Module 5
Wireless Network Security

Security in GSM; UMTS Security; Bluetooth Security; WEP; WPA2.

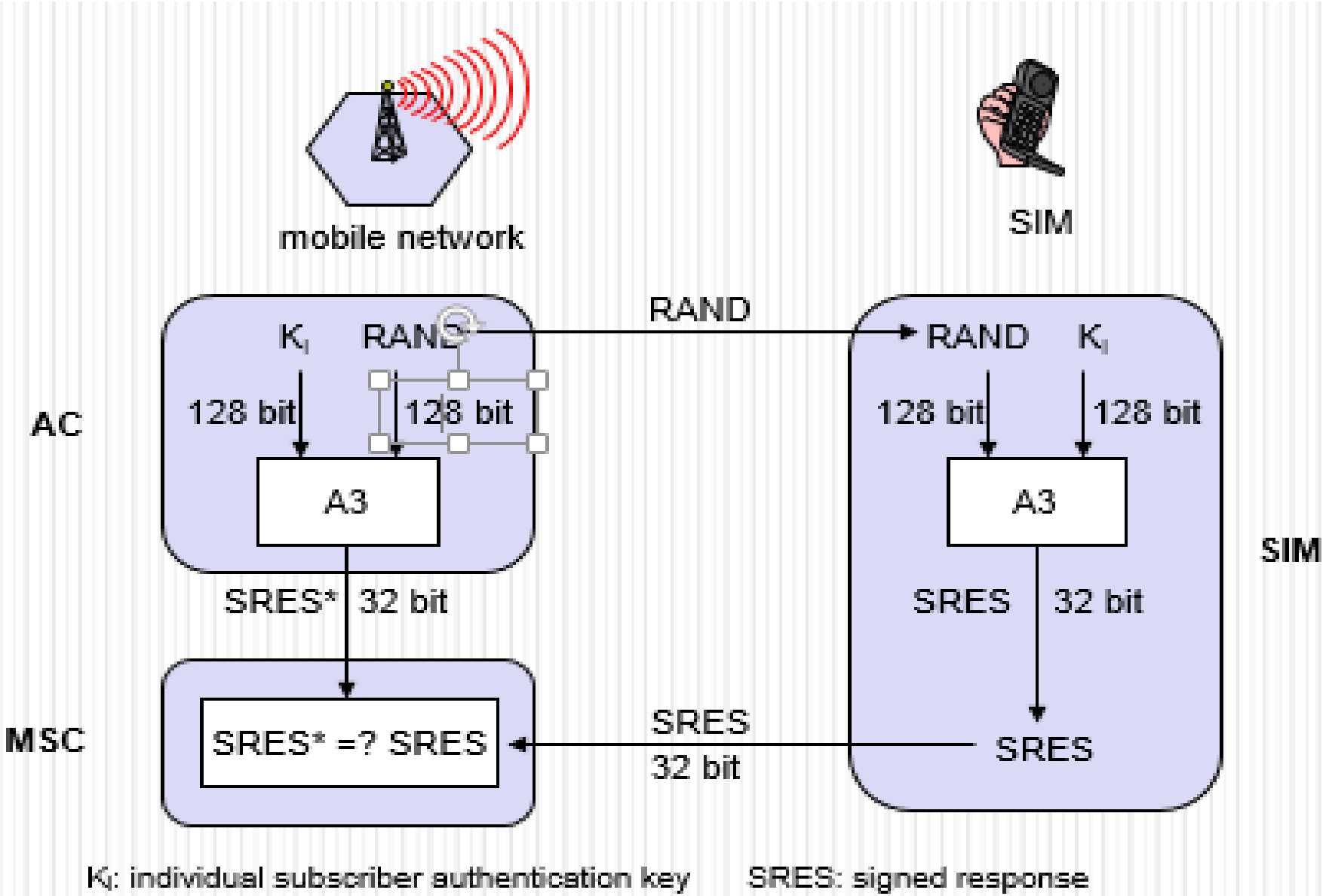
Self-learning Topics :- Study of Wireless Security Tools.

Security in GSM

- Security is implemented **to prevent unauthorized use of the mobile** subscriber number over the air.
- The voice conversations need to encrypted using secrecy algorithm in GSM.
- Authentication is done with the help of a pre- defined protocol that is used to compare IMSI of MS reliably.
- A unique secret key (128 bits) is stored in SIM card.
- It uses 3 algorithms

1. **A3** – for Authentication (verify users password within SIM)
2. **A5** – for confidentiality (it scramble coded data)
3. **A8** – generate privacy key that used to encrypt voice or data messages.

GSM - authentication



Ki is the 128-bit Individual Subscriber Authentication Key utilized as a secret key shared between the Mobile Station and the Home Location Register of the subscriber's home network.

RAND is 128-bit random challenge generated by the Home Location Register.

SRES is the 32-bit Signed Response generated by the Mobile Station and the Mobile Services Switching Center.

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism.

Step 1: A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki).

Step 2:Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.

- The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases.
- If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue.
- If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.
- The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

Signalling and Data Confidentiality

Kc is the 64-bit ciphering key used as a Session Key for encryption of the over-the-air channel.

Kc is generated by the Mobile Station from the random challenge presented by the GSM network and the Ki from the SIM utilizing the A8 algorithm.

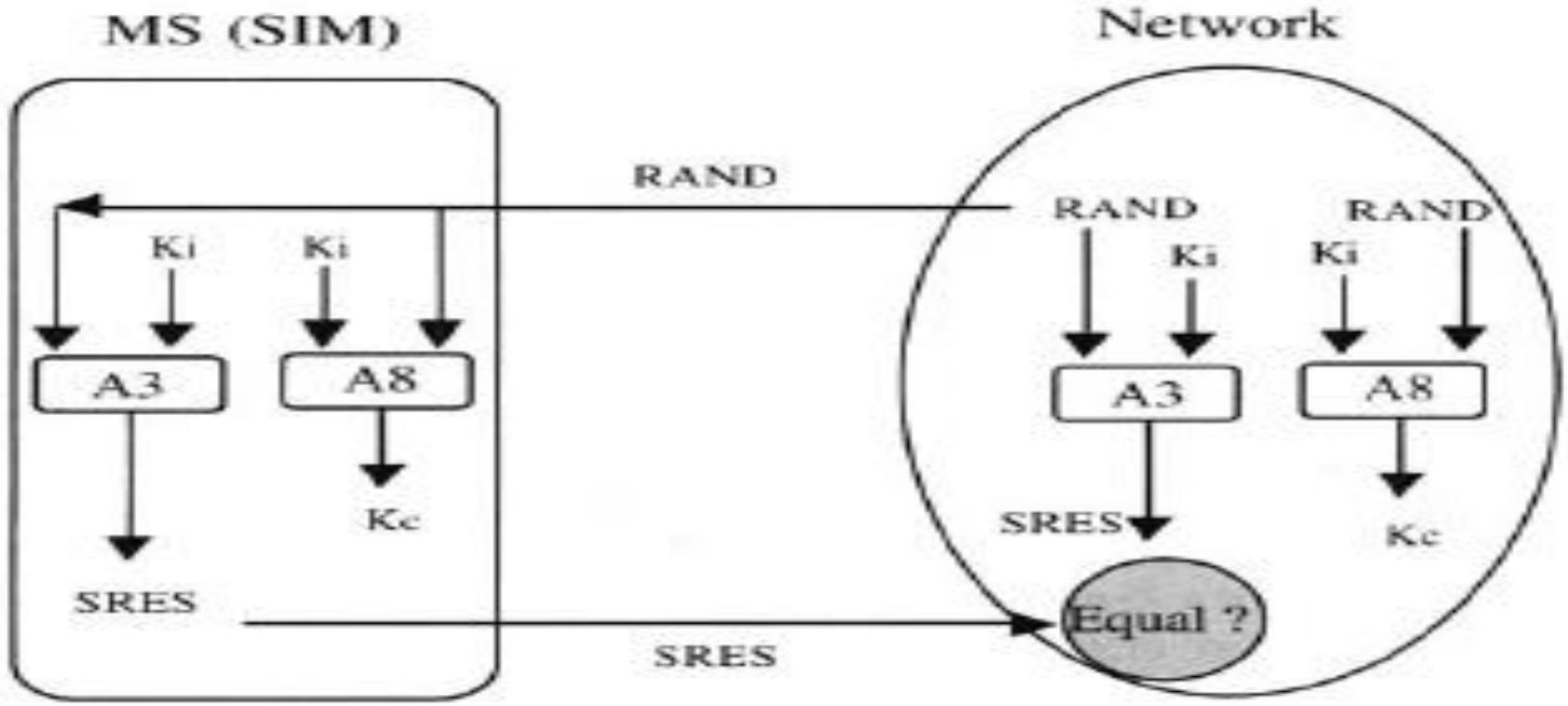
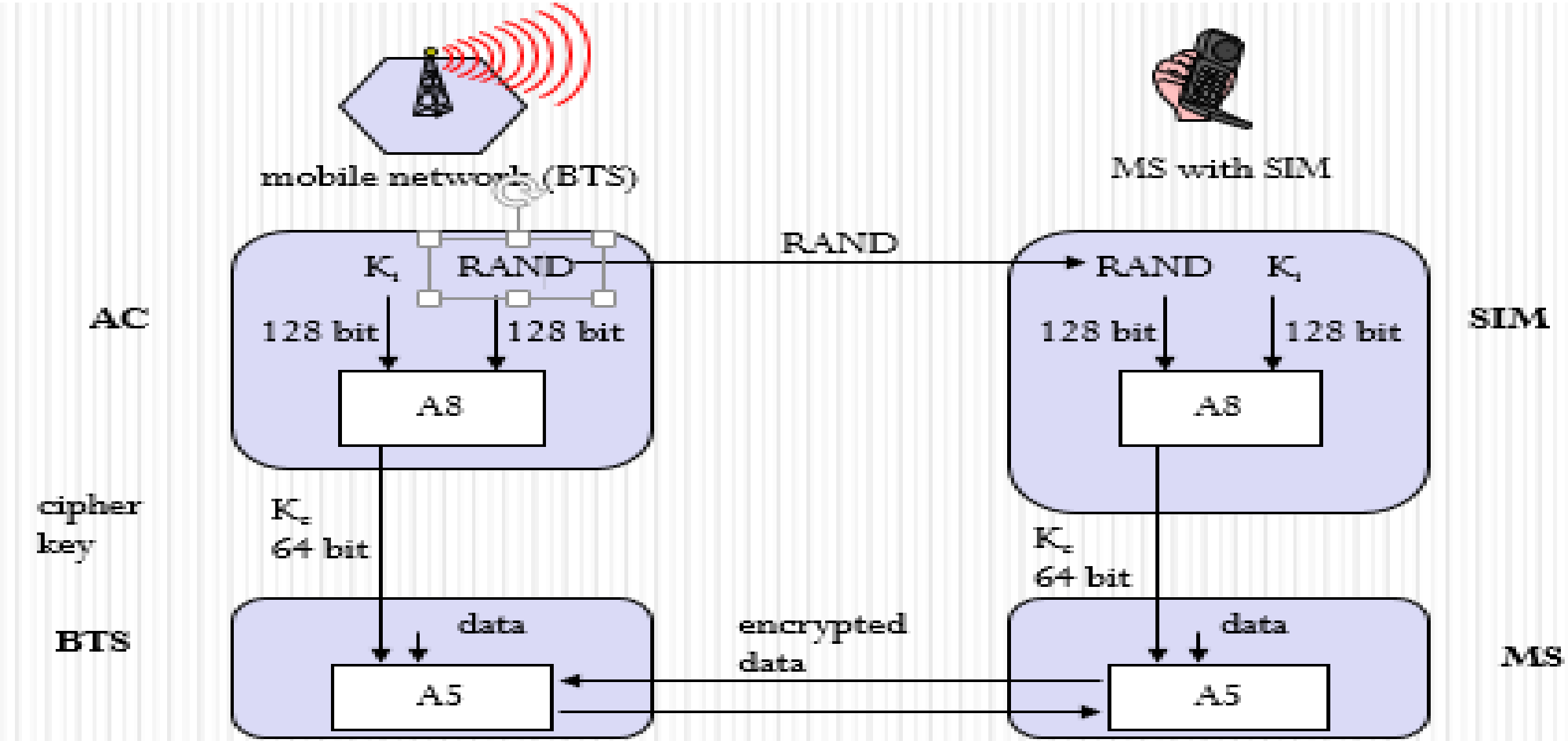


Figure 3.6 General authentication process and ciphering key generation.

- The SIM contains the ciphering key generating algorithm (A8) that is used to produce the 64-bit ciphering key (Kc).
- This key is computed by applying the same random number (RAND) used in the authentication process to ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).

- GSM provides an additional level of security by having a way to change the ciphering key, making the system more resistant to eavesdropping.
- The ciphering key may be changed at regular intervals as required. As in case of the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM.
- Therefore, sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.

GSM - key generation and encryption



- Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5.

- Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).

Subscriber Identity Confidentiality

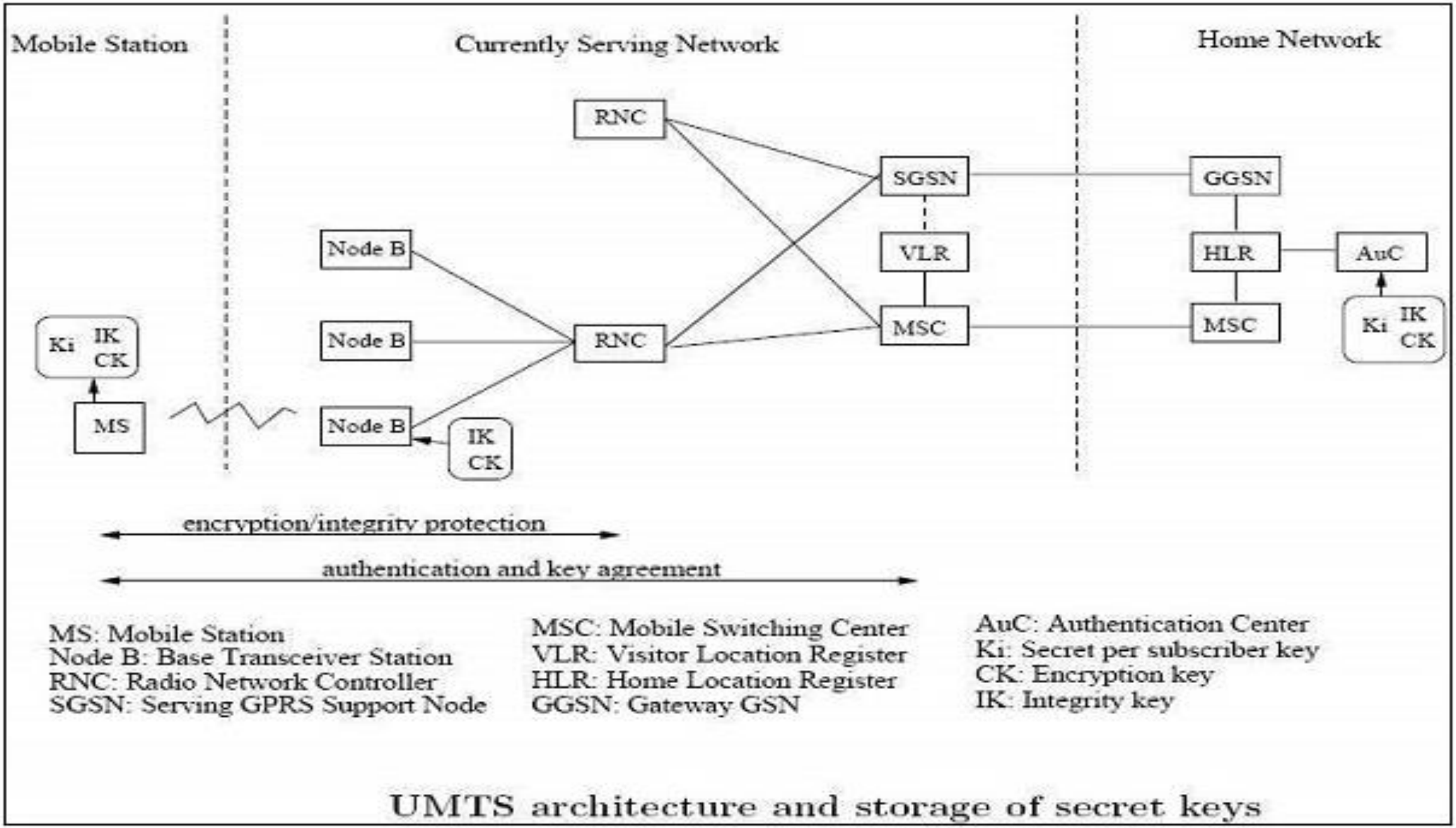
- To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used.
- Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station.
- After the receipt, the mobile station responds.
- The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.

UMTS Security Procedure

- UMTS **Authentication and Key Agreement (AKA)** is a security mechanism used to accomplish the authentication features.

- It is based on a challenge/response authentication protocol which is used for a MS to verify the identity of another mobile subscriber without revealing a secret password shared by the two.

- The key concept is that each mobile subscriber must prove to the other that it knows the password without actually revealing or transmitting such a password.



UMTS architecture and storage of secret keys

Steps of Authentication and Key Agreement procedure:

- **Step 1:** Visited network's VLR/SGSN requests a set of AVs [authentication vectors] from the HLR/AuC in the mobile subscriber's home network.
- **Step 2.** HLR/AuC computes an array of AVs. This is done by means of the 'authentication algorithms and the mobile subscriber's private secret key K, which is stored only in the home network's HLR/ AuC and the user Identity Module (USIM) in the mobile subscriber's mobile subscriber.
- **Step 3.** Home network's HLR/ AuC responds by sending *n* authentication vectors back to the visited network's VLR/SGSN.
- **Step 4.** Visited network's VLR/SGSN chooses one AV and challenges the mobile subscriber's USIM by sending the RAND and AUTN fields in the vector to it.
- **Step 5**. The mobile subscriber's USIM processes the AUTN.

Steps of Authentication and Key Agreement procedure: (cont)

- With the aid of the private secret key K, the mobile subscriber is able to verify that the received challenge data could only have been constructed by someone who had access to the same secret key K.
- The USIM will also verify that the AV has not expired by checking its Sequence Number (SEQ) field
- Provided that the network can be authenticated and that the AV is still valid, the USIM proceeds to generate a Confidentiality Key (CK), an Integrity Key (IK) and a Response for the network (RES).
- **Step** 6. The mobile subscriber responds with RES to the visited network.
- **Step** 7. Visited network's VLR/SGSN verifies that response is correct by comparing the Expected Response (XRES) from the current AV with the Response (RES) received from the mobile subscriber's USIM

UMTS Subscriber to UMTS Network

Both the network and the mobile station supports all the security mechanisms of UMTS.

Authentication and Key agreement is as follows –

- The MSand the BS establish a radio resource control connection (RRC connection).
- During the establishment of the connection the MS sends its security capabilities to the BS. Security features include UMTS integrity and encryption algorithms supported and possibly GSM encryption capabilities as well.
- The MS sends its temporary identity TMSI current on the network.

- If the network cannot solve the TMSI, he asks the MS to send its permanent identity and the mobile stations responding to the request with the IMSI.

- The visited network requests authentication of the home network of the mobile station data.
- The home network returns a random challenge RAND, the corresponding authentication token AUTN, authentication
- Response XRES, integrity key IK and the encryption key CK.
- The visited network sends RAND authentication challenge and authentication token AUTN to the mobile Station.
- The MS checks AUTN and calculates the authentication response.
- If AUTN is corrected. The mobile station sends its authentication response RES to the visited network. Else Mobile station ignores the message.

- Visiting network checks if RES = XRES and decide which security algorithms radio subsystem is allowed to use.

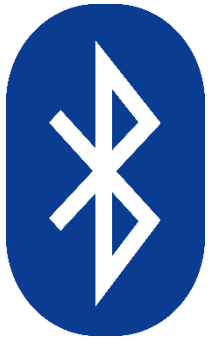
- The visited network sends algorithms admitted to the radio subsystem.
- The radio access network decides permit (s) algorithms to use.
- The radio access network informs the mobile station of their choice in the security mode command message.
- The message also includes the network security features received from the mobile station in step 1.
- This message is integrity protected with the integrity key IK.
- The mobile station confirms the protection of the integrity and verify the accuracy of the safety functions.

UMTS Subscriber to GSM Base Station

- The mobile unit (subscriber UMTS) supports both USIM and SIM application.
- The base station system uses GSM while the VLR / MSC technology components are respectively the UMTS SGSN.
- The mobile station and the core network both support all security mechanisms of UMTS.
- However, the base station system GSM (BSS) does not support the protection of the integrity and uses the GSM encryption algorithms.

- The first eight steps of the authentication protocol are performed as in the classical case. GSM BSS simply forwards the UMTS authentication traffic.

- The MSC / SGSN decides which GSM encryption algorithms are allowed and calculates the key GSM Kc UMTS keys IK, CK.
- The MSC / SGSN advises the GSM BSS authorized algorithms and transmits the GSM cipher key Kc.
- GSM BSS decide which encryption algorithms allowed to use based encryption capabilities of the mobile station.
- GSM BSS sends the GSM cipher mode command to the station.



Bluetooth Security

Introduction

- Bluetooth is a wireless radio specification, design to replace cable as the medium for data and voice signal between electronics device.
- Bluetooth design on small size, low power consumption and low cost.
- Mostly it uses in Laptop computers, cellular phones, PDA's, Headset, keyboards, as well as in digital camera and other consumer electronics devices.

- Uses the radio range of 2.45 GHz
- Theoretical maximum bandwidth is 1 Mb/s
- Several Bluetooth devices can form an ad hoc network called a "piconet"
  - In a piconet one device acts as a master (sets frequency hopping behavior) and the others as slaves.
  - Example: A conference room with many laptops wishing to communicate with each other.
    - Range < 10m.
    - Piconets: 1 master and up to 7 slaves.

Bluetooth Security

- ***Authentication:*** Verifies the identification of the devices that are communicating in the channel.
- ***Confidentiality:*** Protecting the data from the attacker by allowing only authorized users to access the data.
- ***Authorization:*** Only authorized users have control over the resources.

Security mode of bluetooth

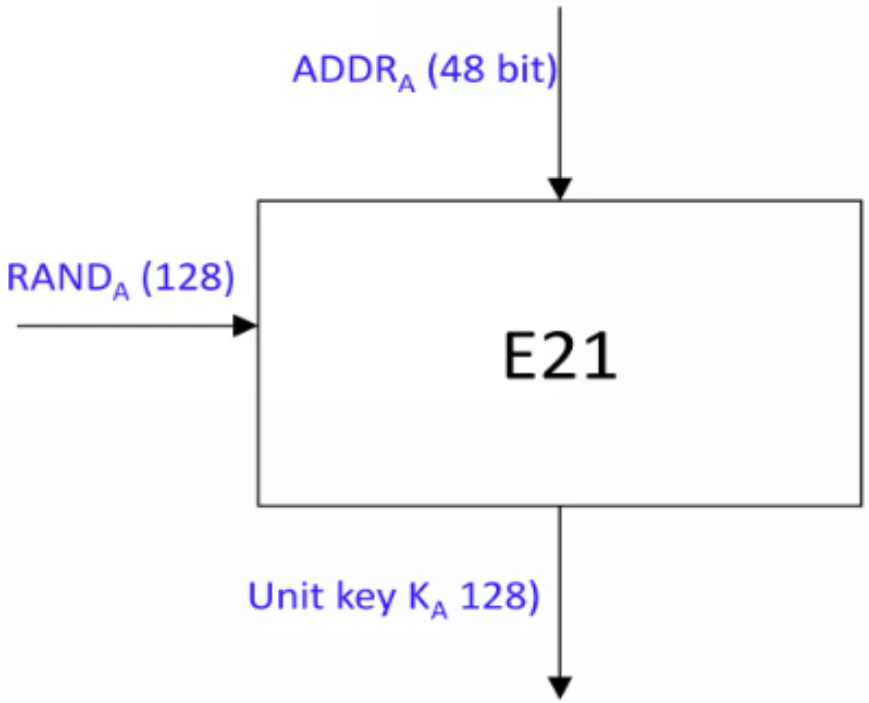
- ***Security Mode 1:*** No-Secure Mode, (There won't be any authentication or encryption in this mode. Bluetooth device can easily be connected with the other devices).
- ***Security Mode 2:*** Service level security mode, (The management of the access control and interfaces with other protocols and device users is handled by the centralized security manager.)
- ***Security Mode 3:*** Link-level security mode, (This is a built in security mechanism that offers the authentication (unidirectional or mutual) and encryption based on the secret key shared by the pair of devices).

Protocols in Bluetooth

1. Generation of unit key.
2. Generation of initialization key.
3. Generation Combination Key.
4. Authentication.
5. Generation of encryption key.
6. Generation of key stream.
7. Encryption of data.

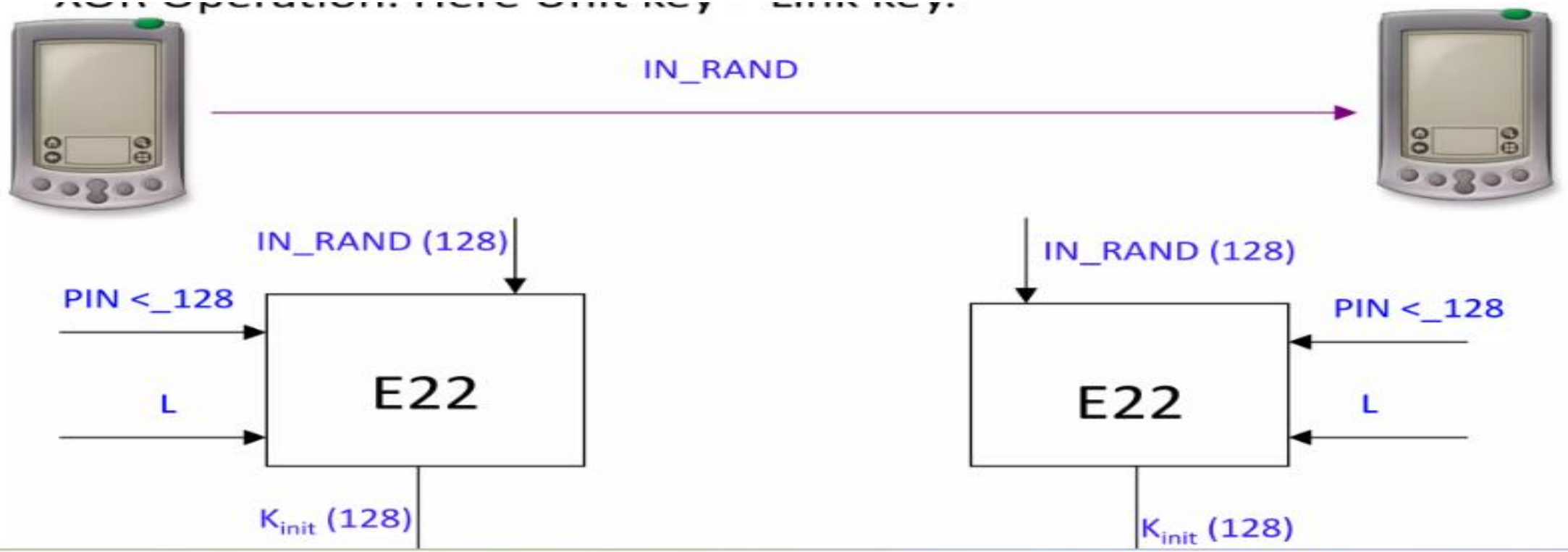
1. Generation unit key

- It is a Semi permanent Key.
- Bluetooth Device Operated for the First time.



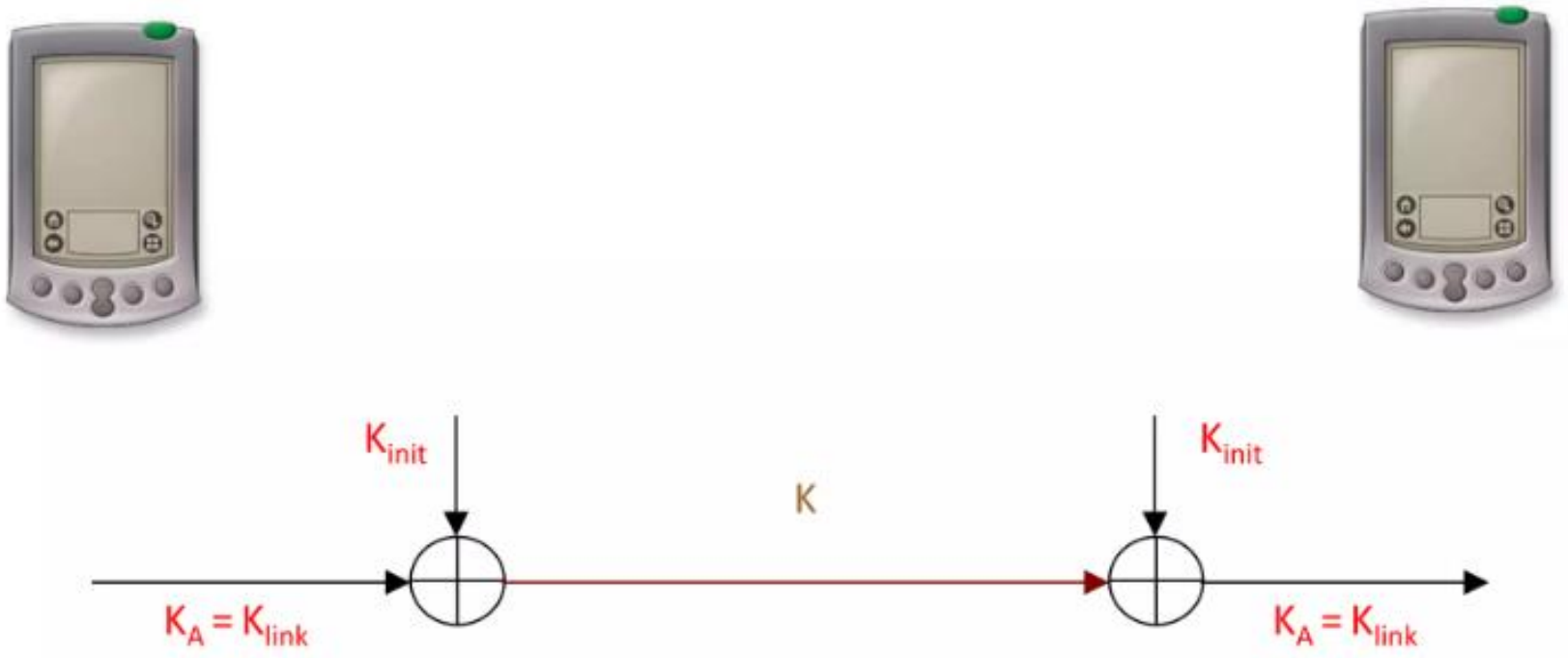
2. Generation initialization key

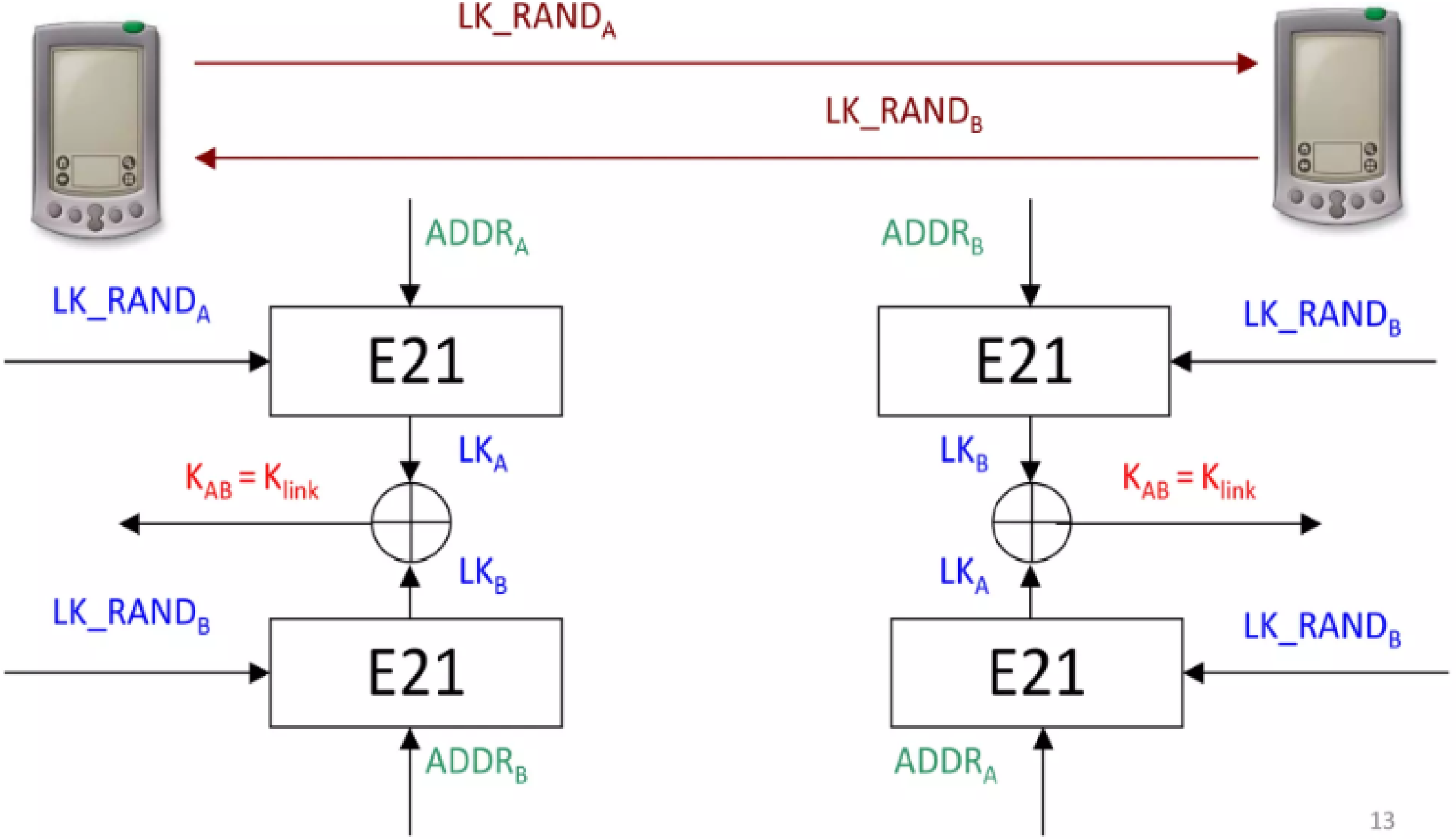
- it's a temporarily Key.
- Communication between two Device (P'=PIN + BD_ADDR).
- XOR Operation. Here Unit key = Link key.



Generation Combination key

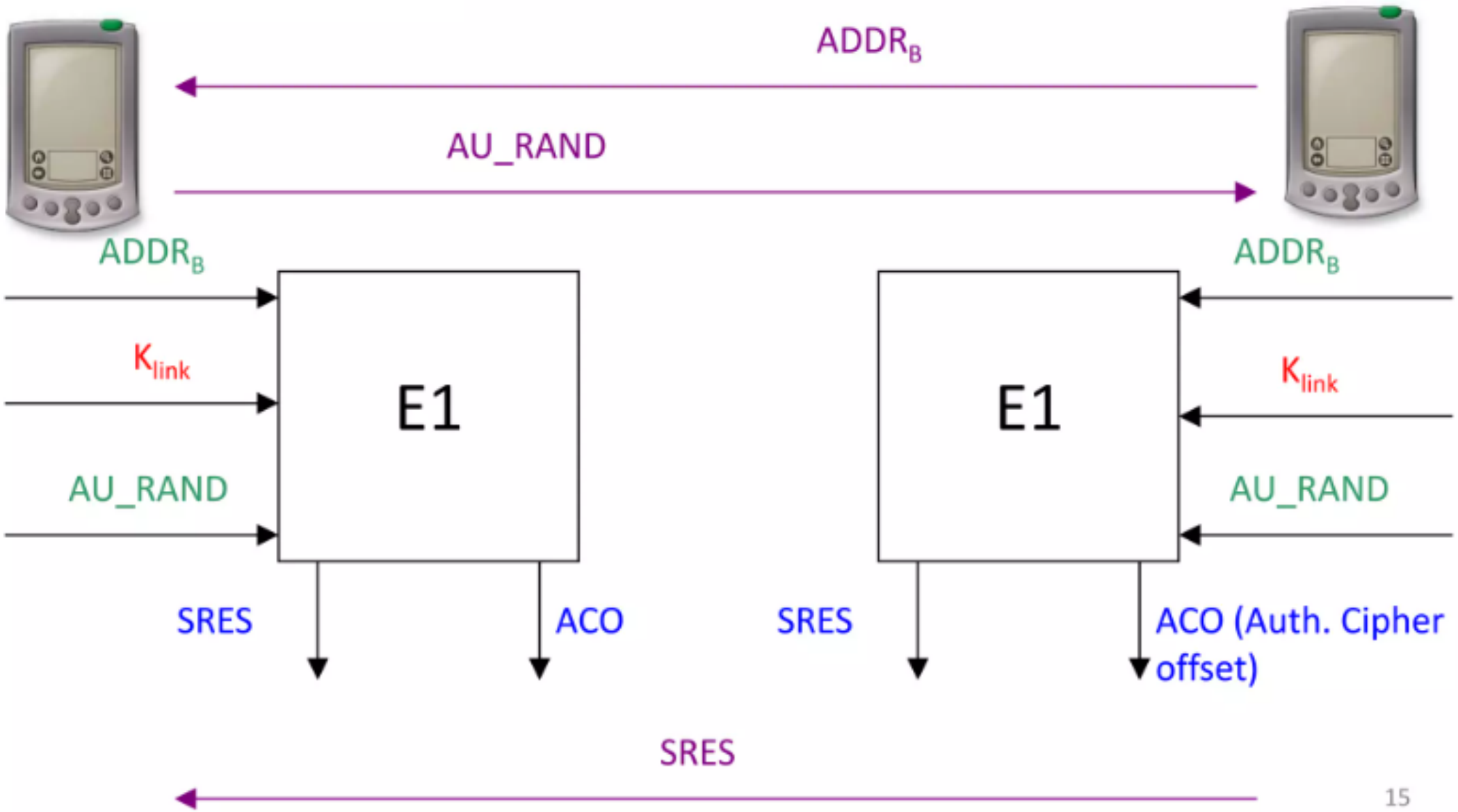
- The Combination key is the combination of two generated in a device A and B, Respectively.
- Each device generates a random no. LK_RAND_A and LK_RAND_B.
- Then utilizing E_{21} they generate LK_K_A and LK_K_B respectively.
- $LK\_K=E_{21}$ (LK_RAND, BD_ADDR)
- LK_K_A and LK_K_B are XORed with the current link key.
- Device A calculate LK_RAND_A and Device B calculate LK_RAND_B.
- K_{AB} is calculated simply by XORing LK_K_A and LK_K_B.

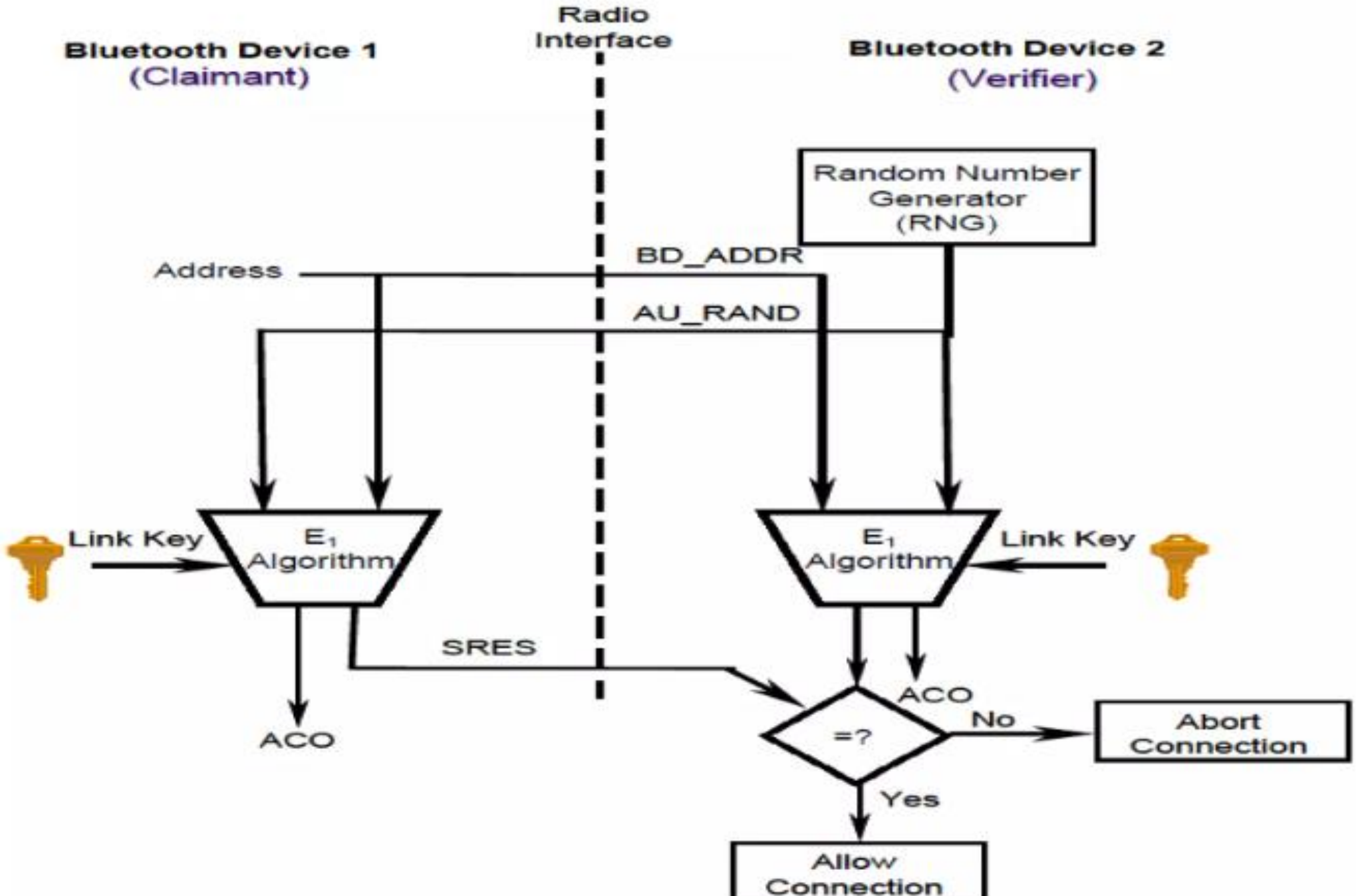

K_{init}
K_{init}
K
$K_A = K_{link}$
$K_A = K_{link}$


LK_RAND_A
LK_RAND_B
ADDR_A
ADDR_B
LK_RAND_A
LK_RAND_B
E21
E21
LK_A
LK_B
K_AB = K_link
K_AB = K_link
LK_B
LK_A
LK_RAND_B
LK_RAND_B
E21
E21
ADDR_B
ADDR_A

Authentication

- Both device A & B use the common link key for authentication, they don't need generate a new $K_{init.}$ During each authentication a new AU_RAND_A is issued.
- Authentication uses a challenge-response scheme in which a claimant's Knowledge of a secret key is checked through a 2-step protocol using symmetric secret key.
- It return SRES to the verifier.
- When the authentication attempt fails, for each subsequent authentication failure with the same Bluetooth Device address, the waiting interval is increased exponentially.


ADDR_B
AU_RAND
ADDR_B
ADDR_B
K_link
E1
AU_RAND
K_link
E1
AU_RAND
SRES
ACO
SRES
ACO (Auth. Cipher offset)
SRES

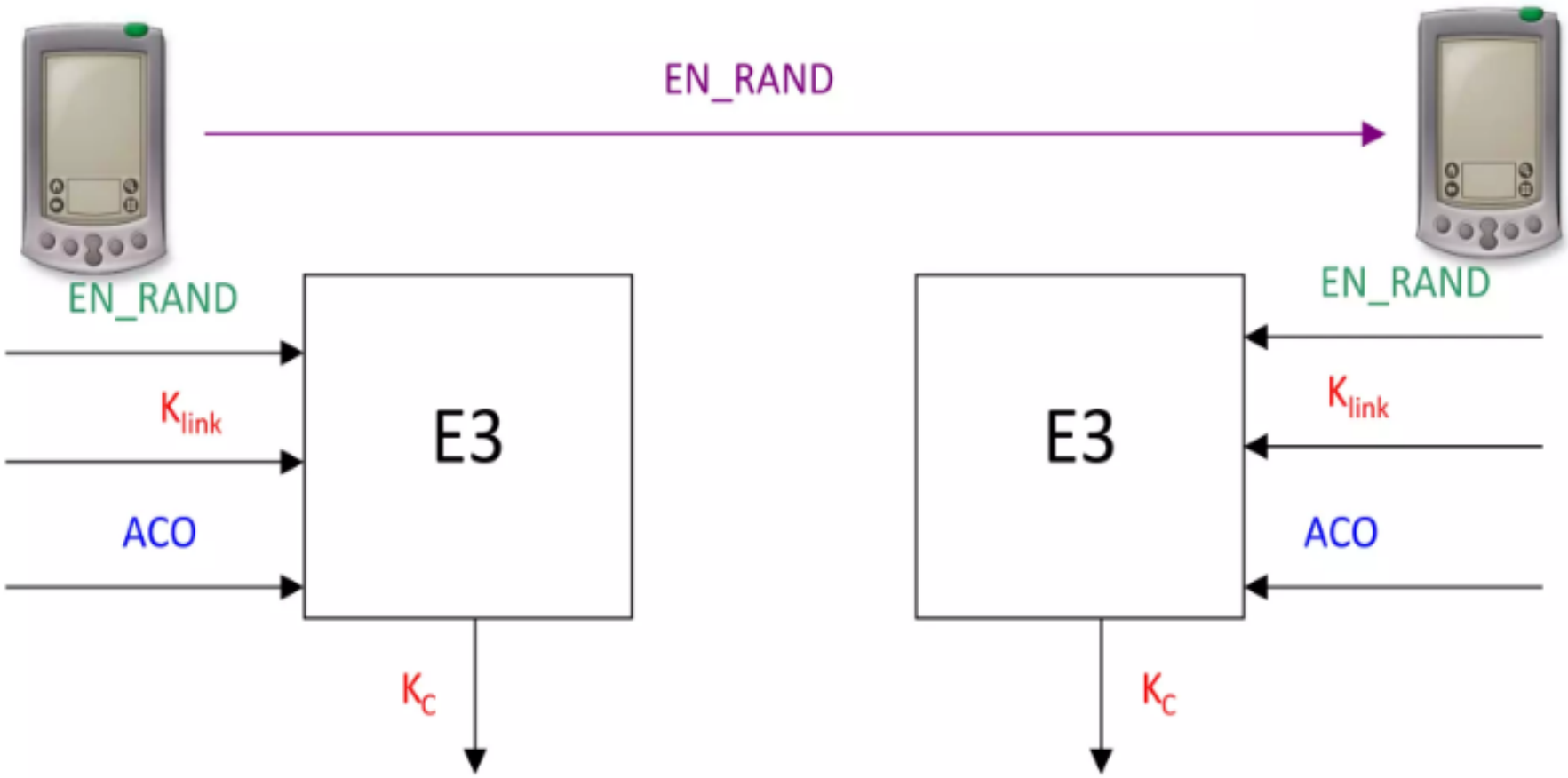

Bluetooth Device 1
(Claimant)
Radio
Interface
Bluetooth Device 2
(Verifier)
Random Number
Generator
(RNG)
BD_ADDR
Address
AU_RAND
Link Key
E1
Algorithm
E1
Algorithm
Link Key
SRES
ACO
ACO
=?
No
Abort
Connection
Yes
Allow
Connection

Authentication Summary

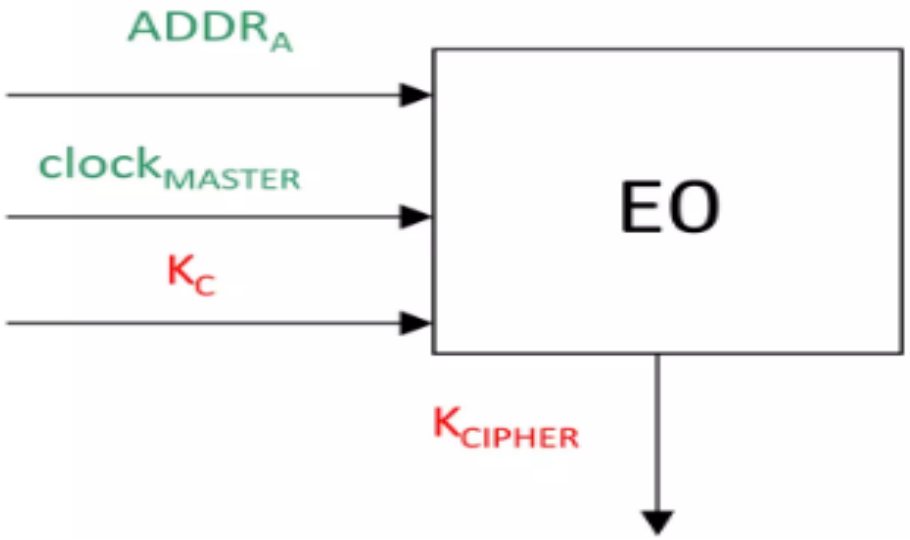
Authentication Process

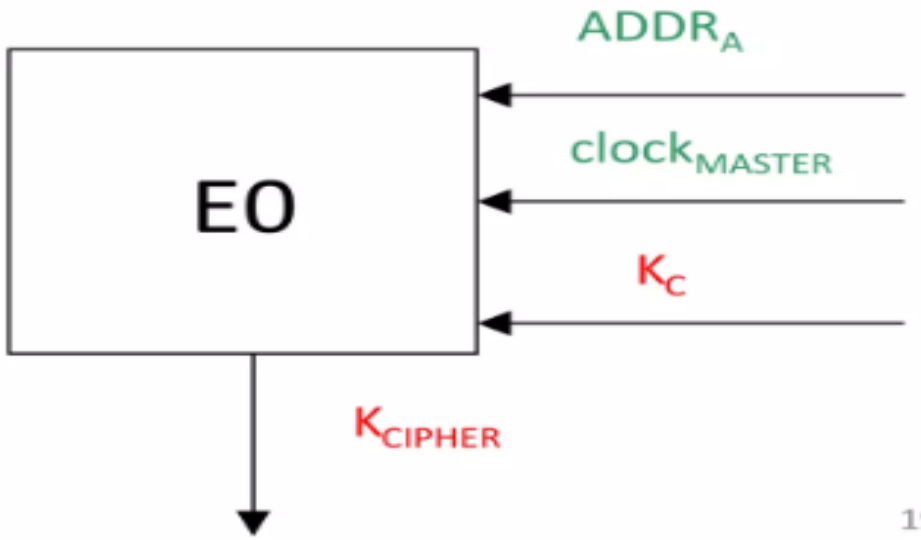
Parameter	Length	Secrecy parameter
Device Address	48 Bits	Public
Random Challenge	128 Bits	Public
Authentication (SRES) Response	32 Bits	Public
Link Key	128 Bits	Secret

Generation of encryption key

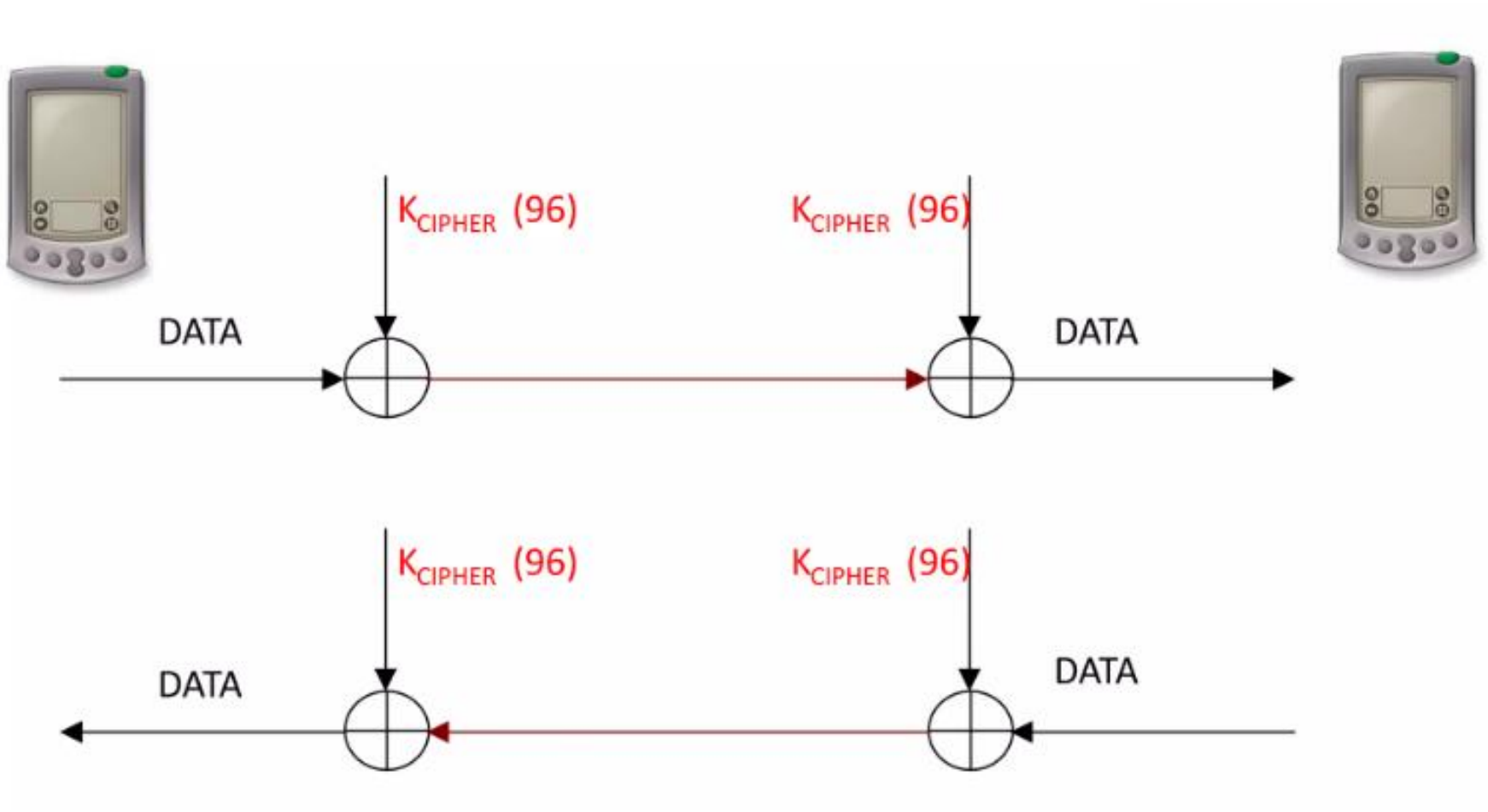


Generation key stream





7. Encryption of data



Security weakness

- Problems with E0
- Unit key
- PIN
- Problems with E1
- Location privacy
- Denial of service attacks

Summary

- Bluetooth technology allows for replacing many proprietary cables that connect one device to another with one universal short range radio link.

- Bluetooth radio technology provides a universal bridge to existing data networks, a peripheral interface, and a mechanism to form small, private ad hoc groupings of connected devices away from fixed network infrastructures.

- The Bluetooth technology has a number of advantages including minimal hardware dimensions, low cost of components, and low power consumption.
- These advantages make it possible to introduce Bluetooth in many types of devices at a low cost.
- The 720 kbps data capability provided by Bluetooth can be used for cable replacement and several other applications, such as LAN.