Bluetooth Security

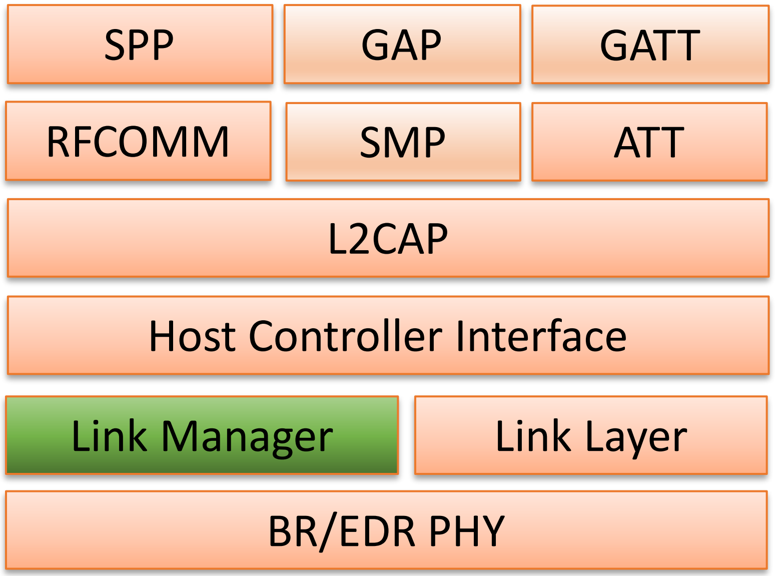
Mohit Sethi
Ericsson, Finland
Aalto University, Finland

Bluetooth Security - Outline

- Part 1:
  - Bluetooth standard evolution
  - Bluetooth stack and protocols
- Part 2:
  - Pairing and Bonding
  - Privacy with Private addresses
- Part 3:
  - Mesh and secure joining

Bluetooth – Pairing

- Pairing in BR/EDR vs. BLE:
  - Security Manager: defines protocols for managing pairing, authentication, and encryption



SPP | GAP | GATT

RFCOMM | SMP | ATT

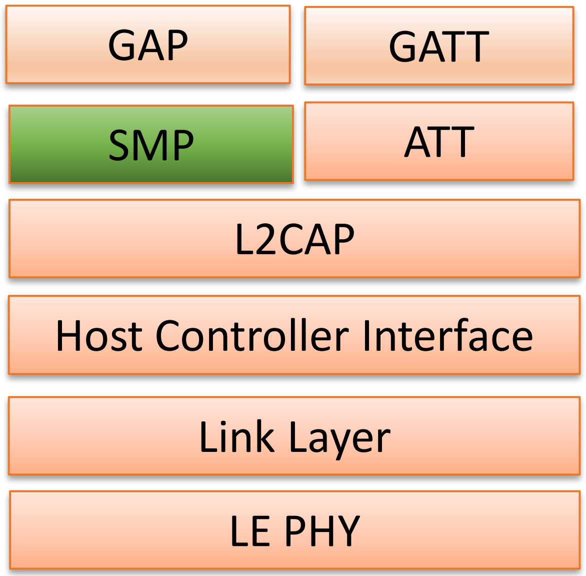
L2CAP

Host Controller Interface

Link Manager | Link Layer

BR/EDR PHY

BR/EDR protocol stack



GAP | GATT

SMP | ATT

L2CAP

Host Controller Interface

Link Layer

LE PHY

LE protocol stack

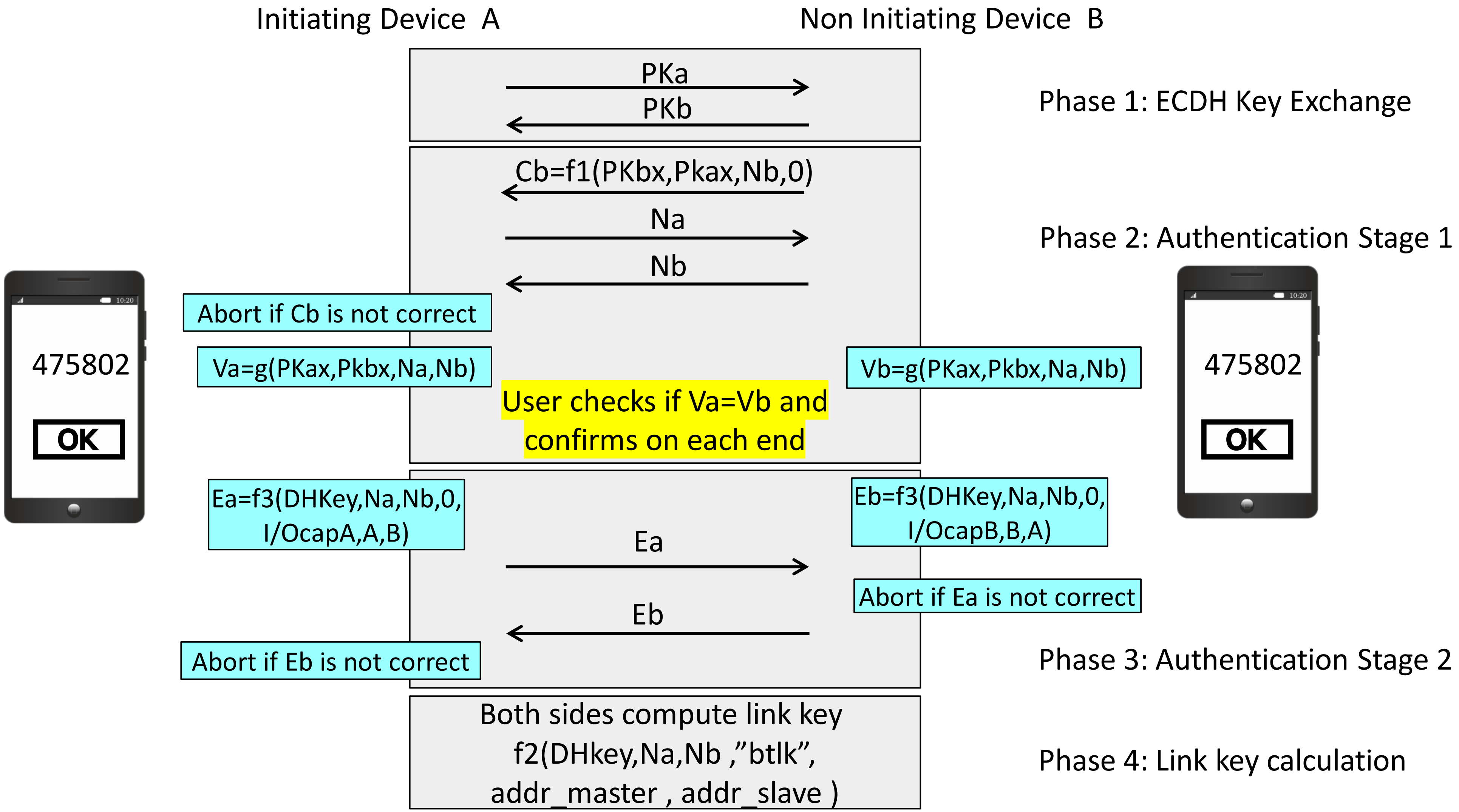
Bluetooth – Pairing

- Many versions and names
  - BR/EDR:
    - Version 2.1 – Secure Simple Pairing
    - Version 4.2 – Secure connections
  - LE:
    - Version 4.0/4.1 – called LE legacy pairing (based on SSP with modifications)
    - Version 4.2 – Secure connections
  - Most devices support old versions for interoperability => Susceptible to attacks

Bluetooth – Pairing

- Exchange I/O capabilities – decides association model:
  - Just works – protection only from passive attacker
  - Numeric Comparison – short 6-digit confirmation values show
  - Out-of-band – message sent over NFC for example
  - Passkey entry – user enters passkey into two devices being paired
- Phases:
  - Exchange of ECDH public keys
  - Authentication stage 1 and 2
  - Link-key calculation

Bluetooth – Pairing with Numeric Comparison



Initiating Device A

Non Initiating Device B

PKa

PKb

Phase 1: ECDH Key Exchange

Cb=f1(PKbx,Pkax,Nb,0)

Na

Nb

Phase 2: Authentication Stage 1

Abort if Cb is not correct

Va=g(PKax,Pkbx,Na,Nb)

Vb=g(PKax,Pkbx,Na,Nb)

User checks if Va=Vb and confirms on each end

Ea=f3(DHKey,Na,Nb,0, I/OcapA,A,B)

Eb=f3(DHKey,Na,Nb,0, I/OcapB,B,A)

Ea

Abort if Ea is not correct

Eb

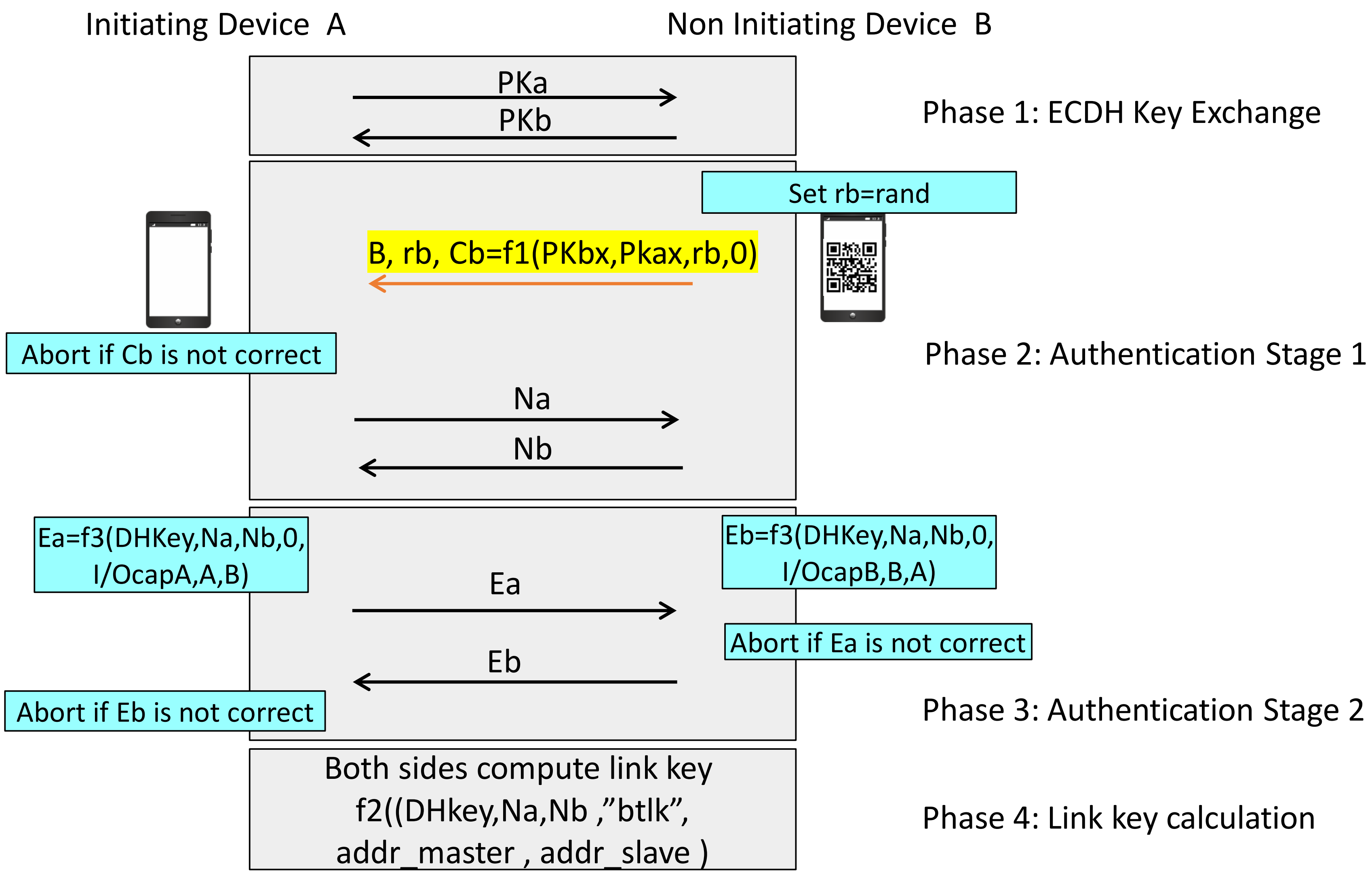
Abort if Eb is not correct

Phase 3: Authentication Stage 2

Both sides compute link key f2(DHkey,Na,Nb ,”btlk”, addr_master , addr_slave)

Phase 4: Link key calculation

Bluetooth – Pairing with OOB



Initiating Device A

Non Initiating Device B

PKa

PKb

Phase 1: ECDH Key Exchange

Set rb=rand

B, rb, Cb=f1(PKbx,Pkax,rb,0)

Abort if Cb is not correct

Na

Nb

Phase 2: Authentication Stage 1

Ea=f3(DHKey,Na,Nb,0, I/OcapA,A,B)

Eb=f3(DHKey,Na,Nb,0, I/OcapB,B,A)

Ea

Abort if Ea is not correct

Eb

Abort if Eb is not correct

Phase 3: Authentication Stage 2

Both sides compute link key f2((DHkey,Na,Nb ,"btlk", addr_master , addr_slave)

Phase 4: Link key calculation

Bluetooth – Bonding and LMP authentication

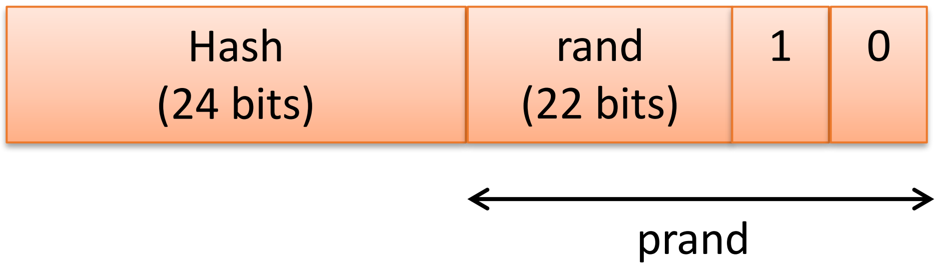
- Pairing results in generation of link-key
- Bonding stores a LTK after pairing for establishing future connections without pairing
  - Bonding in LE also distributes Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK)
- LMP authentication – mutual authentication to confirm that both have same link key
  - Secure authentication: exchange random numbers, compute hash with link-key and random numbers, send SRES (expected response). If SRES match with locally computed values, link-key authenticated and fresh keys generated

Bluetooth LE - Privacy

- 4 types of address in LE
  - Public address: Fixed, global (registration with IEEE), never changes
  - Random addresses:
    - Static address: Can change at bootup but static during runtime
    - Resolvable private address: Optional. Changes periodically (≈ 15 min): generated using IRK and a random number. Can be resolved by other devices which have bonded earlier
    - Non-resolvable private address: Optional. Also changes periodically. No one else can resolve such addresses. Used for privacy in beacons or Covid-19 tracing

Bluetooth LE - Privacy

- Resolvable private address:
  - Generation: hash = ah(IRK, prand) concatenated with prand



Hash
(24 bits)

rand
(22 bits)

1

0

prand

  - Resolution: Receiver uses the prand with all IRKs in its database to lookup the peer device