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

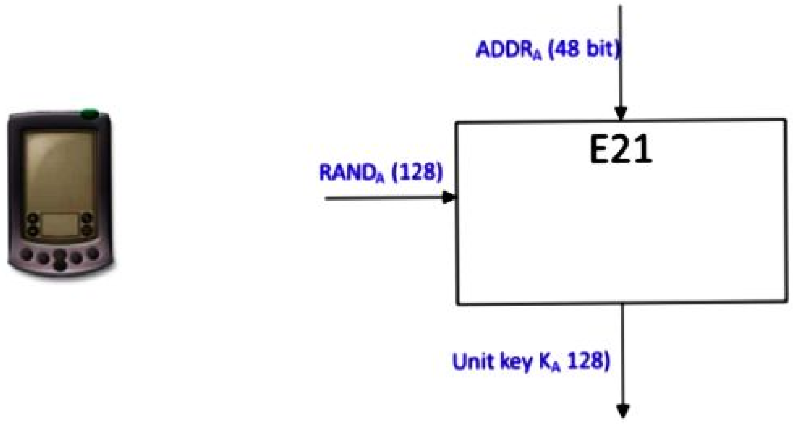
- ***Security Mode 1:*** No-Secure Mode, (There won't be any authentication or encryption in this mode. Bluetooth device can easily be connected with the other devices).
- ***Security Mode 2:*** Service level security mode, (The management of the access control and interfaces with other protocols and device users is handled by the centralized security manager, it includes Authentication, Configuration and Authorization).
- ***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.

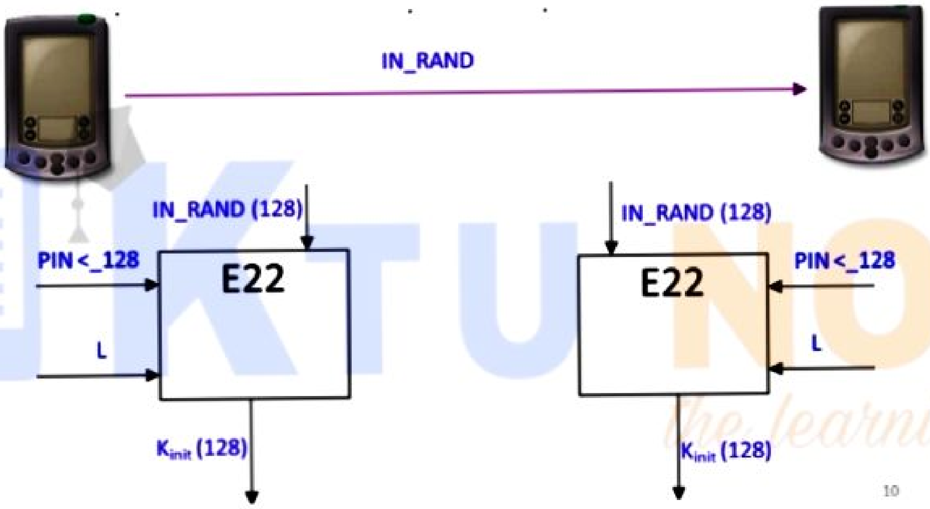
1. Generation unit key

- ✓ It is a Semi permanent Key.
- ✓ Bluetooth Device Operated for the First time.
- ✓ ADDR_A (48 bit)



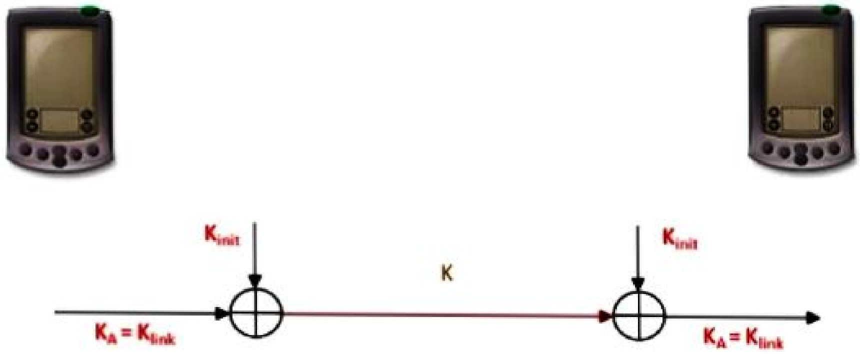
2. Generation initialization key

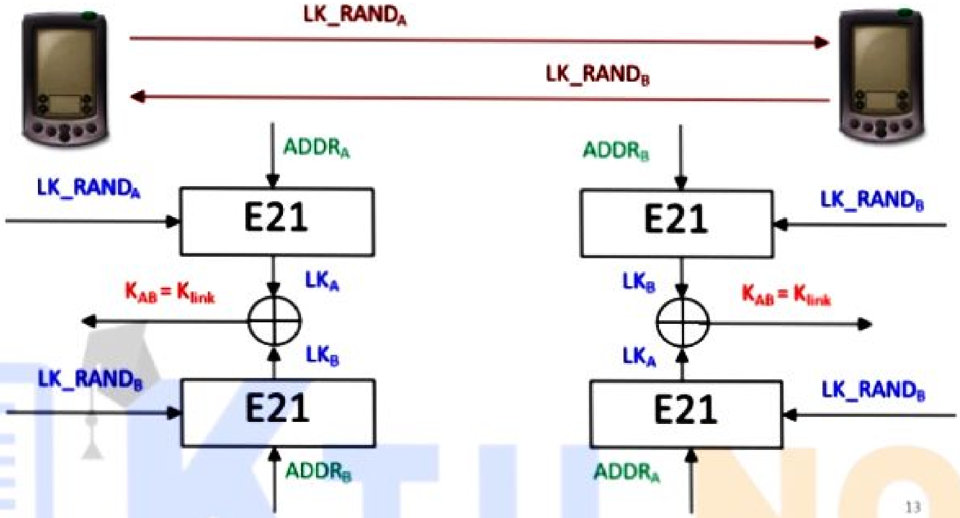
- ✓ it's a temporarily Key.
- ✓ Communication between two Device (P'=PIN + BD_ADDR).
- ✓ XOR Operation. Here Unit key = Link key.



3. Generation Combination Key

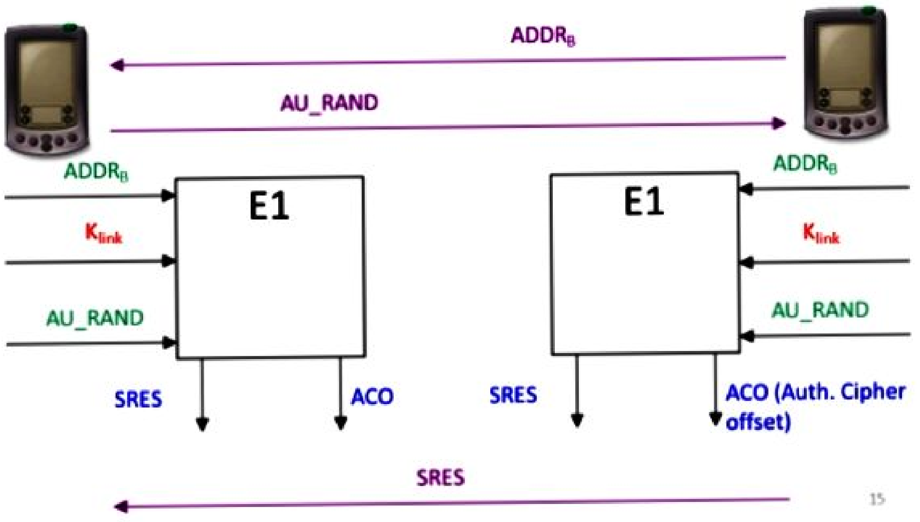
- The Combination key is the combination of two generated in a device A and B, Respectively.
- Each device generates a random no. LK_RAND$_A$ and LK_RAND$_B$.
- Then utilizing E$_{21}$ they generate LK_K$_A$ and LK_K$_B$ respectively.
- LK_K=E$_{21}$ (LK_RAND, BD_ADDR)
- LK_K$_A$ and LK_K$_B$ are XORed with the current link key.
- Device A calculate LK_RAND$_A$ LK_RAND$_B$.
- K$_{AB}$ is calculated simply by XORing LK_K$_A$ and LK_K$_B$.

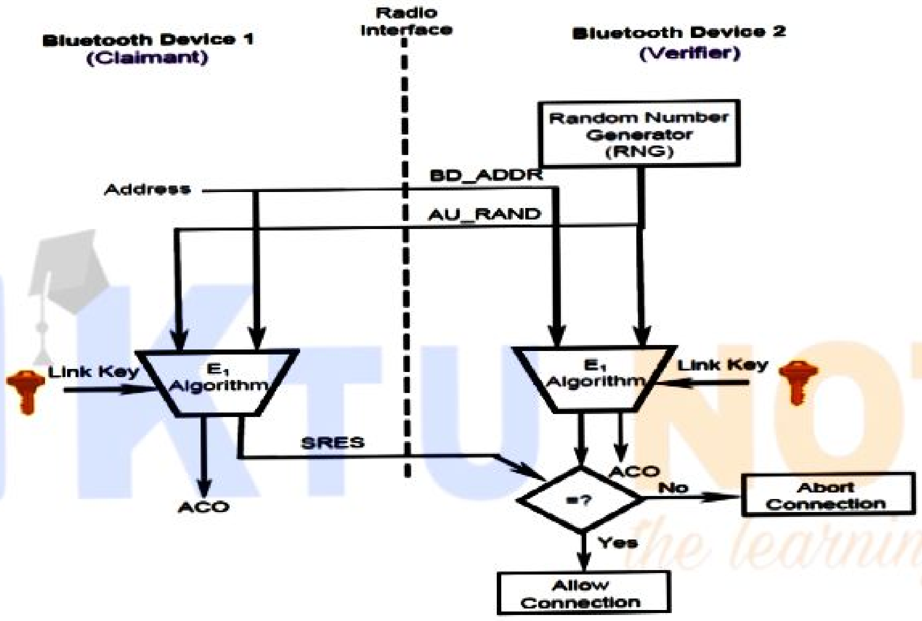




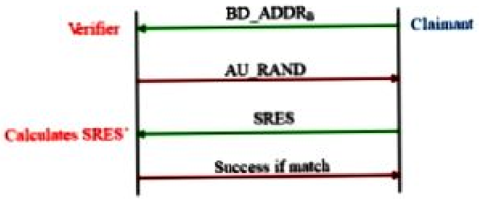
4. Authentication

- 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.





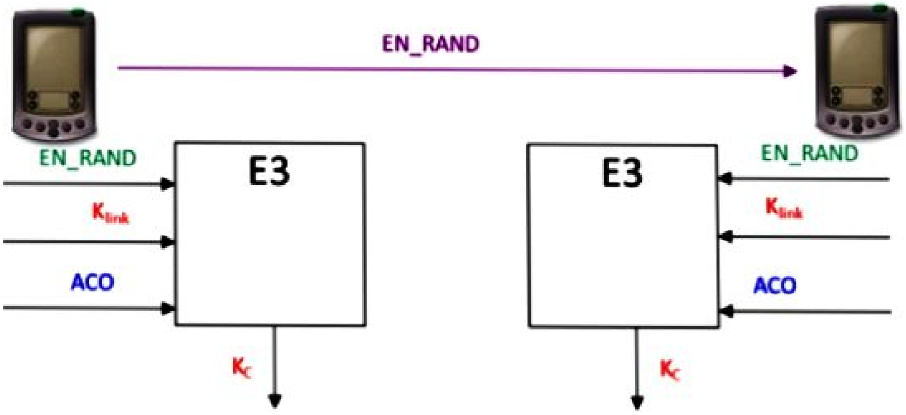
Authentication Summary



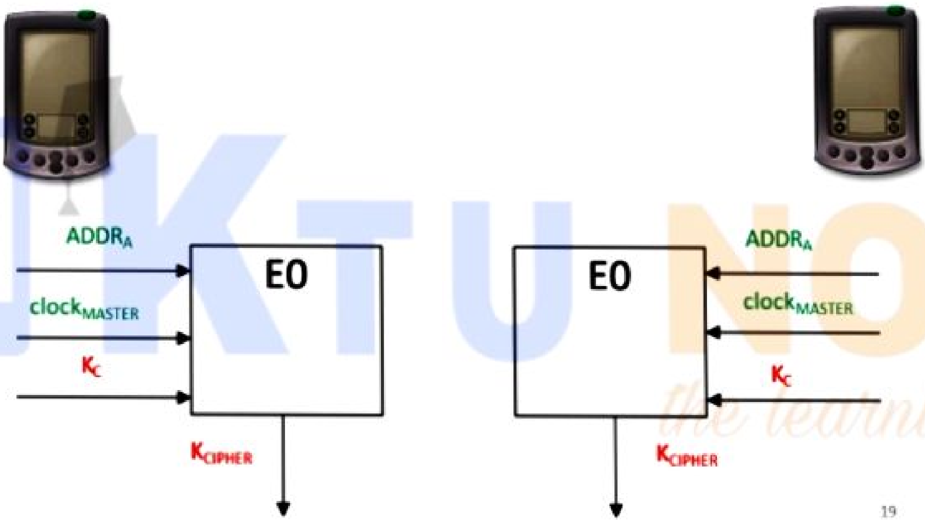
Authentication Process

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

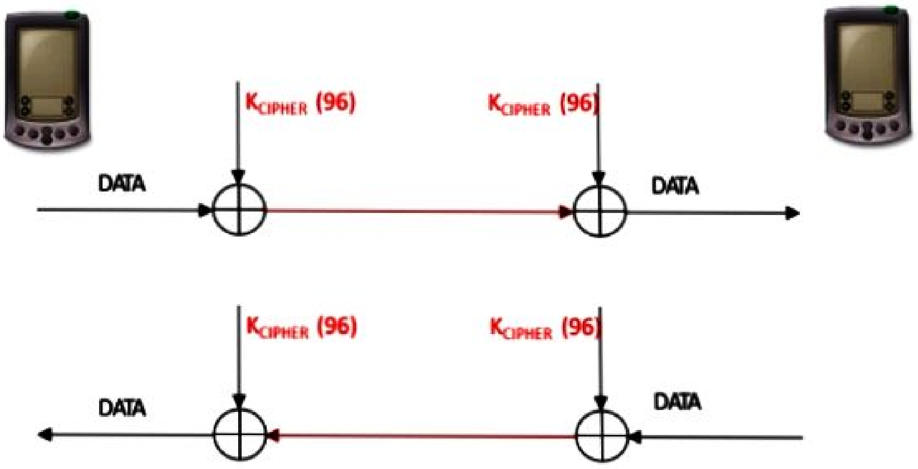
5. Generation encryption key



6. Generation key stream



7. Encryption of data



Most important security weaknesses

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