Network Security: WLAN Security: WPA3

Mohit Sethi

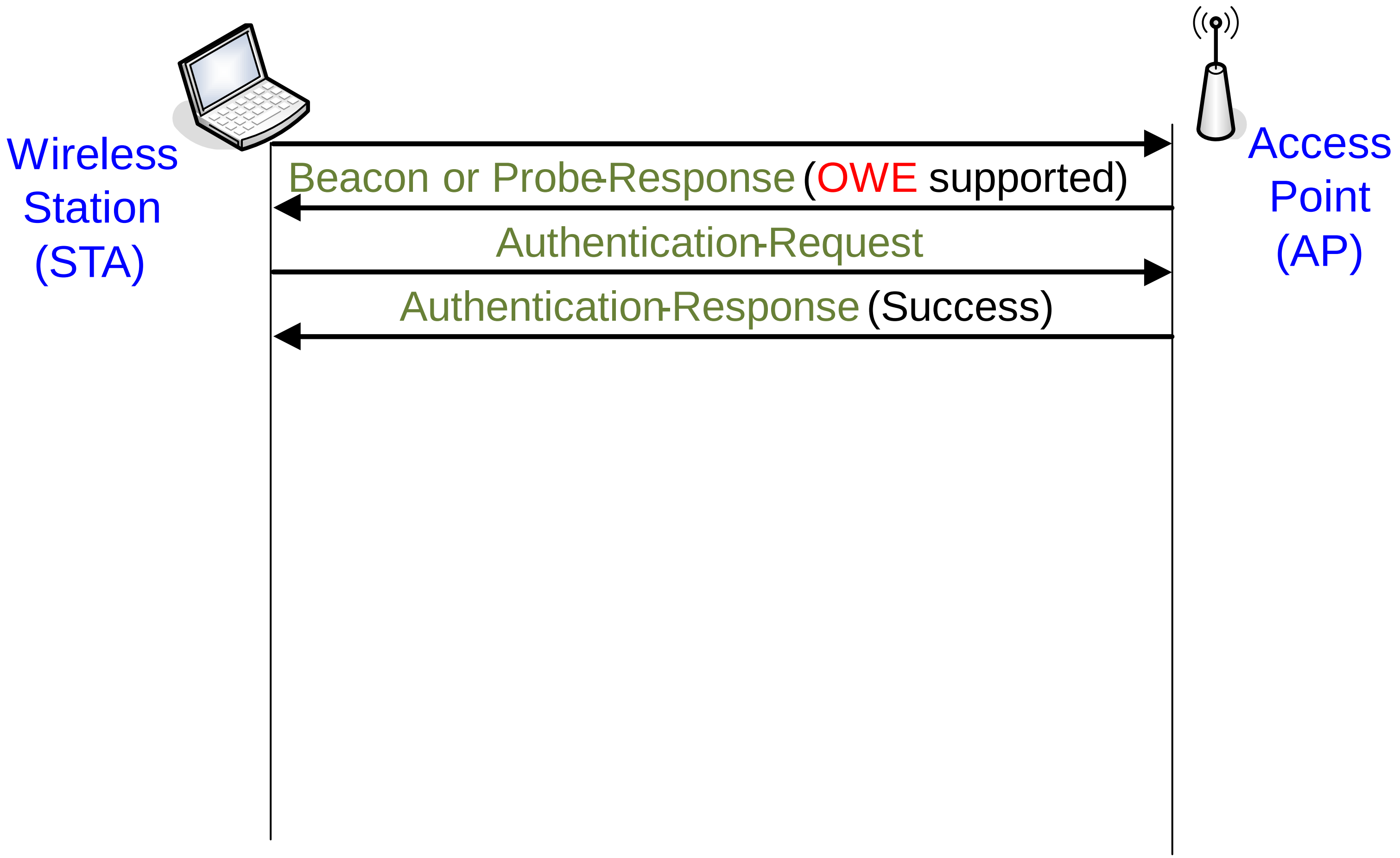
Ericsson, Finland

Aalto University, Finland

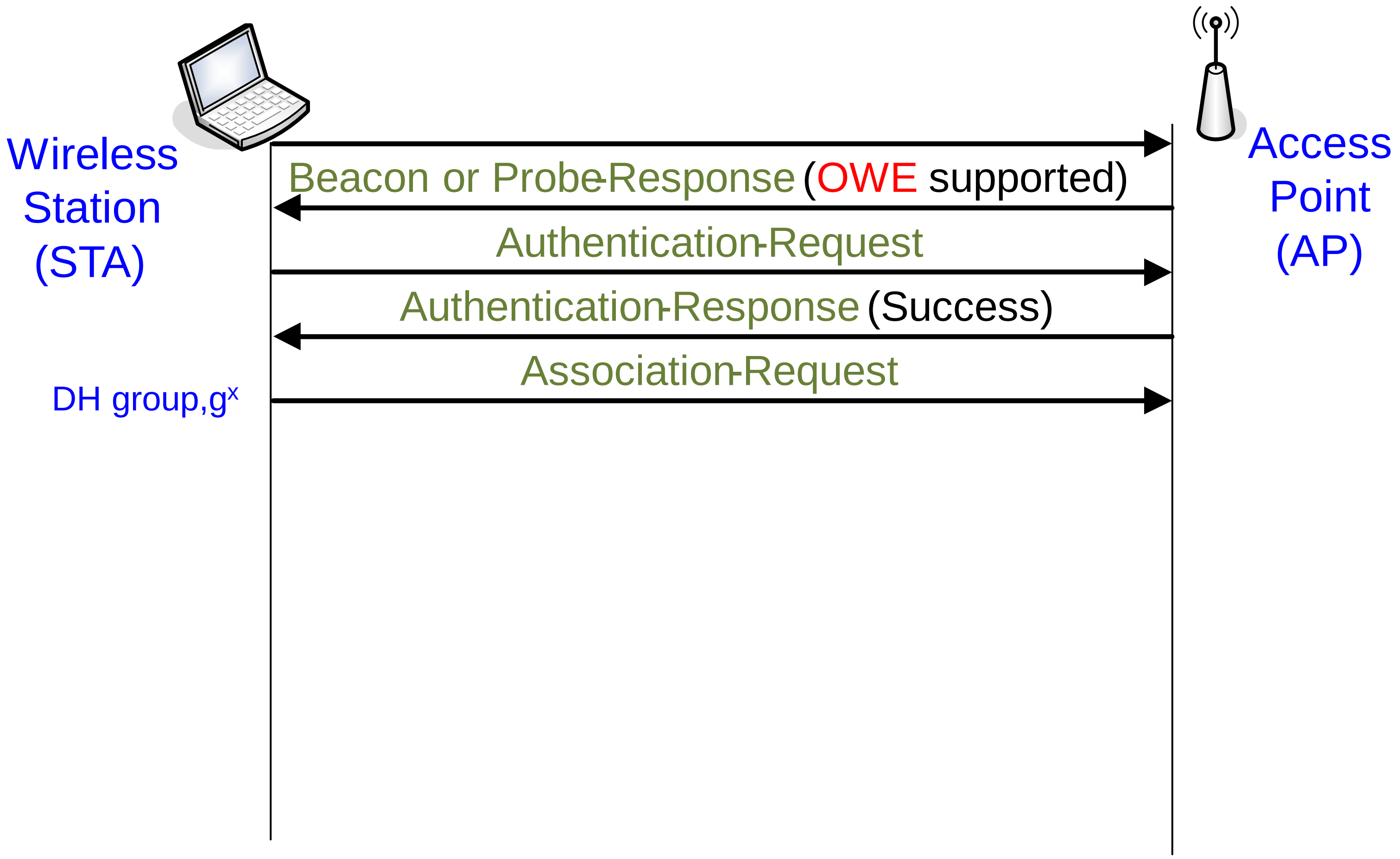
WPA3 Enhanced Open

- Open networks used in cafes and airports
  - Better user experience than asking for passphrase
- WPA3 Enhanced Open provides Opportunistic Wireless Encryption (OWE) for open networks – RFC 8110
- Station and AP perform Diffie-Hellman (DH) exchange during association
- A PMK is derived from DH shared secret
- PMK is used in 4 – way handshake as before

WPA3 Enhanced Open


Wireless Station (STA)
Access Point (AP)
Beacon or Probe-Response (OWE supported)
Authentication-Request
Authentication-Response (Success)

WPA3 Enhanced Open



Wireless Station (STA)

Access Point (AP)

Beacon or Probe-Response (OWE supported)

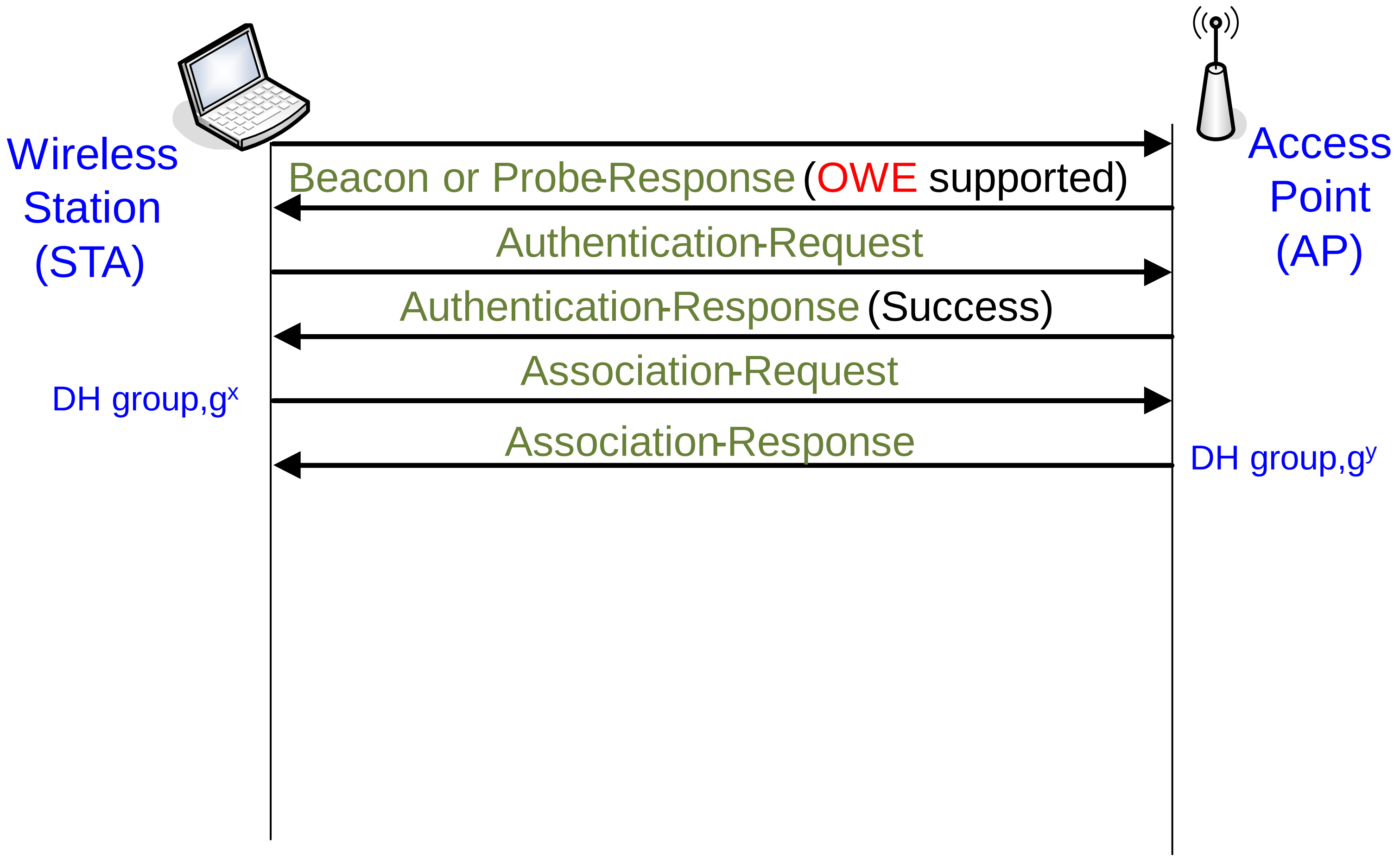
Authentication-Request

Authentication-Response (Success)

Association-Request

DH group,g^x

WPA3 Enhanced Open



Wireless Station (STA)

Access Point (AP)

Beacon or Probe-Response (OWE supported)

Authentication-Request

Authentication-Response (Success)

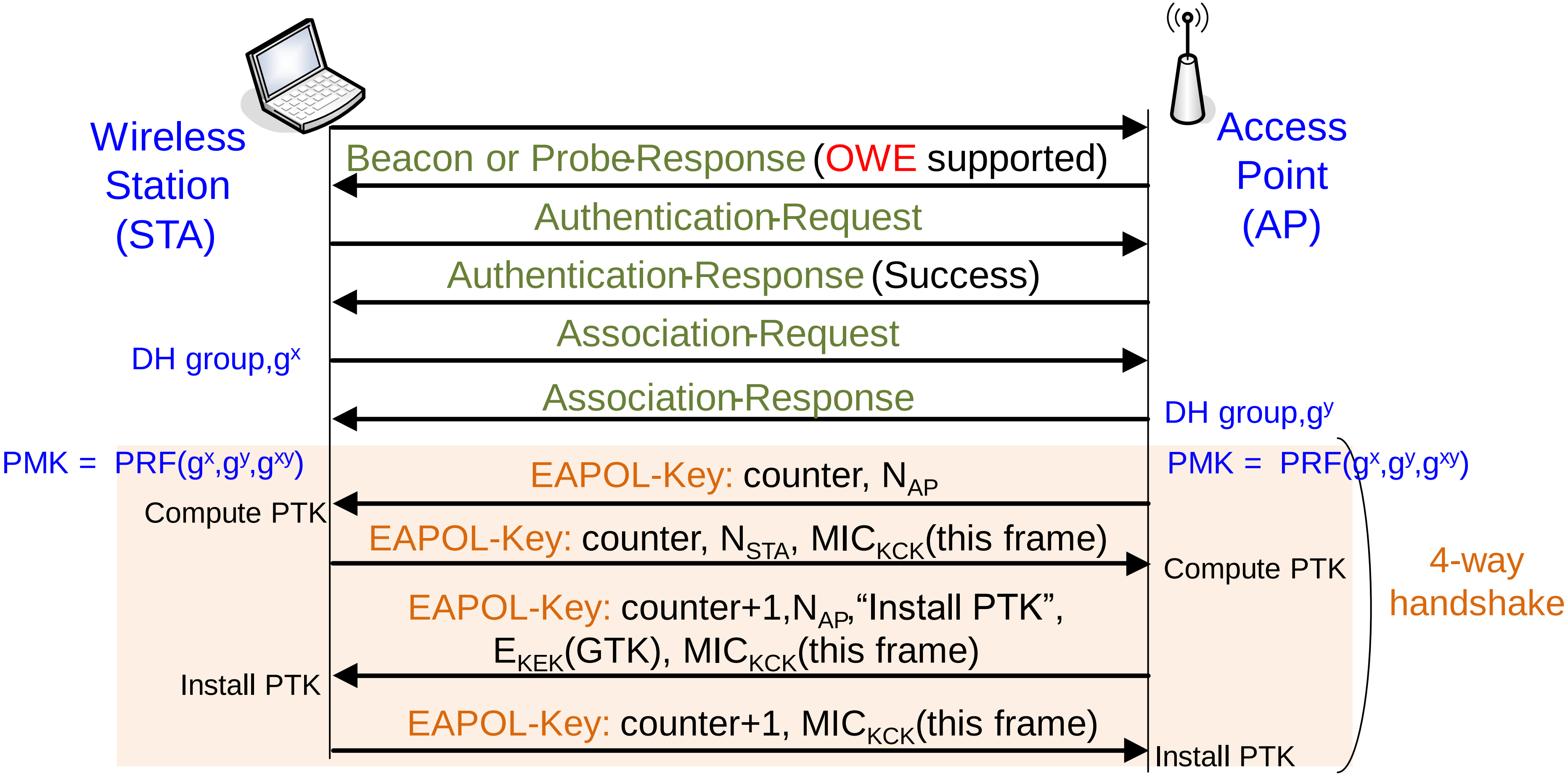
Association-Request

DH group,g^x

Association-Response

DH group,g^y

WPA3 Enhanced Open

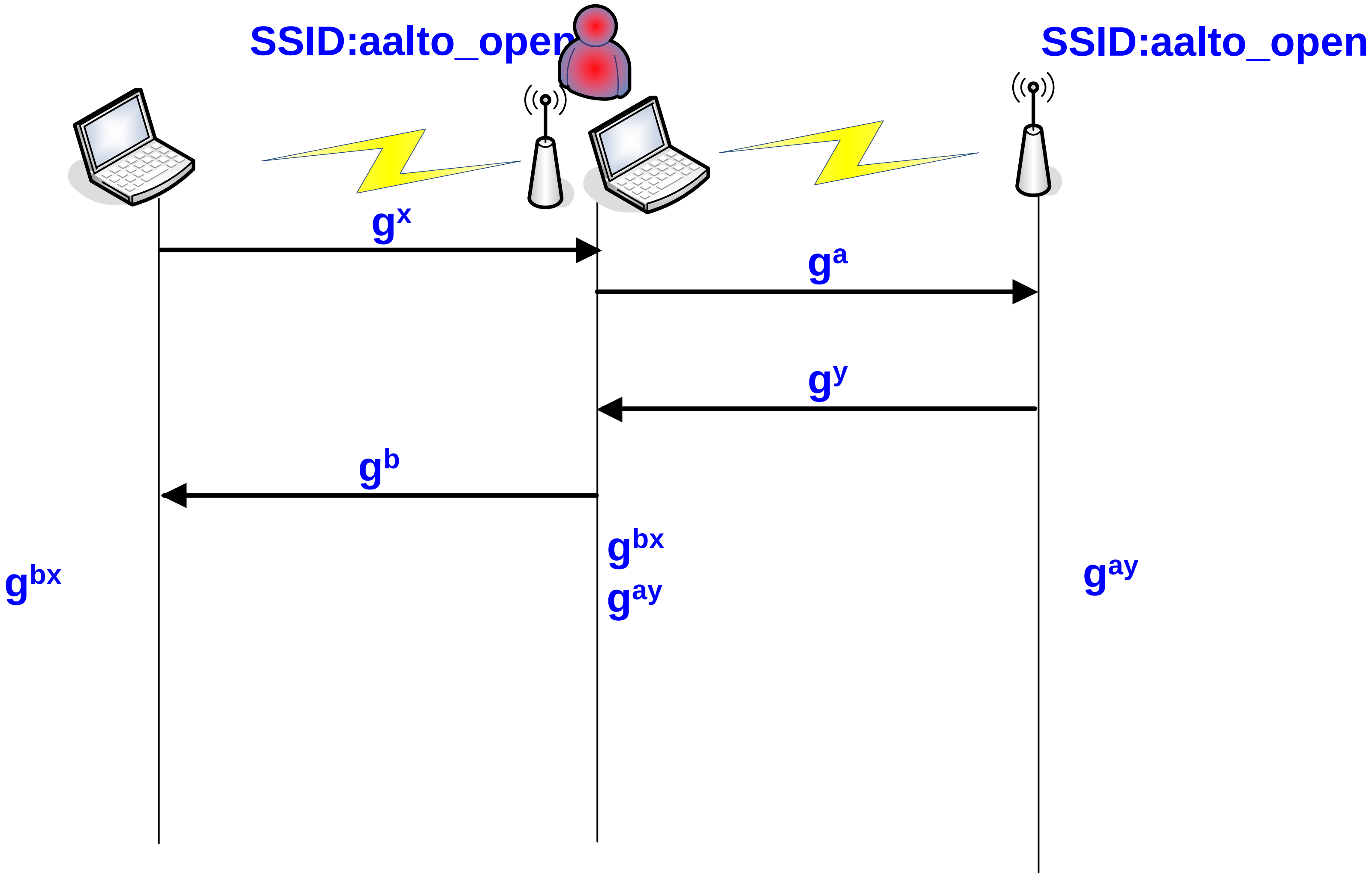


Wireless Station (STA)
Access Point (AP)
Beacon or Probe Response (OWE supported)
Authentication Request
Authentication Response (Success)
Association Request
DH group, g^x
Association Response
DH group, g^y
PMK = PRF(g^x,g^y,g^{xy})
PMK = PRF(g^x,g^y,g^{xy})
EAPOL-Key: counter, N_{AP}
Compute PTK
EAPOL-Key: counter, N_{STA}, MIC_{KCK}(this frame)
Compute PTK
4-way handshake
EAPOL-Key: counter+1, N_{AP}, “Install PTK”, E_{KEK}(GTK), MIC_{KCK}(this frame)
Install PTK
EAPOL-Key: counter+1, MIC_{KCK}(this frame)
Install PTK

WPA3 Enhanced Open

- OWE is encryption NOT authentication
  - Susceptible to active MiTM attack
  - Does NOT prevent evil twin APs

WPA3 Enhanced Open



SSID:aalto_open

SSID:aalto_open

g^x

g^a

g^y

g^b

g^{bx}

g^{bx}

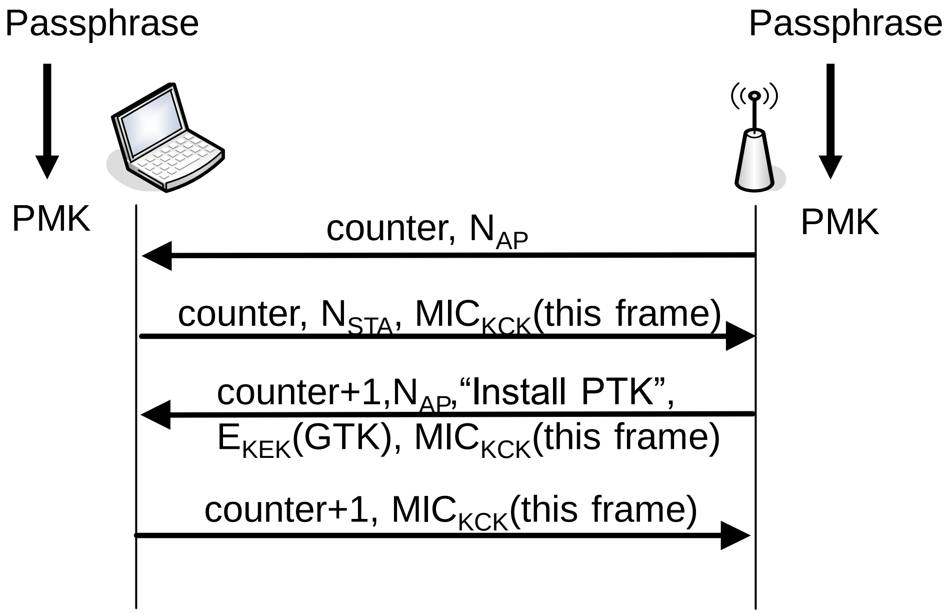
g^{ay}

g^{ay}

WPA3 Enhanced Open

- Both ECC and FFC based Diffie-Hellman supported
- OWE is encryption NOT authentication
  - Susceptible to active MiTM attack
  - Does NOT prevent evil twin Aps
- No prior contact between Station and AP for PMK (= no shared knowledge of passphrase)
- Better than open authentication:
  - Passive attacker now needs to be active
  - Attacker cannot inject packets without active MiTM first
  - Forward secrecy when private keys are deleted
- Can do client authentication later with captive portal

WPA2 – Personal: Weakness



Passphrase

PMK

Passphrase

PMK

counter, N_{AP}

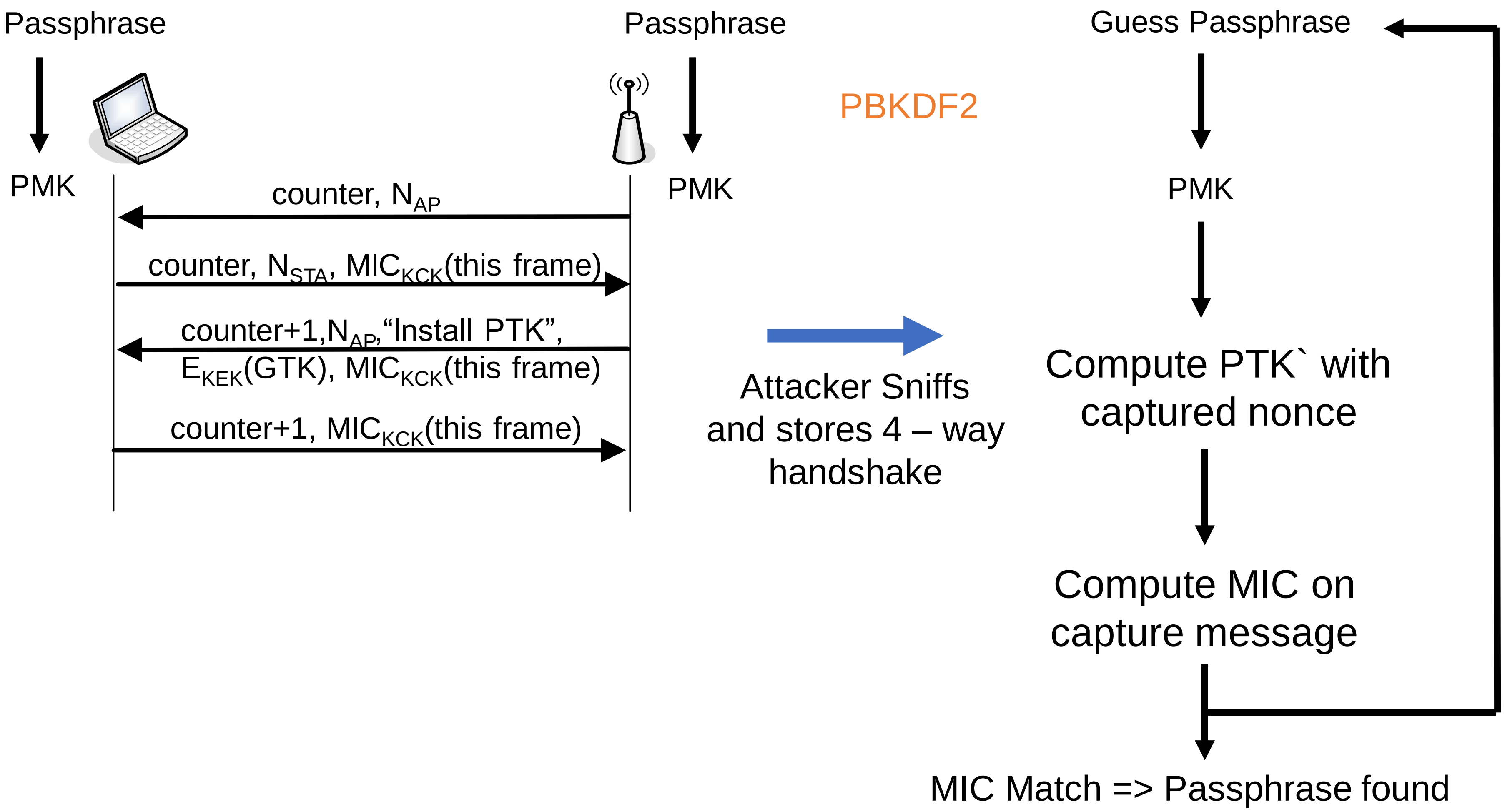
counter, N_{STA}, MIC_{KCK}(this frame)

counter+1,N_{AP},“Install PTK”, E_{KEK}(GTK), MIC_{KCK}(this frame)

counter+1, MIC_{KCK}(this frame)

PBKDF2

WPA2 – Personal: Weakness



Passphrase

PMK

Passphrase

PMK

counter, N_{AP}

counter, N_{STA}, MIC_{KCK}(this frame)

counter+1,N_{AP},“Install PTK”, E_{KEK}(GTK), MIC_{KCK}(this frame)

counter+1, MIC_{KCK}(this frame)

PBKDF2

Attacker Sniffs and stores 4 – way handshake

Guess Passphrase

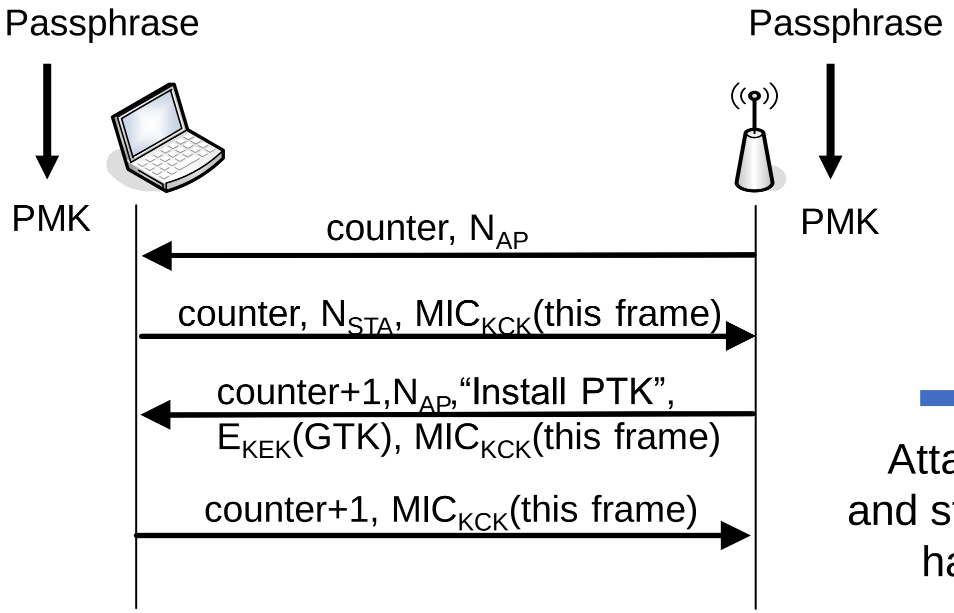
PMK

Compute PTK` with captured nonce

Compute MIC on capture message

MIC Match => Passphrase found

WPA2 – Personal: Weakness



Passphrase

PMK

Passphrase

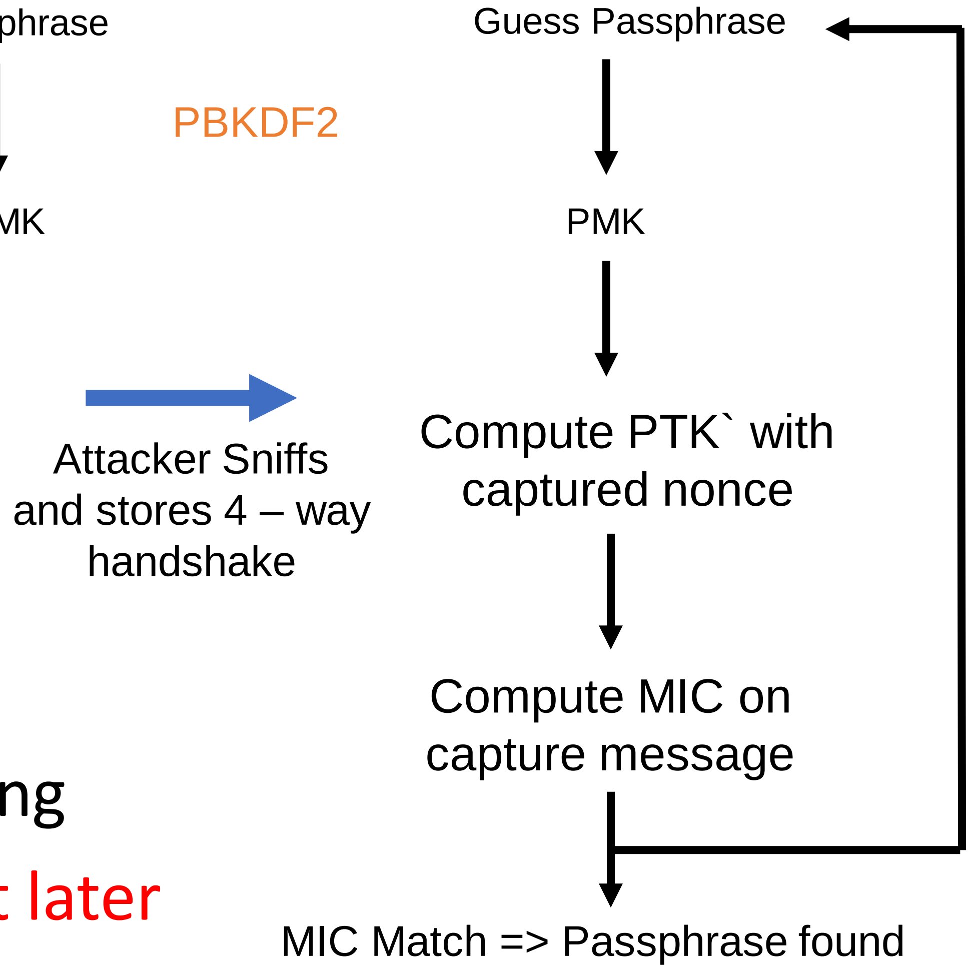
PMK

counter, N_{AP}

counter, N_{STA}, MIC_{KCK}(this frame)

counter+1,N_{AP},"Install PTK",
E_{KEK}(GTK), MIC_{KCK}(this frame)

counter+1, MIC_{KCK}(this frame)



PBKDF2

Attacker Sniffs
and stores 4 – way
handshake

Guess Passphrase

PMK

Compute PTK` with
captured nonce

Compute MIC on
capture message

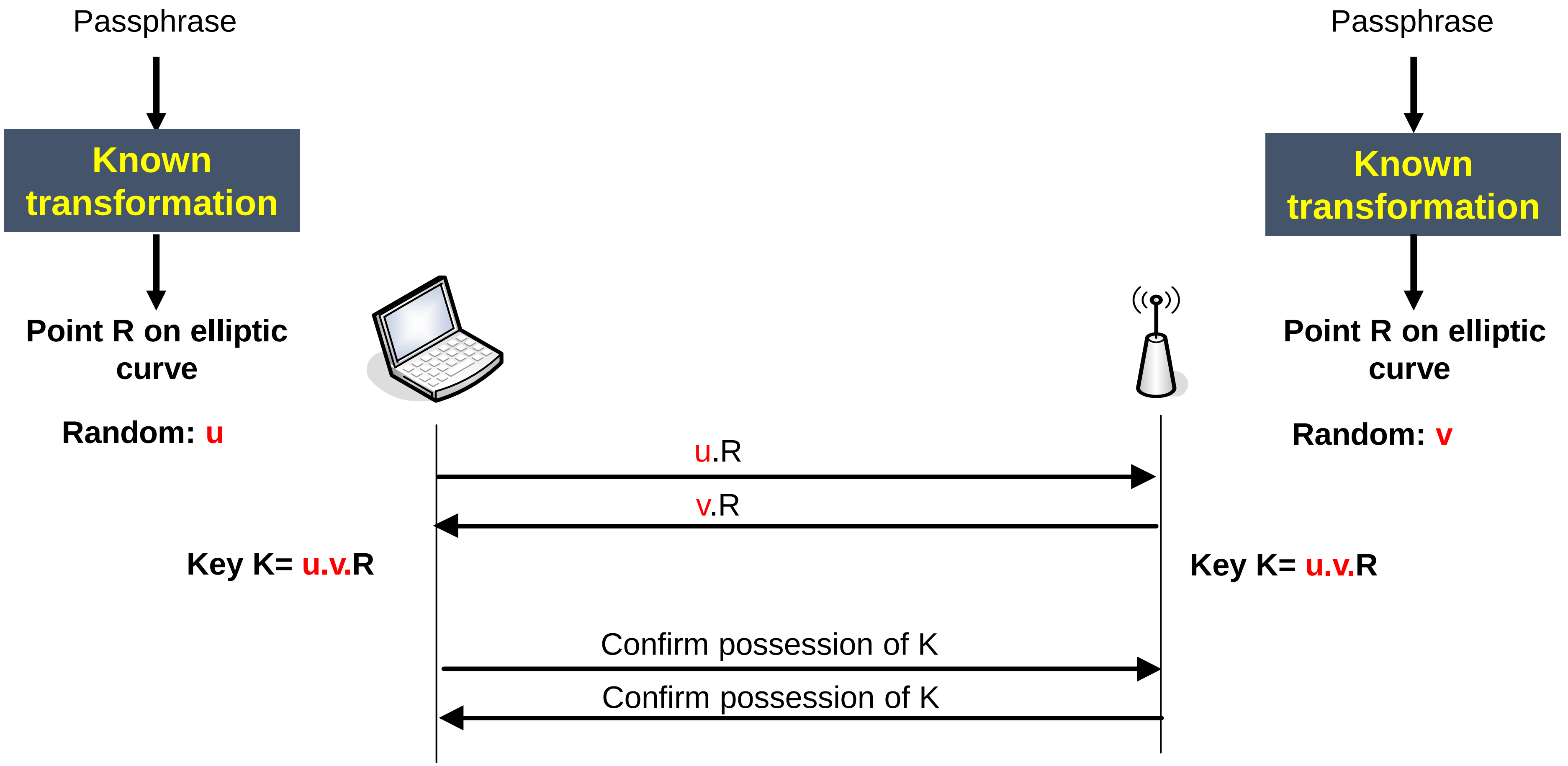
MIC Match => Passphrase found

- Unlimited offline guessing
- Capture today – decrypt later

WPA3 PAKE : Dragonfly

- WPA3 uses Password Authenticated Key Exchange (PAKE) for preventing password guessing
  - WPA3 uses a variant of Dragonfly – RFC 7664 as PAKE
  - Original protocol called Simultaneous Authentication of Equals (SAE) defined in 802.11s in 2016
  - Standard for security in mesh networks
- Offline attacker cannot perform password guessing
- A live attacker physically present in the network can keep guessing but devices can setup protection against such repeated guessing - denial of service (DoS)

PAKE example



Passphrase

Known transformation

Point R on elliptic curve

Random: u

Passphrase

Known transformation

Point R on elliptic curve

Random: v

u.R

v.R

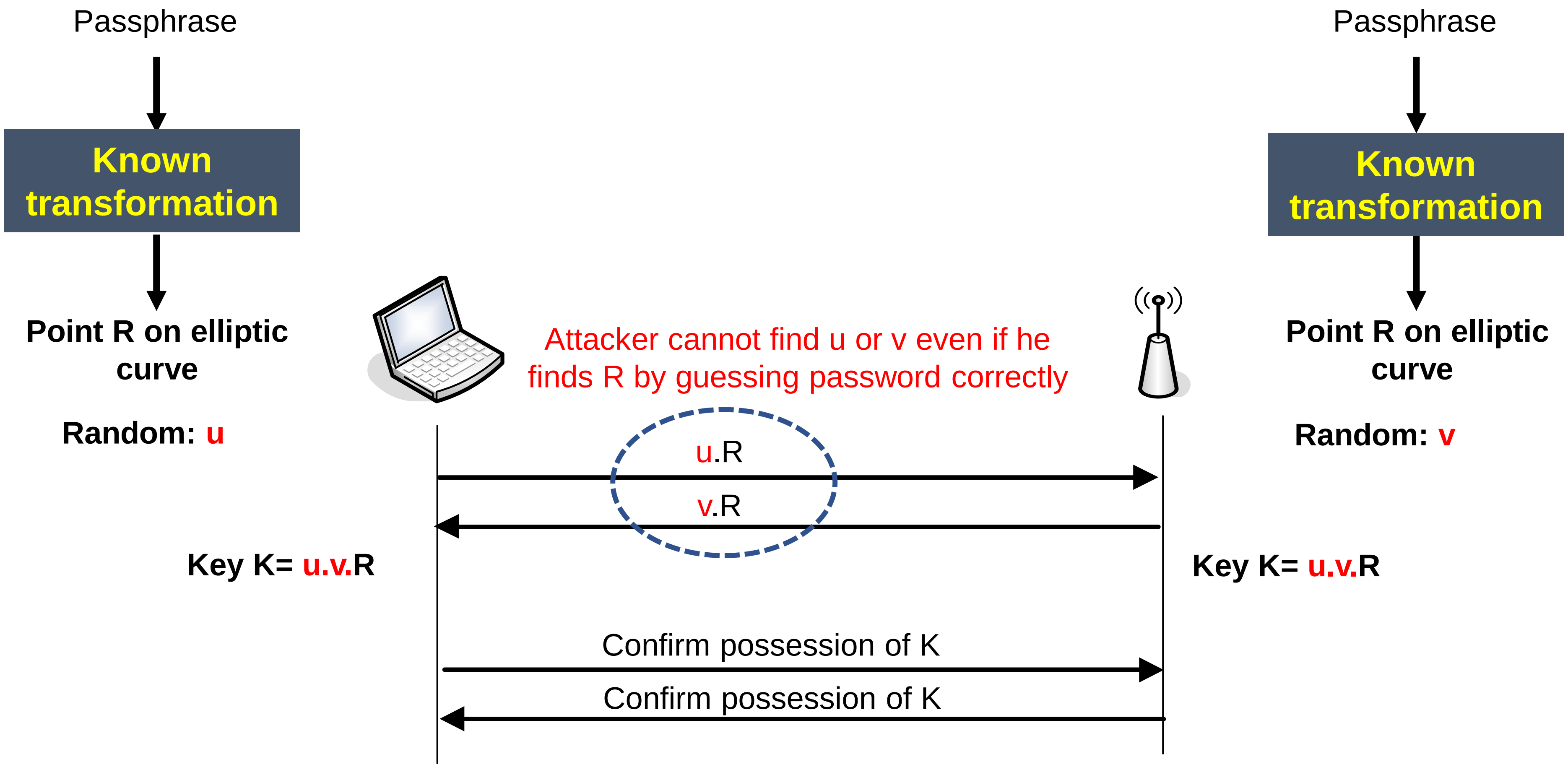
Key K= u.v.R

Key K= u.v.R

Confirm possession of K

Confirm possession of K

PAKE example



Passphrase

Known transformation

Point R on elliptic curve

Random: u

Key K= u.v.R

Attacker cannot find u or v even if he finds R by guessing password correctly

u.R

v.R

Confirm possession of K

Confirm possession of K

Passphrase

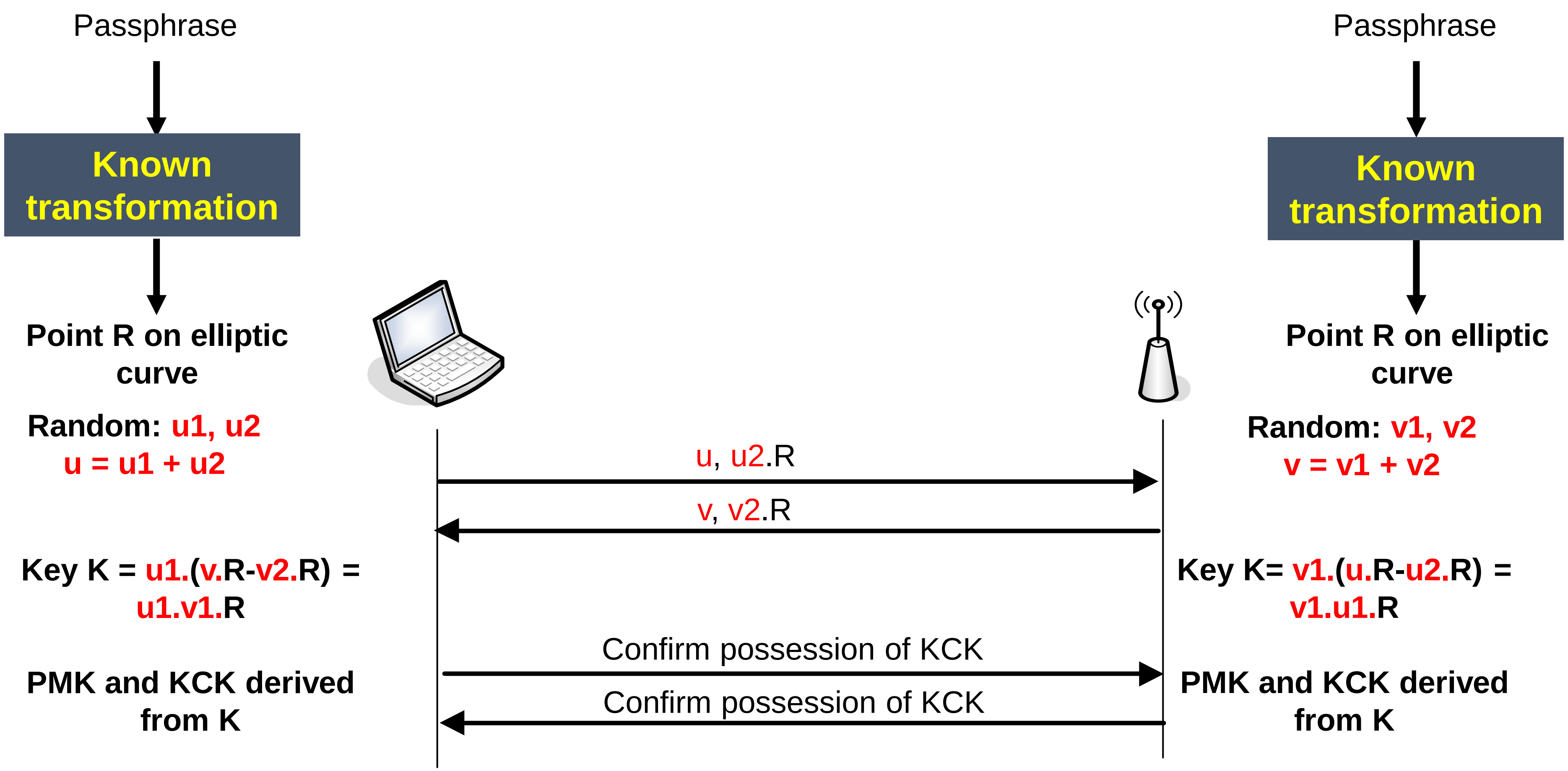
Known transformation

Point R on elliptic curve

Random: v

Key K= u.v.R

Dragonfly



Passphrase

Known transformation

Point R on elliptic curve

Random: u1, u2
u = u1 + u2

Key K = u1.(v.R-v2.R) = u1.v1.R

PMK and KCK derived from K

u, u2.R

v, v2.R

Confirm possession of KCK

Confirm possession of KCK

Passphrase

Known transformation

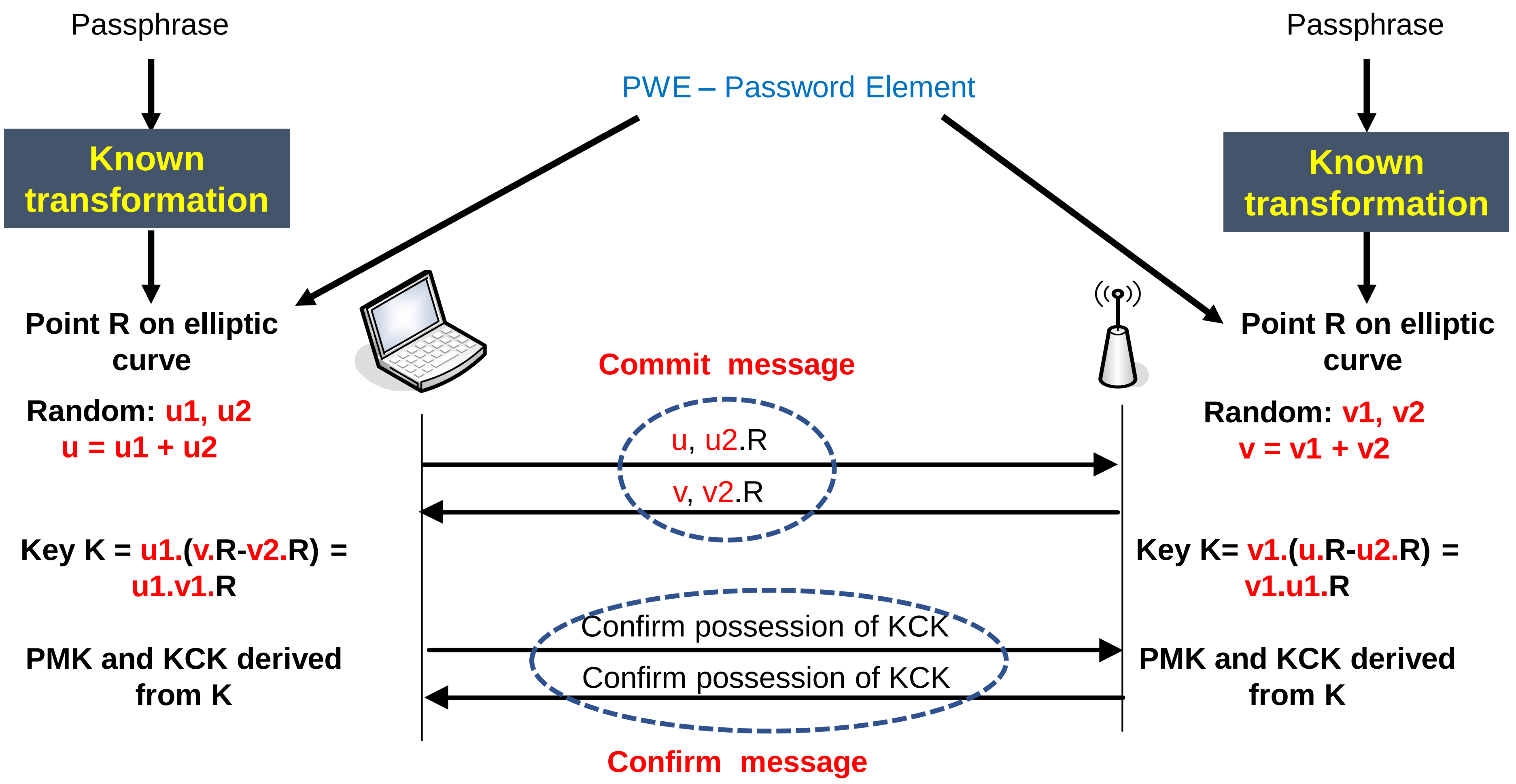
Point R on elliptic curve

Random: v1, v2
v = v1 + v2

Key K= v1.(u.R-u2.R) = v1.u1.R

PMK and KCK derived from K

Dragonfly



Passphrase

Known transformation

Point R on elliptic curve

Random: u1, u2

u = u1 + u2

Key K = u1.(v.R-v2.R) = u1.v1.R

PMK and KCK derived from K

PWE – Password Element

Commit message

u, u2.R

v, v2.R

Confirm possession of KCK

Confirm possession of KCK

Confirm message

Passphrase

Known transformation

Point R on elliptic curve

Random: v1, v2

v = v1 + v2

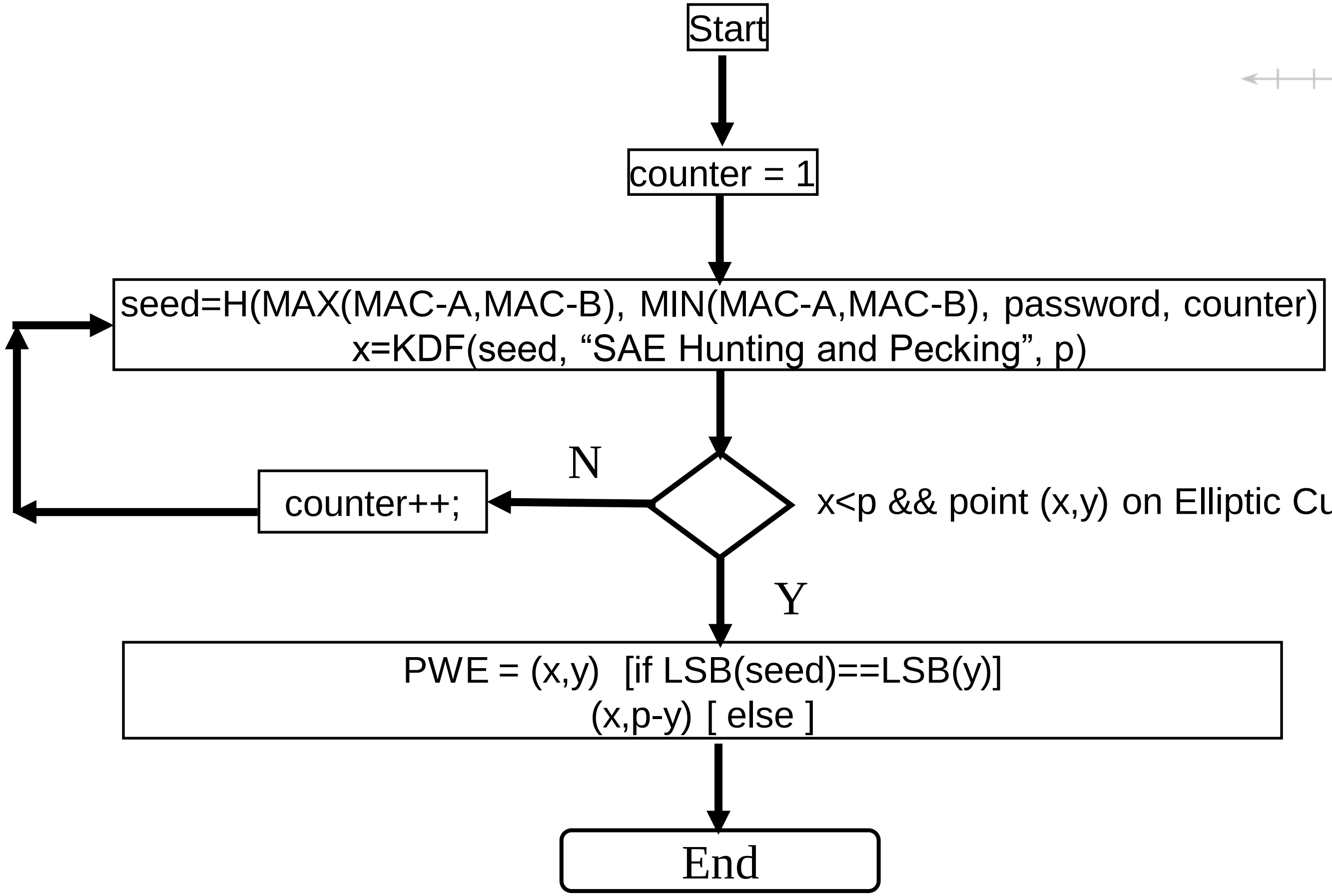
Key K= v1.(u.R-u2.R) = v1.u1.R

PMK and KCK derived from K

WPA3 PAKE : Dragonfly

- Dragonfly supports ECC and FFC group
- If not carefully implemented, side channel attacks are very possible
- Designed as a balanced PAKE – both sides know passphrase in plain
- Fresh PMK negotiated each time. This PMK is used in 4 – way handshake as before.
- PMK cannot be recovered even if passphrase is revealed later => forward secrecy after deleting u and v.

Example of PWE selection



Start

counter = 1

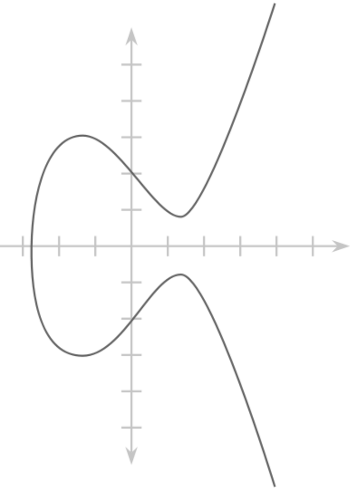
seed=H(MAX(MAC-A,MAC-B), MIN(MAC-A,MAC-B), password, counter)
x=KDF(seed, “SAE Hunting and Pecking”, p)

x<p && point (x,y) on Elliptic Curve P exists?

counter++;

PWE = (x,y) [if LSB(seed)==LSB(y)]
(x,p-y) [else]

End



WPA3 PAKE : Dragonfly

- Lot of controversy in IETF/IRTF when publishing
  - Trevor Perrin (well-known and respected cryptographer):
  - Questioned CFRG process: https://mailarchive.ietf.org/arch/msg/cfrg/0mnqMOmLy2N2H2K_F93MdUN_G28
  - Provided a critical review of Dragonfly: https://mailarchive.ietf.org/arch/msg/cfrg/YE4eKgOE9LTGbYd_hzN-nGDN-No
  - Asked for removal of CFRG chair: https://mailarchive.ietf.org/arch/msg/cfrg/scLoq7DvtXzo9Jl9AG9fQOcSGsM
- Many attacks in published in April 2019
  - https://papers.mathyvanhoef.com/dragonblood.pdf