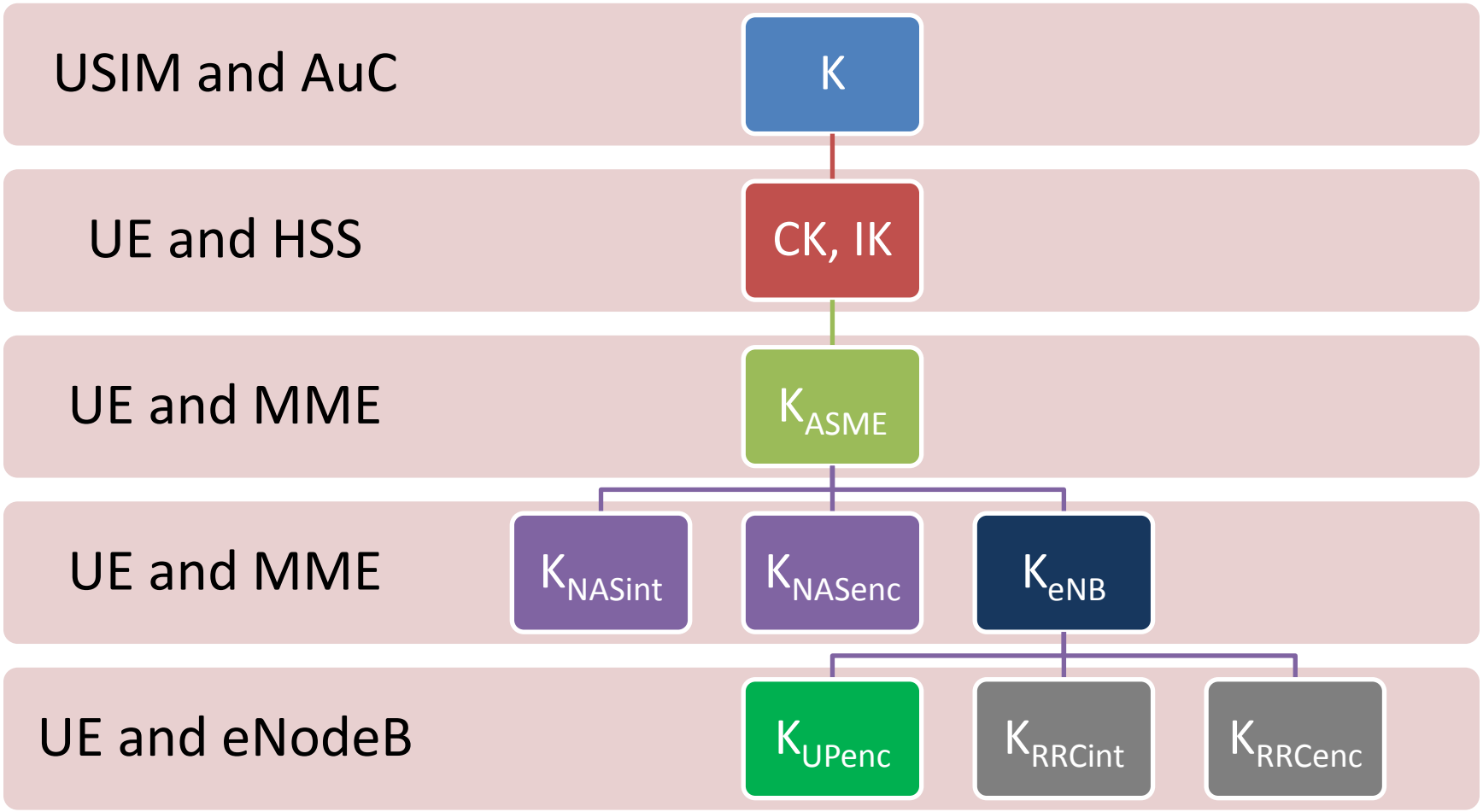
Integrity

- Signaling message receiver verifies that the received message is exactly the message that the transmitter sent
- This is done using an integrity checksum
- Guards against "man in the middle" attacks where the senders messages and intercepted by a hacker and a modified message is relayed to the receiver

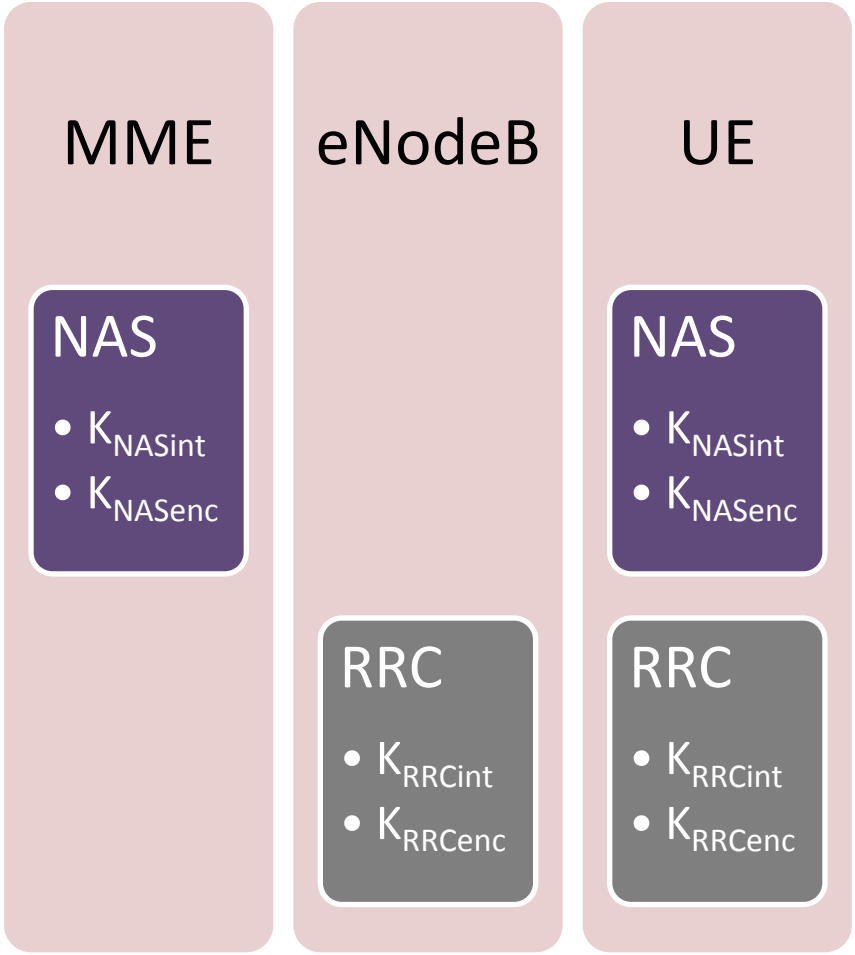
Encryption

- The sender encrypts the data with a secret key that is only known to the receiver
- Only the receiver is able to decode the message
- Guards against hackers listening in on the data

LTE Security Key Hierarchy

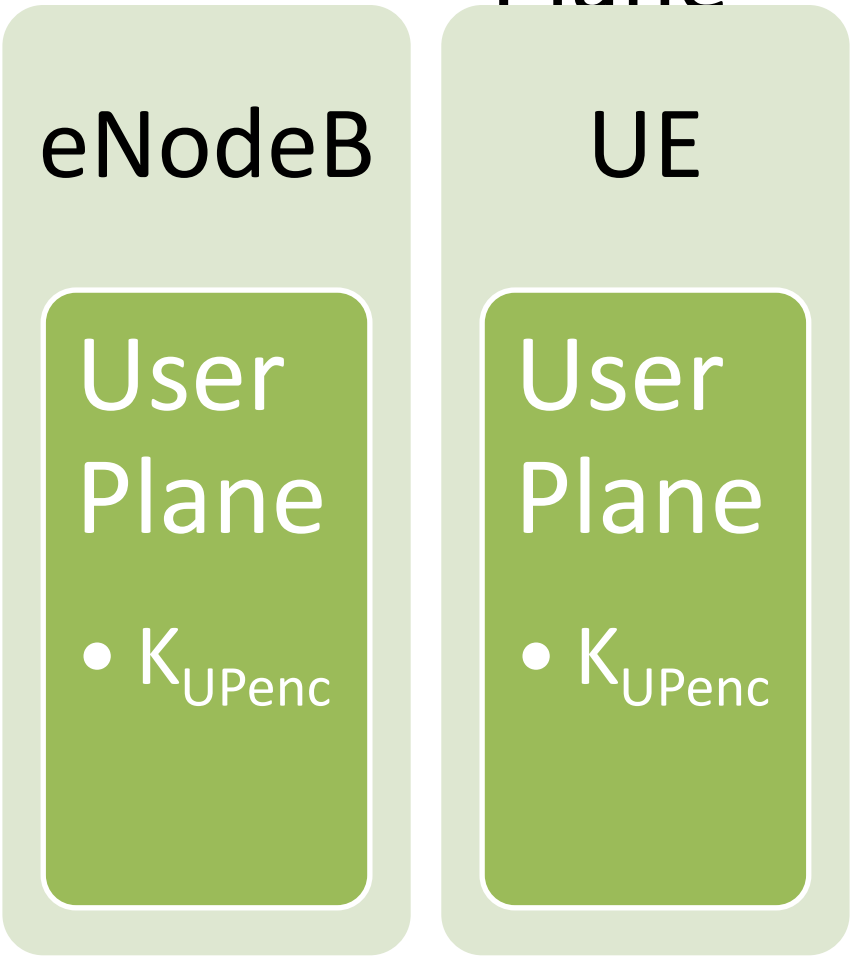


Encryption and Integrity Protection in the LTE Control Plan



- LTE supports two levels on security on the control plane
  - The NAS traffic between the MME and the UE is protected with NAS level keys
  - The RRC connection traffic between the MME and the UE is protected with RRC level keys
- This means that the NAS traffic is being protected with NAS as well as RRC level security

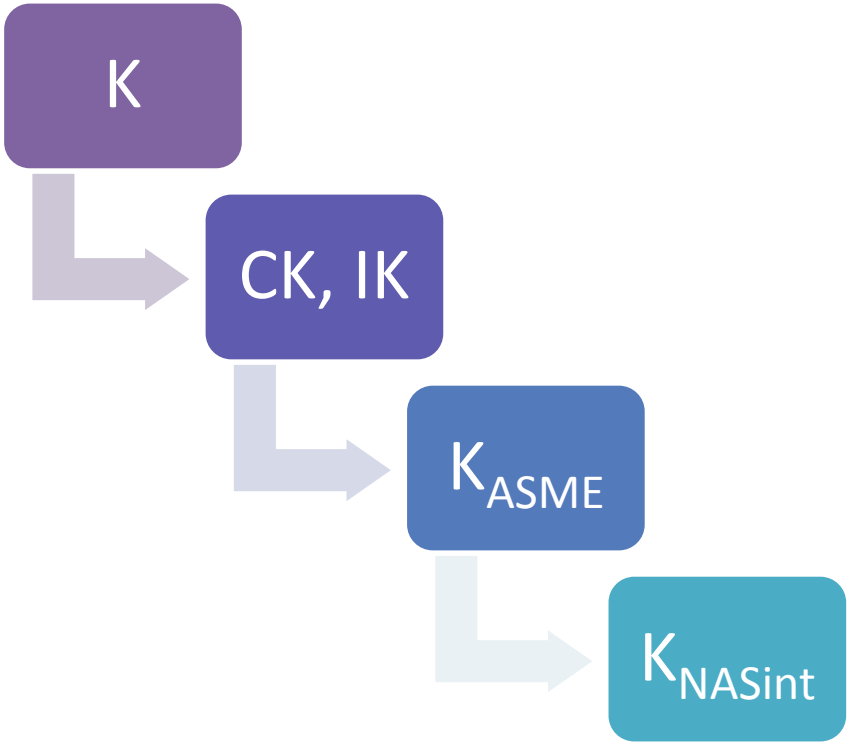
Encryption and Integrity Protection in the LTE User Plane



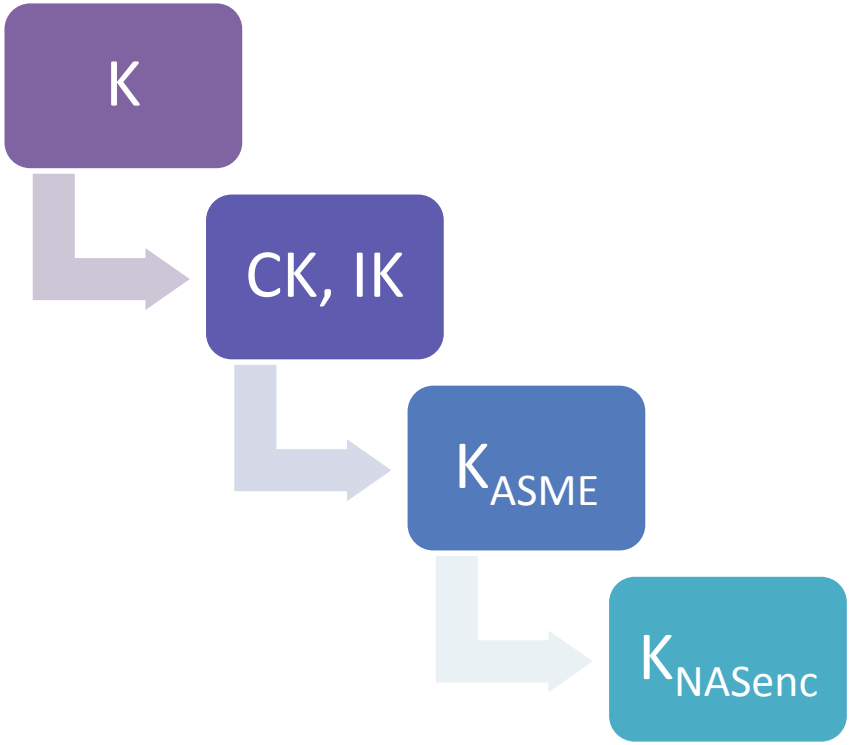
- User plane data is encrypted with the K_{UPenc} key

LTE NAS Key Derivation at the MME and UE

K_{NASint}: Integrity protection key for NAS signaling messages

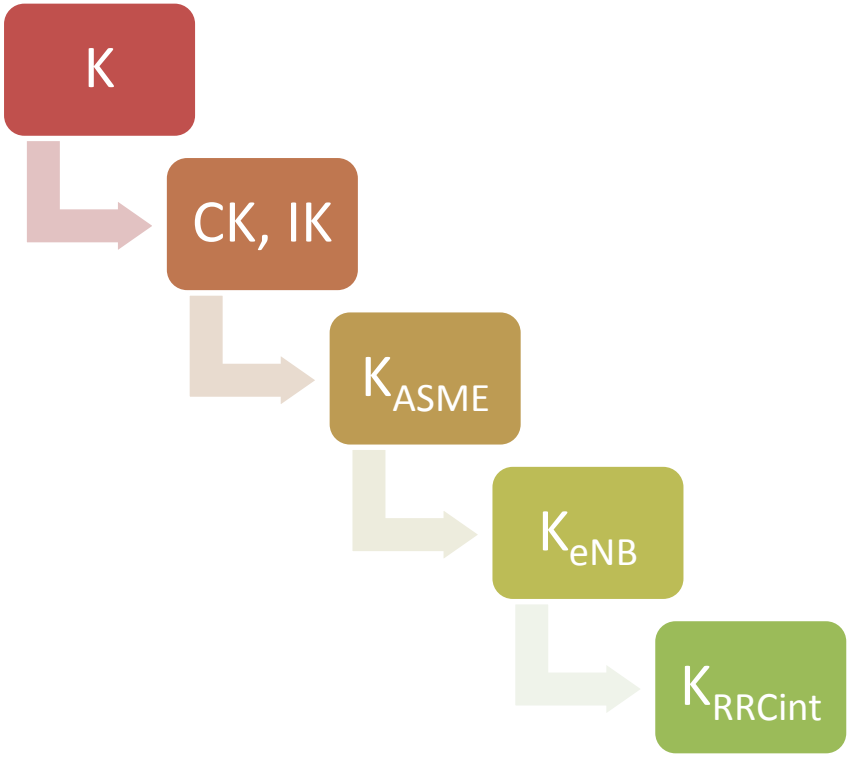


K_{NASenc}: Encryption key for NAS signaling messages

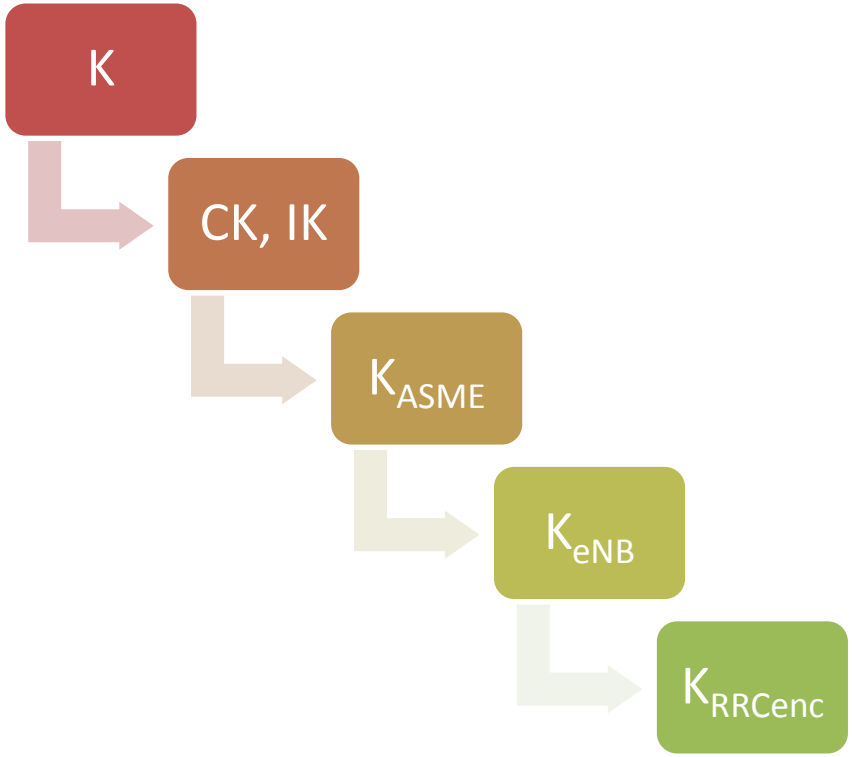


LTE RRC Key Derivation at the eNodeB and UE

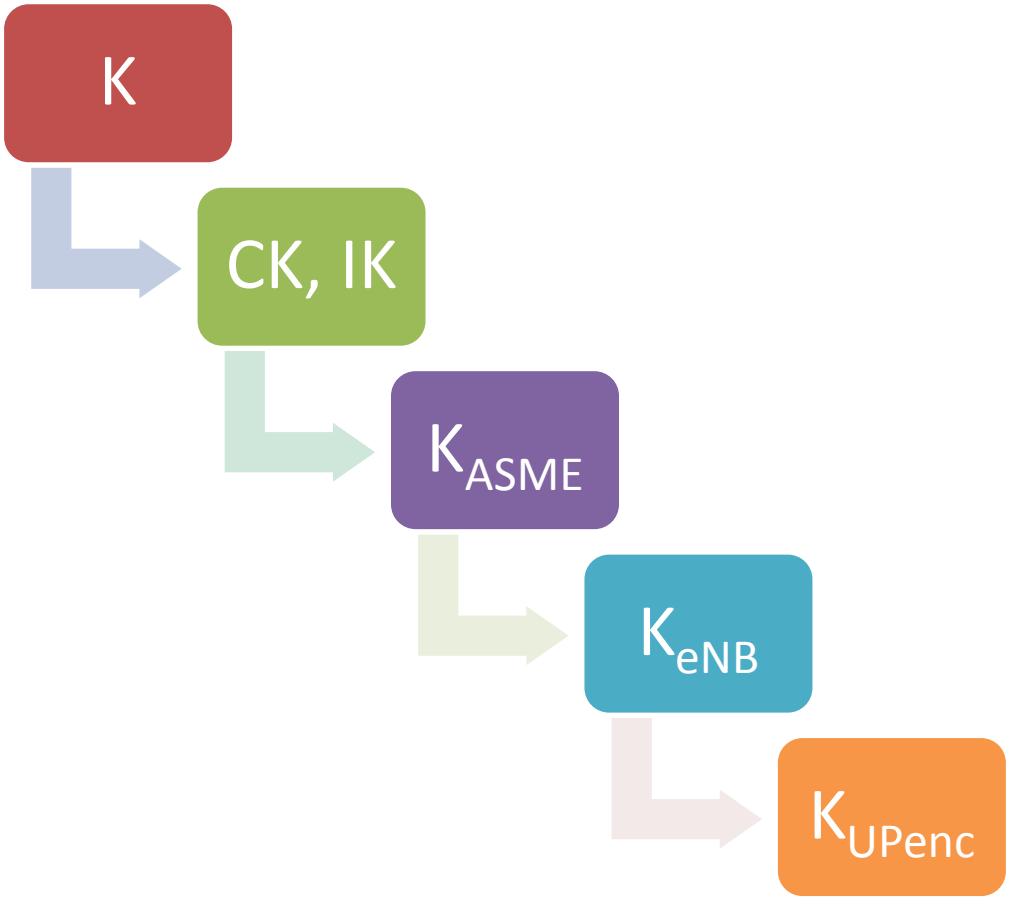
K_{RRCint}: Integrity protection key for RRC signaling messages



K_{RRCenc}: Encryption key for RRC signaling messages



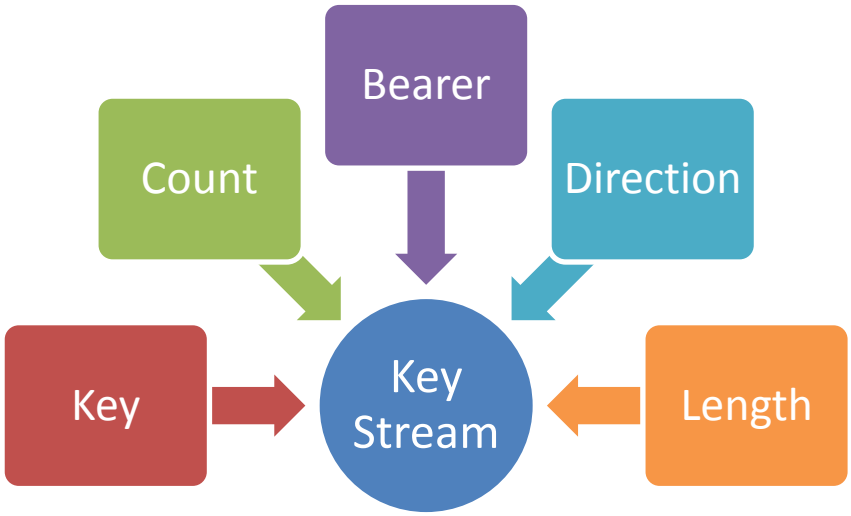
LTE User Plane Key Derivation at the eNodeB and UE



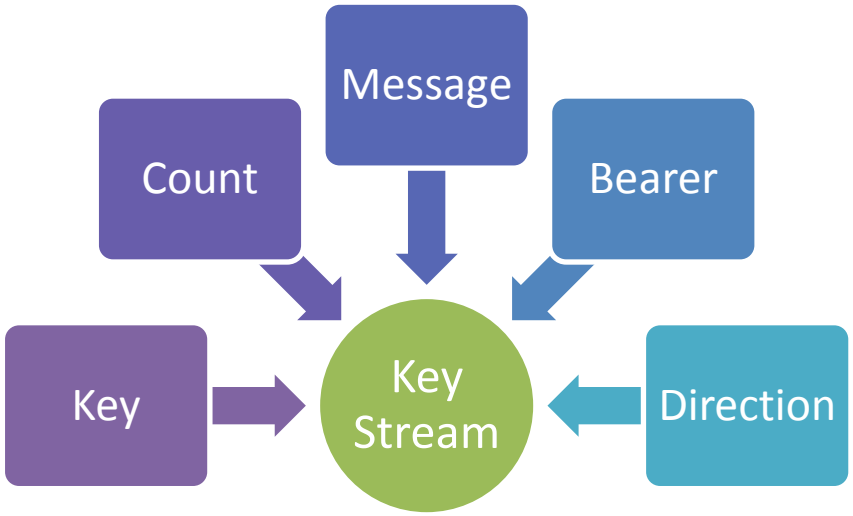
- K_{UPenc}: User plane encryption key

Key Stream Computation

Ciphering



Integrity Protection



3GPP Security Specifications

LTE Security

- 33.401: System Architecture Evolution (SAE); Security architecture
- 33.402: System Architecture Evolution (SAE); Security aspects of non-3GPP

Lawful Interception

- 33.106: Lawful interception requirements
- 33.107: Lawful interception architecture and functions
- 33.108: Handover interface for Lawful Interception

Key Derivation Function

- 33.220: GAA: Generic Bootstrapping Architecture (GBA)

Backhaul Security

- 33.310: Network Domain Security (NDS); Authentication Framework (AF)

Relay Node Security

- 33.816: Feasibility study on LTE relay node security (also 33.401)

Home (e) Node B Security

- 33.320: Home (evolved) Node B Security

Thank You

EventHelix.com
- telecommunication design
- systems engineering
- real-time and embedded systems

Thank you for visiting EventHelix.com. The following links provide more information about telecom design tools and techniques:

Links	Description
EventStudio System Designer	Sequence diagram based systems engineering tool.
VisualEther Protocol Analyzer	Wireshark based visual protocol analysis and system design reverse engineering tool.
Telecom Call Flows	GSM, SIP, H.323, ISUP, LTE and IMS call flows.
TCP/IP Sequence Diagrams	TCP/IP explained with sequence diagrams.
Telecom • Networking • Software	Real-time and embedded systems, call flows and object oriented design articles.