heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

서울대학교 컴퓨터공학부
Seoul National University
Dept. of Computer Science and Engineering

Wireless Security - SU'19

abraham.rubinstein@heig-vd.ch

Chapter III

WPA

How To Improve WEP?

The IV Is Only 24 Bits Long and It Is Sent in Clear Text

- Increase de size of the IV
- Use it differently! Do not make it a direct part of the key

The Shared Secret Is Static Reuse Is Dangerous

- The shared secret is now used as a seed to produce "session" keys
  - They are renewed for every connection
  - They are unique for every user
- In fact, we use a unique key for every frame!

Authentication Is Weak

Challenge and response are easy to capture - no mutual authentication

- Authentication is now mutual
- It is a lot more complex
- Implicit in a new 4-way handshake

WEP Does Not Protect Against Forgery and Double Frames

- Re-injected frames are no longer tolerated
- Injection/forgery attempts lead to network shutdown

WEP Uses a Very Weak Integrity Control

- The new integrity control is now much bigger
- It uses a cryptographic algorithm

Amendment 802.11i

- Specifies two new protocols: TKIP and CCMP
- TKIP was developed so it would be compatible with old equipment
  - It reuses WEP as the basic layer
- Two variants :
  - WPA-Personal
  - WPA-Enterprise
- WPA-Enterprise derives keys from a TLS authentication

Security Today

WPA (WiFi Protected Access)

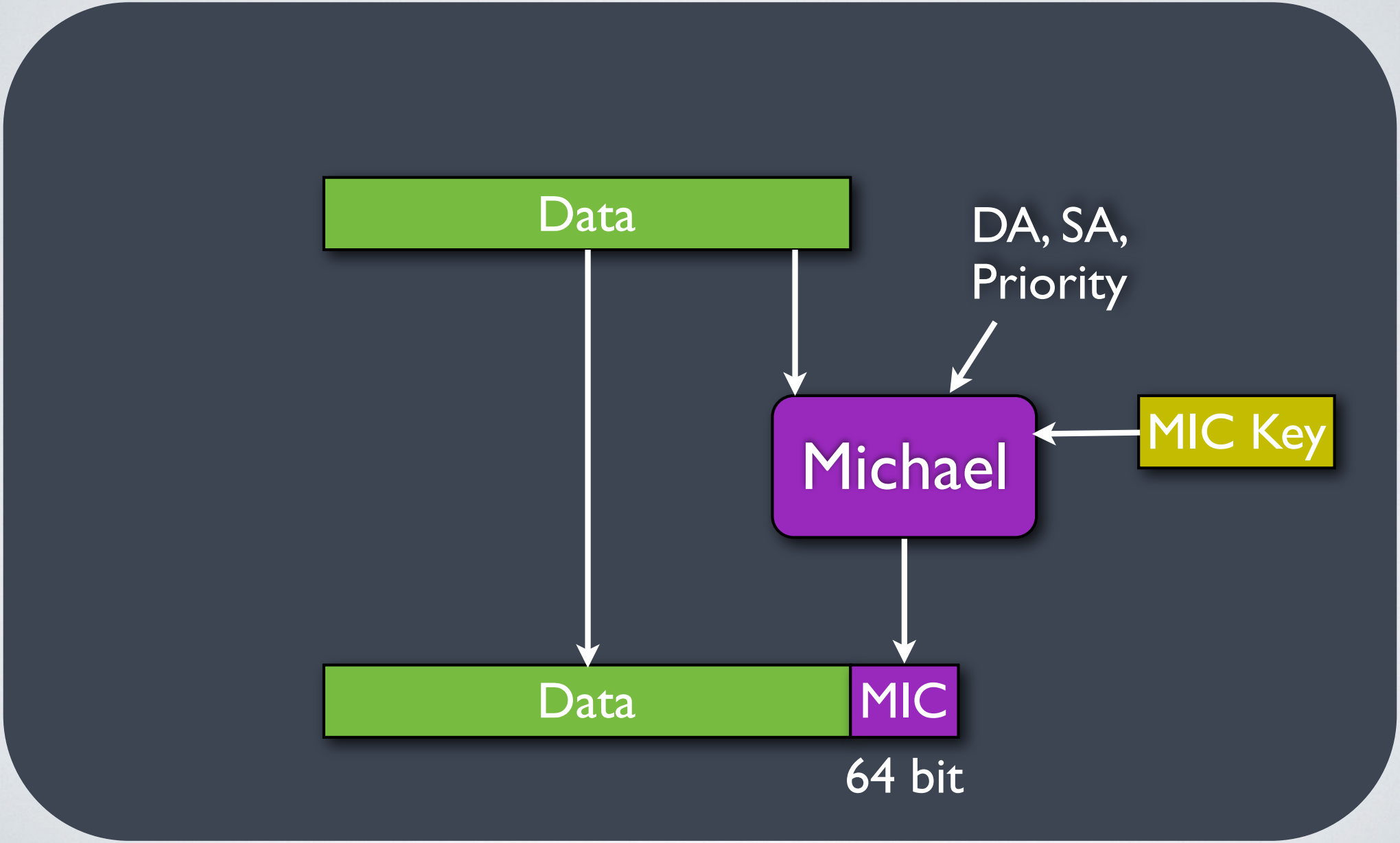
WPA

- New Integrity Control (MIC)
  - Cryptographic
  - 64 bits
- The shared key is derived from nonces, MAC adresses and other elements
  - 4-way handshake
- The shared key and the IV are used in a very different way
  - TKIP algorithm
- IV's are now 48 bits long
  - Used as a sequence counter (protection against re-injection)
  - $2.81474977 \times 10^{14}$ combinations
  - The keystream is **never** reused, even if the IV is reused

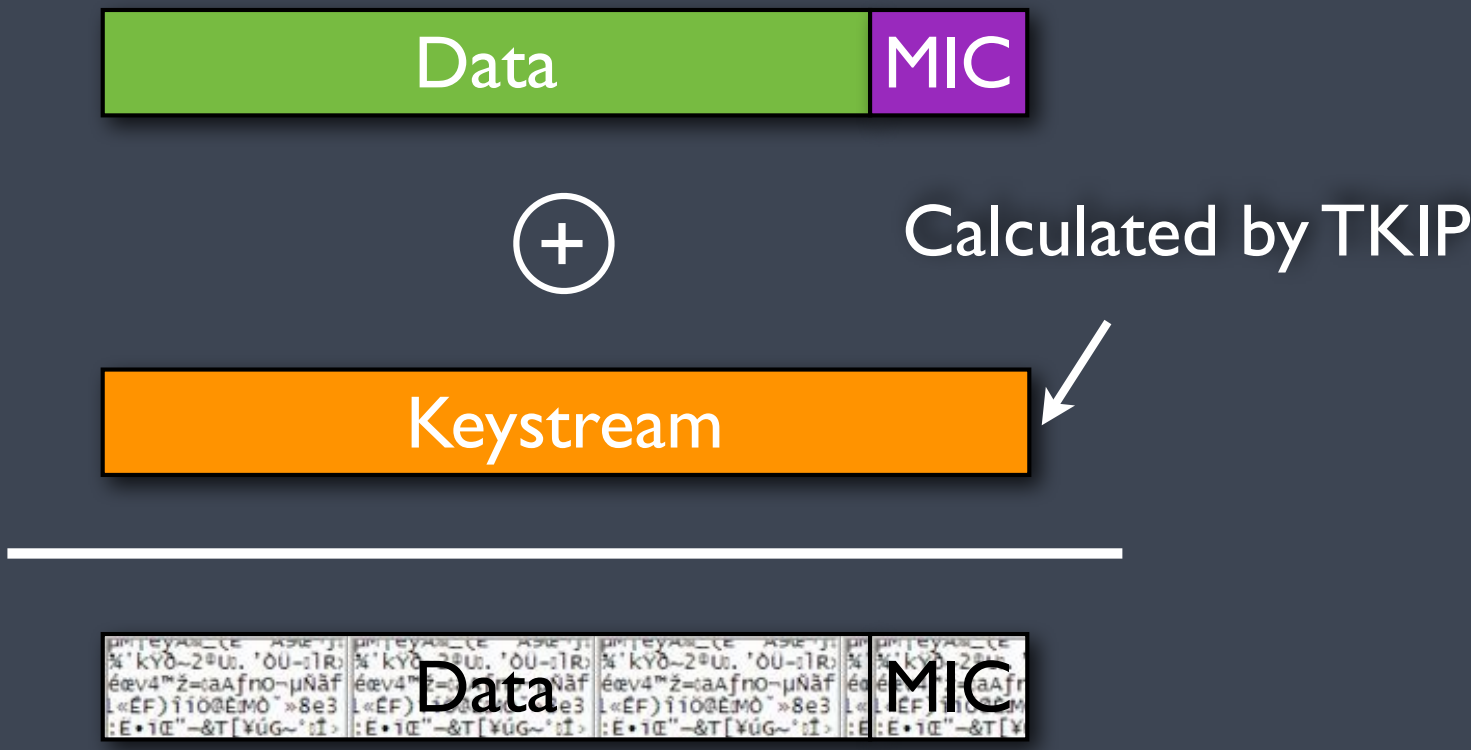
Basic Info…

Integrirty

New Integrity Control - MIC

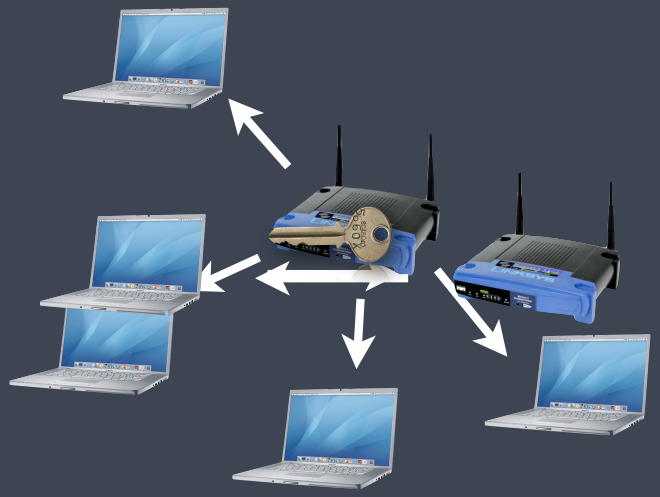


Confidentiality

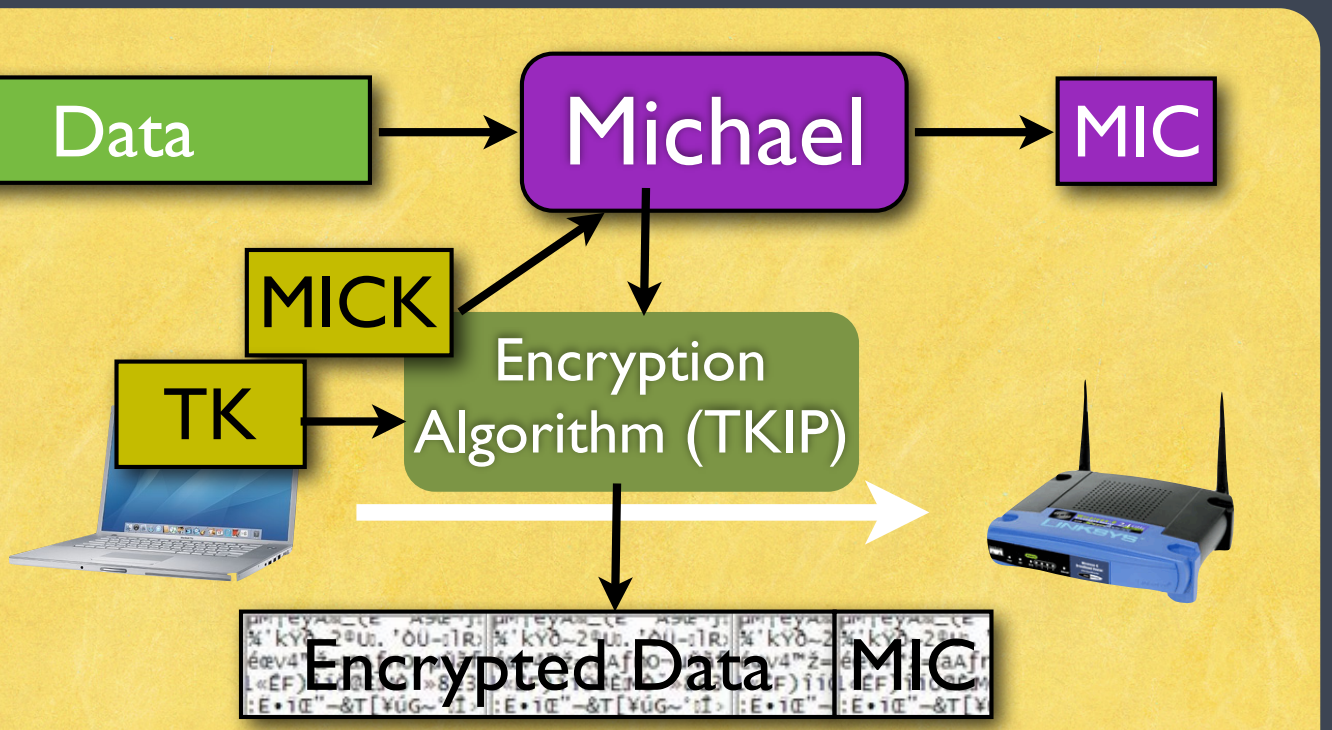


Three Types of Messages

- Unicast Messages
- Broadcast Messages
- Key exchange



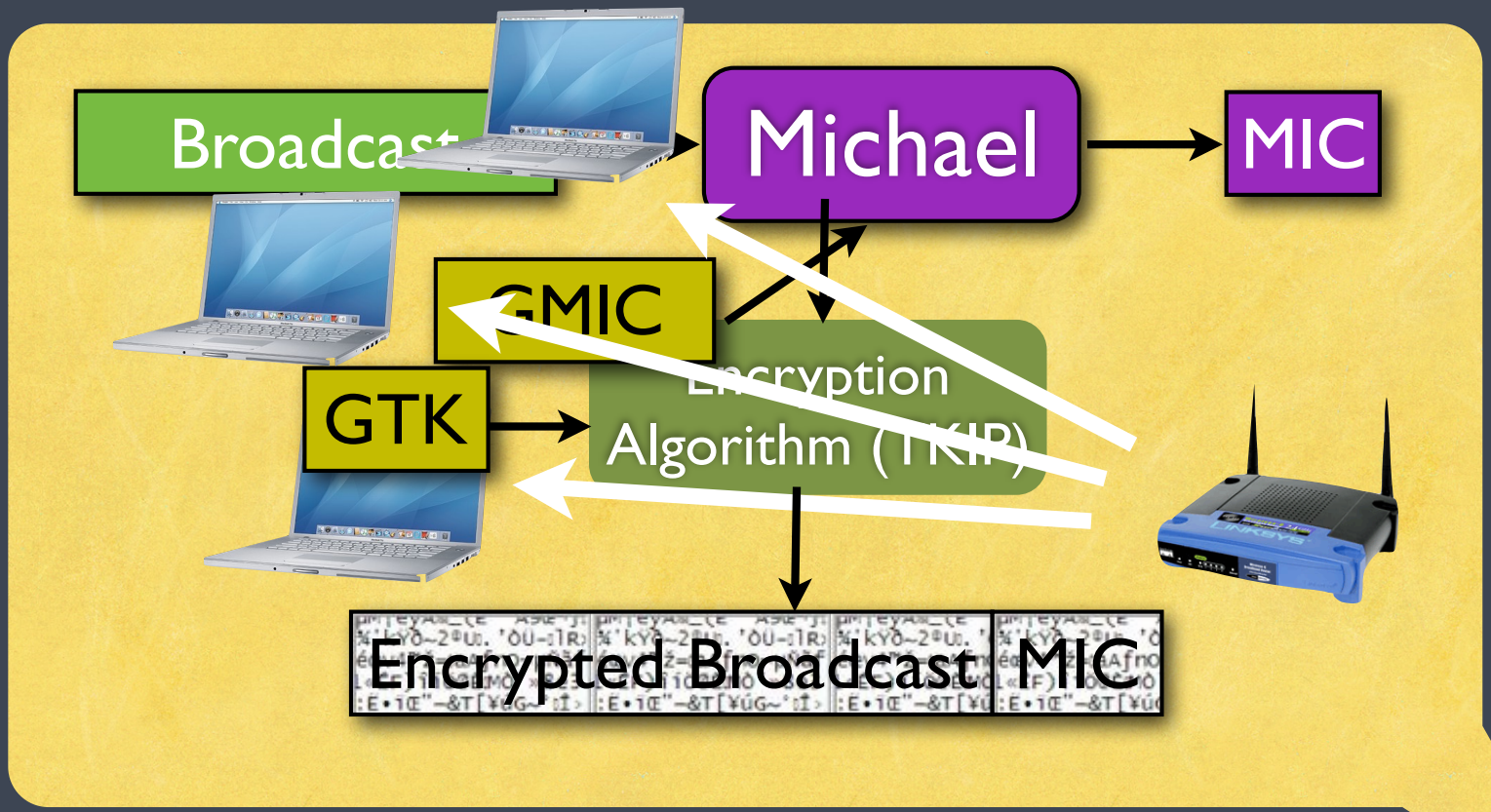
Unicast Messages (Pairwise)



Integrity :

Confidentiality :

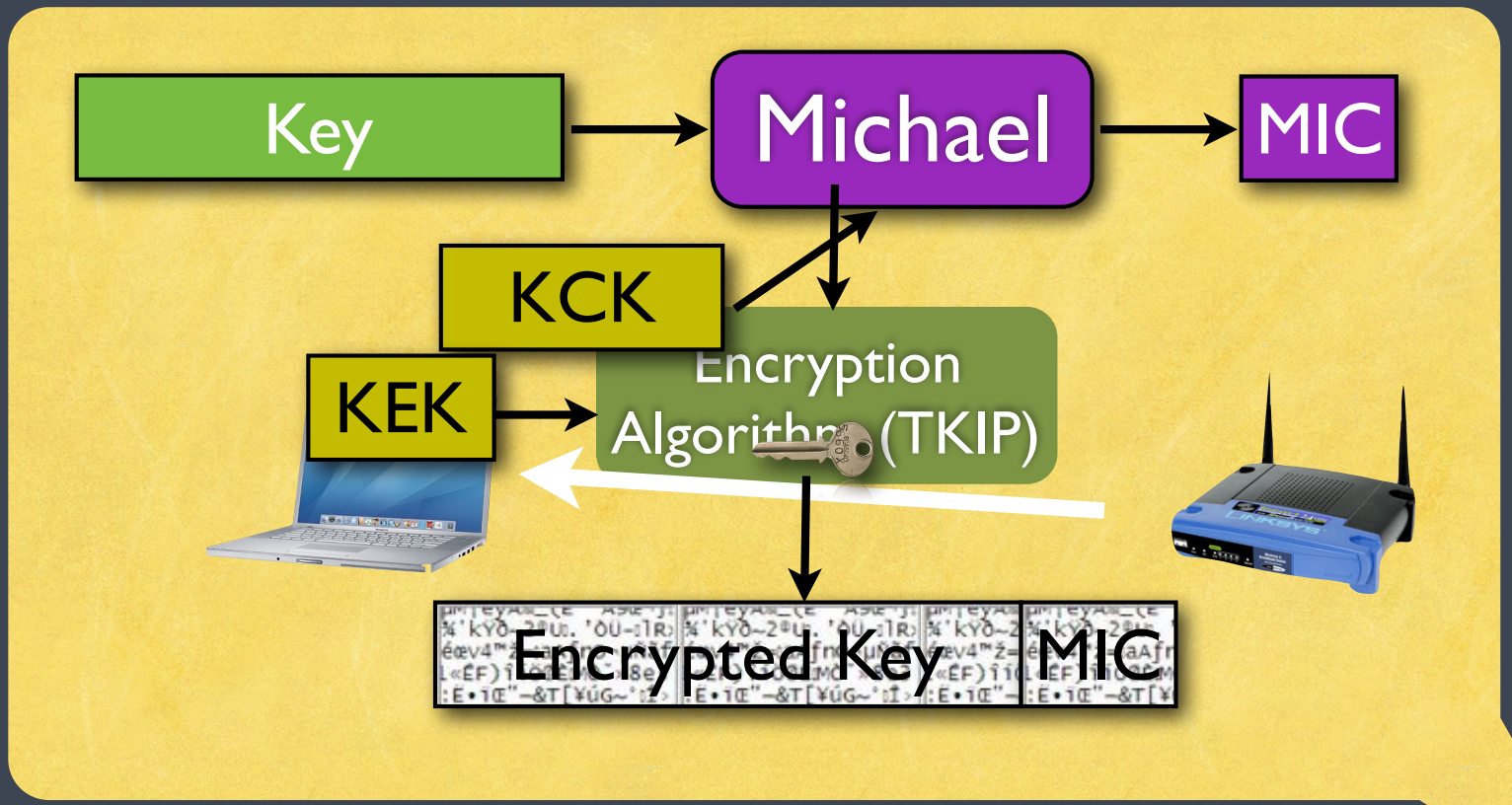
Groupe Messages (Groupwise)



Integrity :

Confidentiality :

Key Exchange



Integrity :

Confidentiality :

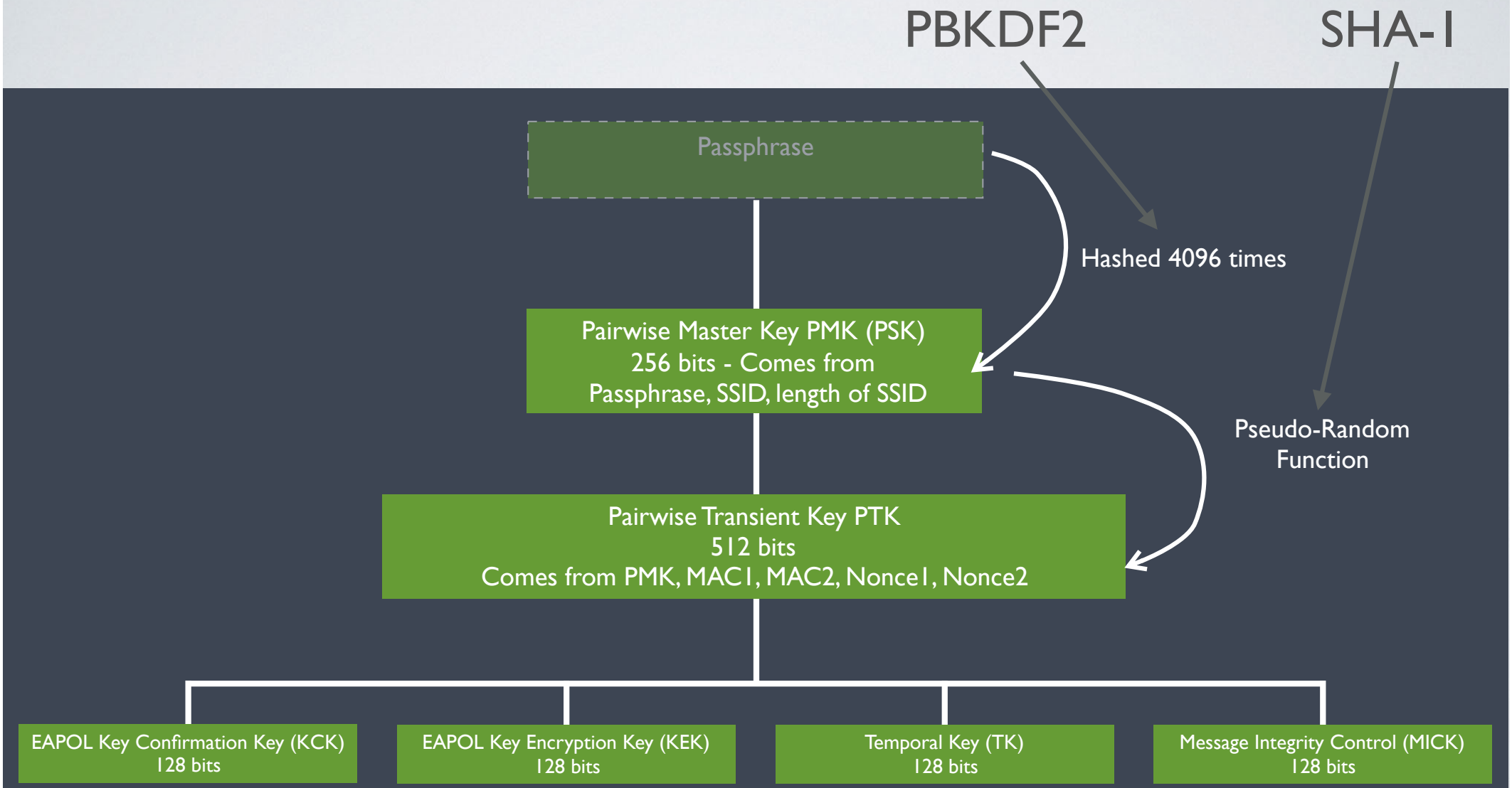
Question…

- How many keys do we need in order to send every type of message in WPA ?
  - Two for pairwise
  - Two for groups
  - Two for key exchange

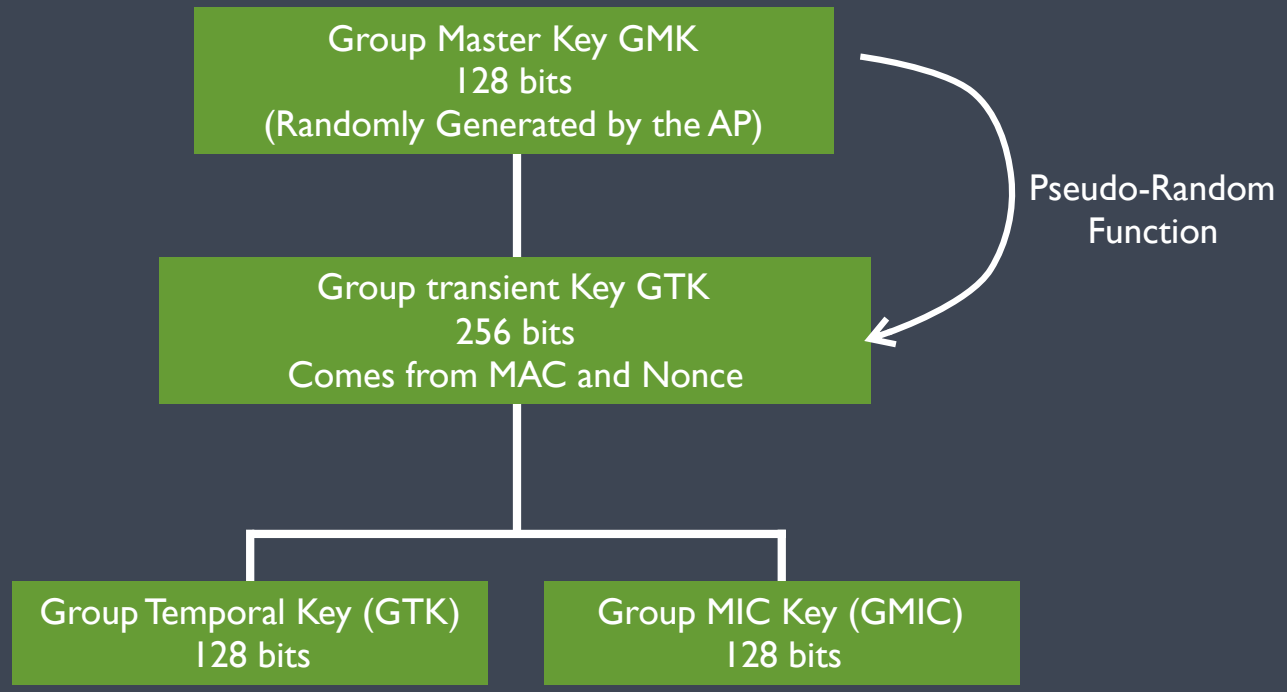
WPA Keys

Pairwise		Group		Key exchange	
Encryption	Integrity	Encryption	Integrity	Encryption	Integrity
TK	MICK	GTK	GMIC	KEK	KCK

Key Derivation



Group Key Derivation

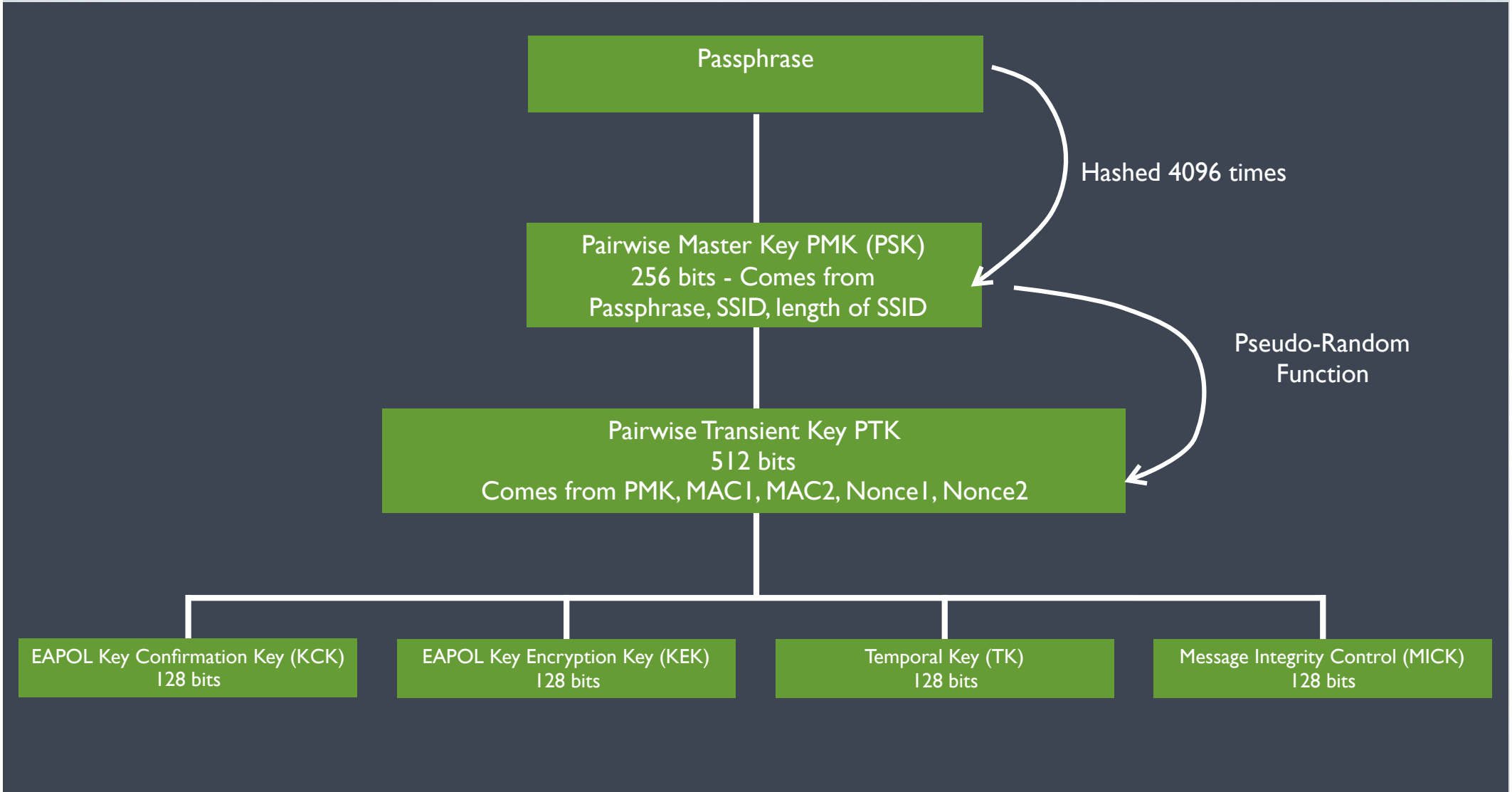


WPA Keys

- Pairwisse Master Key (PMK)
- Pairwisse Transient Key (PTK)
- Key Confirmation Key (KCK)
- Key Encryption Key (KEK)
- Temporal Key (TK)
- Message Integrity Control Key (MICK)

- Group Master Key (GMK)
- Group Transient Key (GTK)
- Group Temporal Key (GTK)
- Group MIC Key (GMIC)

Key Derivation



4-Way Handshake

Pairwise Transient Key PTK
Comes from PMK, MAC1, MAC2, Nonce1, No

Group Master Key GMK
(Randomly Generated by the AP)

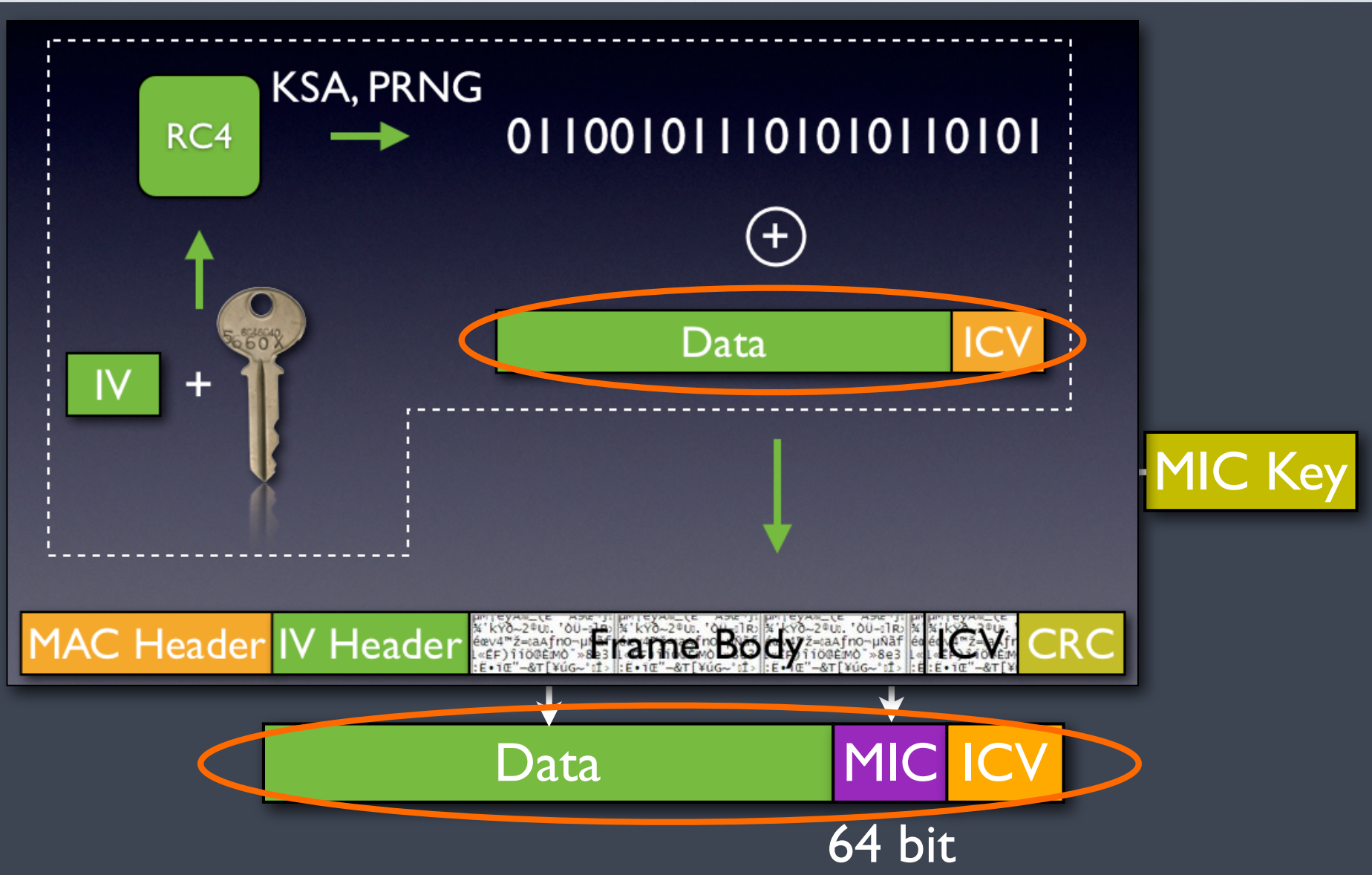
Authenticator Nonce

Supplicant Nonce authenticated (MIC) with the KCK

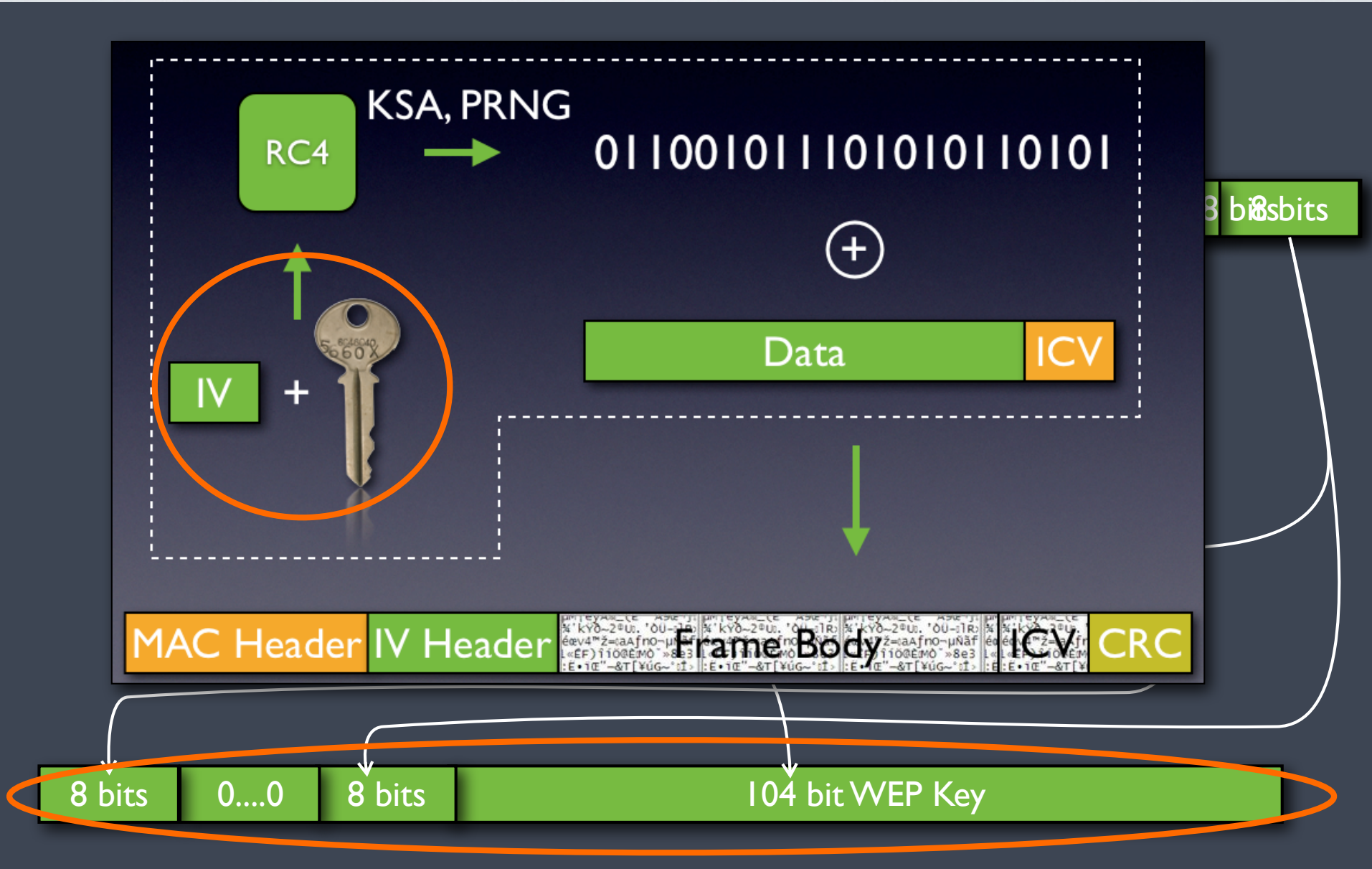
ACK + GTK encrypted with KEK and authenticated with KCK

ACK authenticated with KCK

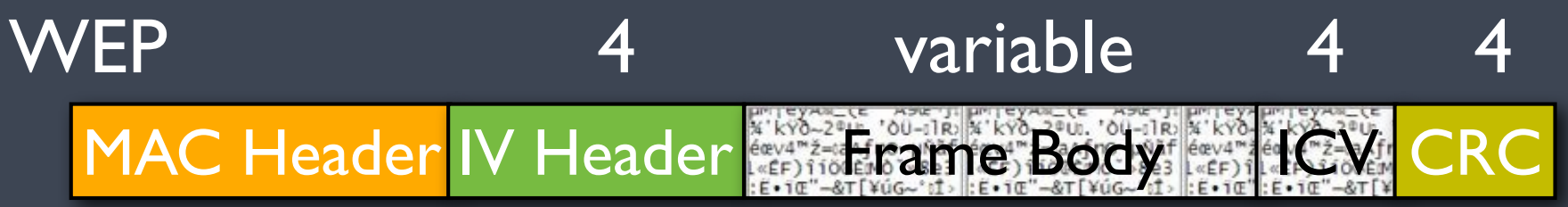
New Integrity Control - MIC



TKIP Algorithm



WEP Vs WPA

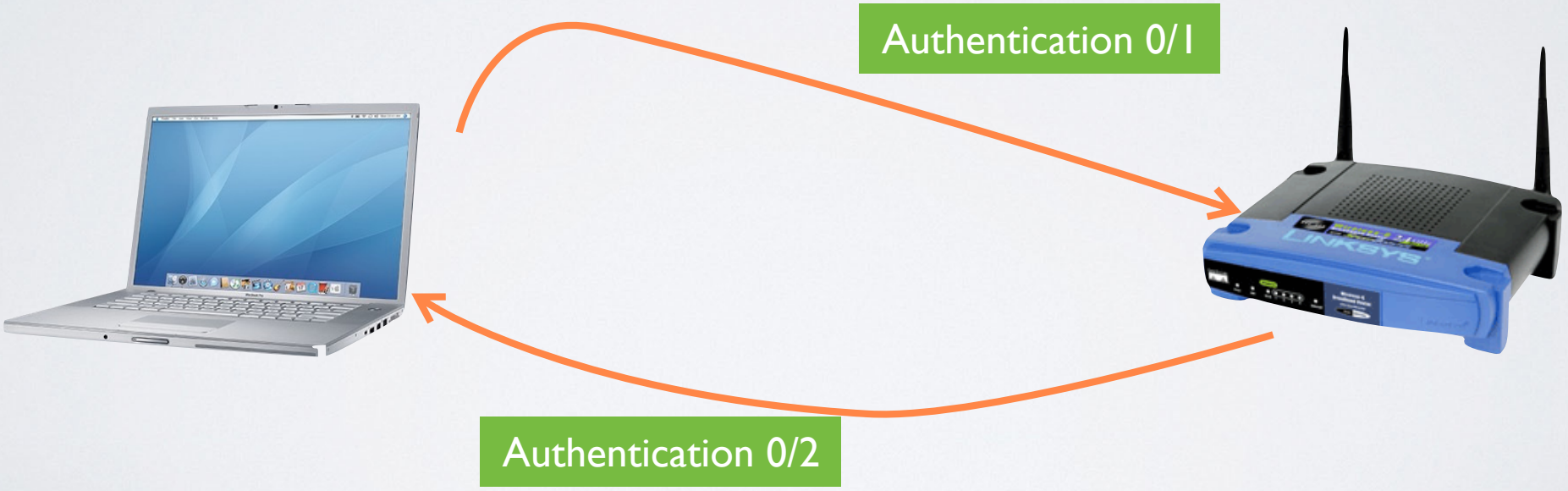

WEP
4
variable
4
4
MAC Header
IV Header
Frame Body
ICV
CRC


WPA
4
4
variable
8
4
4
MAC Header
IV Header
Ext. IV
Frame Body
MIC
ICV
CRC

Improvements of WPA

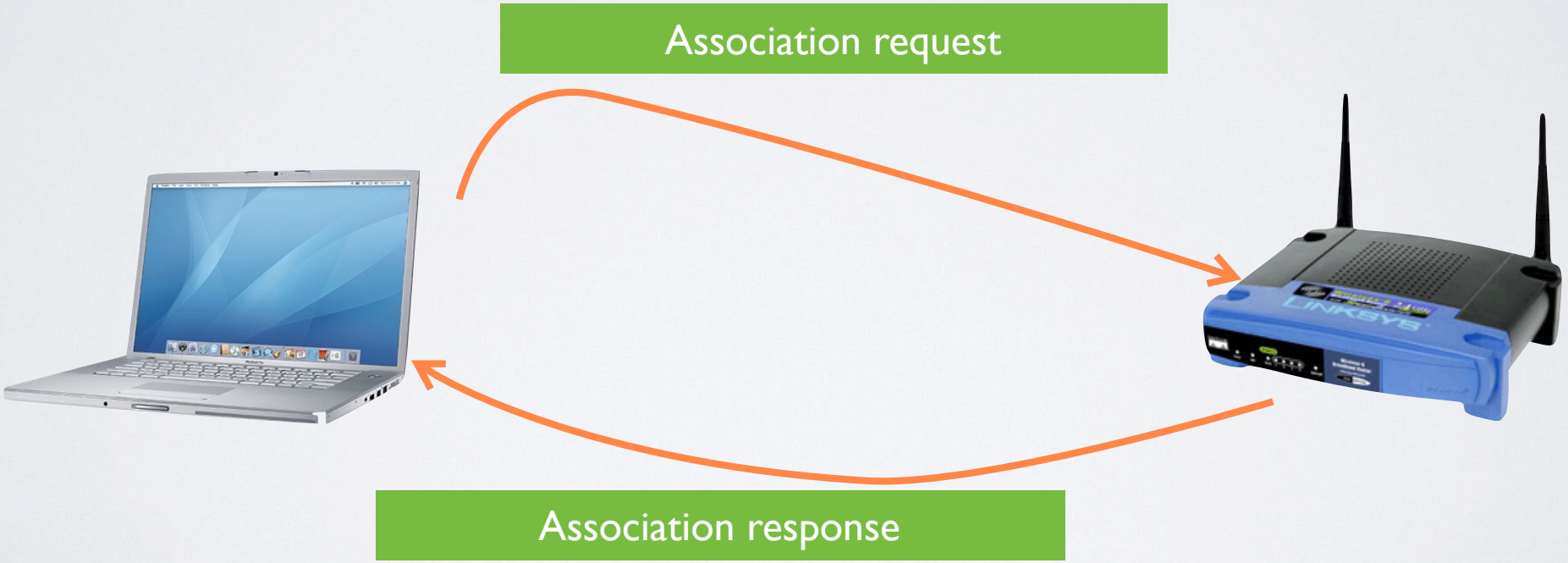
- TKIP (Temporal Key Integrity Protocol)
  - The IV does not repeat
  - The key for the calculation of the keystream depends on a sequence number and on MAC addresses
  - So… the key is **really** different for every frame
  - The MIC (Message Integrity Code) is much stronger than the ICV
- Mutual and improved authentication method

We Start With an Open System Authentication



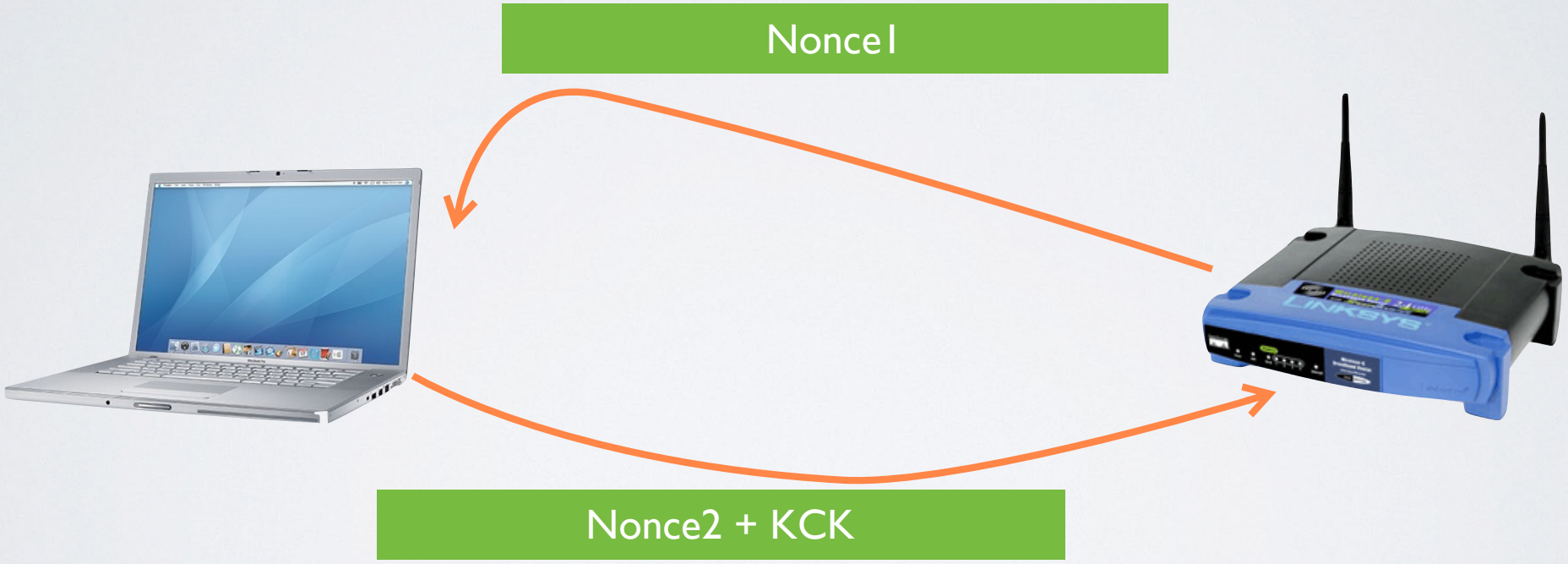
Association

…We Still Need To Do This…



New: Nonce Exchange

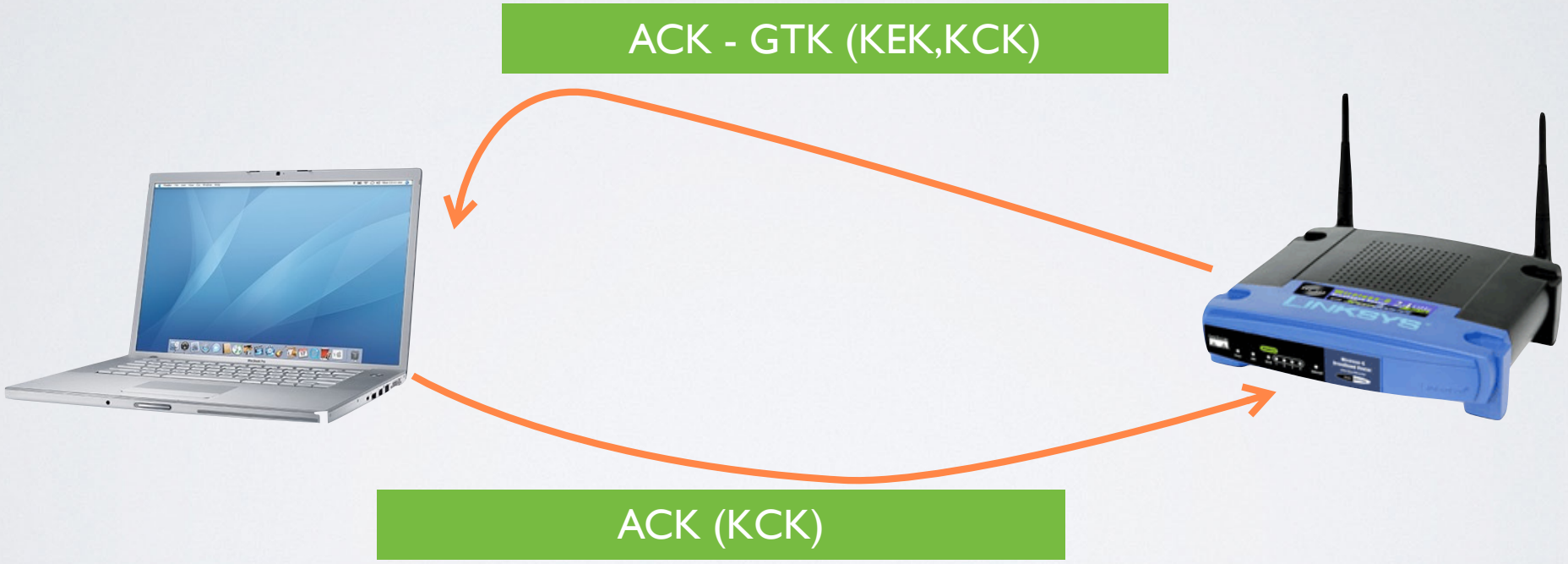
The STA derives keys from:
The secret shared key + Nonce1 + Nonce2



The AP authentifies the STA using the MIC and also derives the keys

New: Group Keys

The STA receives the GTK
The AP is now authenticated



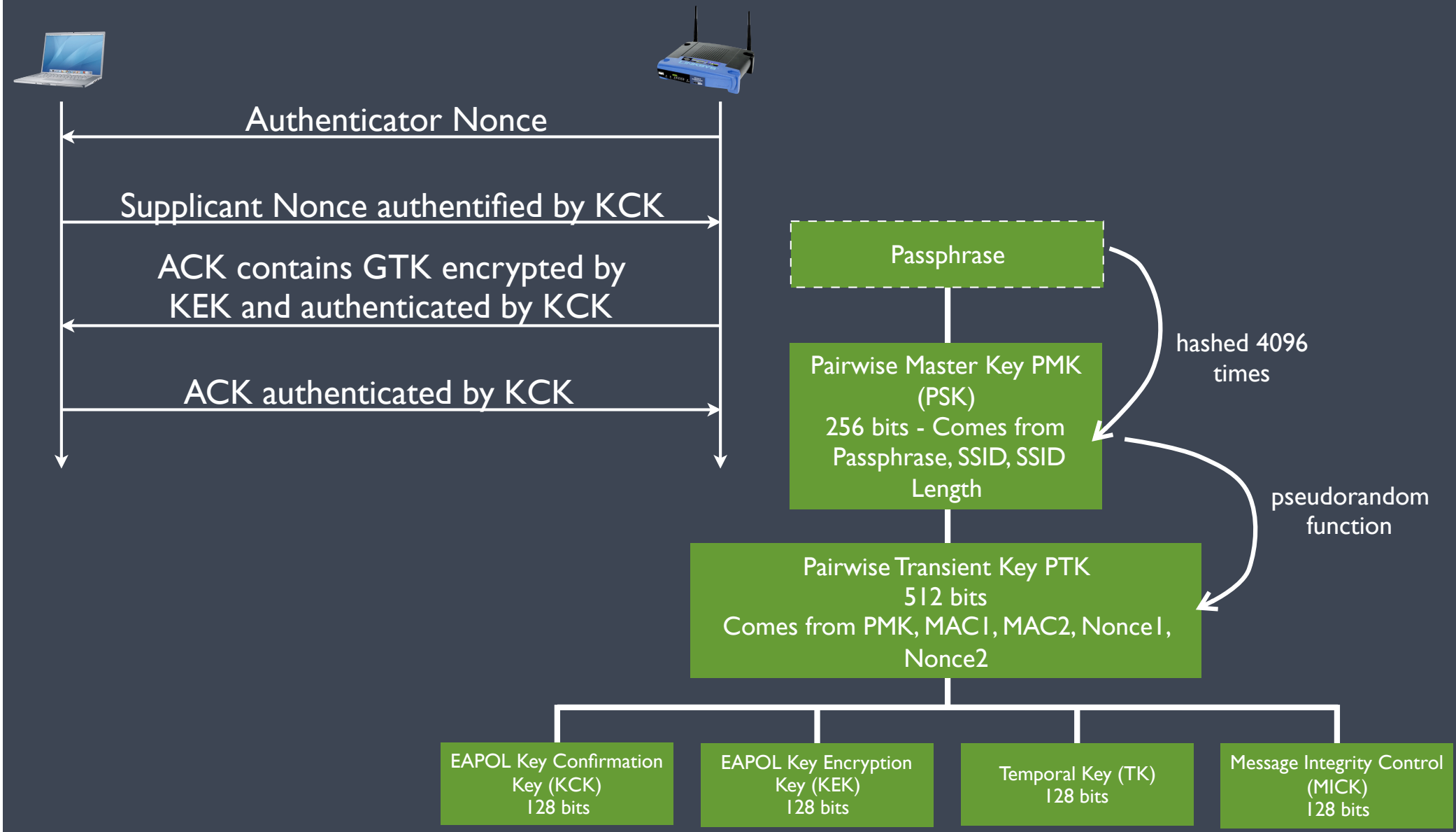
Really Good Security

… but not perfect…

Passive Attaque To Crack the WPA Passphrase

- The WPA handshake is designed to happen over non-secure channels and in clear text
- The only necessary step consists in capturing the authentication handshake between a legal STA and an AP
- If the handshake is captured, the rest of the attack can be performed offline. There's no need to capture any other traffic
- If no clients are connected, it is impossible to perform the attack
- If a client is already connected, a Deauthentication attack can be used to force and capture a new handshake
- Once the handshake is captured, a dictionary/brute force attack is the only way to crack WPA

Cracking WPA



MIC In TKP

- The MIC is calculated using the Michael Algorithm
  - With fast equipment, in a fast network, Michael can be brute-forced in minutes
- Solution: Limit brute-forcing attempts
  - After two fake MICs have been detected over a minute, the network should shut down for another minutes
  - Brute-forcing becomes impossible

Theoretical Fake MIC DoS

- Intercept a valid frame
- Modify the frame
  - Recalculate the ICV and the FCS (they are both CRC)
  - The MIC is no longer valid
- Replay the frame twice
  - The AP shuts down the network for 60 seconds
- Replay… and replay… and replay the same frame…

Solution

- Verify the elements of the frame in the right way
  - Verify the FCS (in an attack, in will pass the test)
  - Verify the ICV (in an attack, in will pass the test)
  - But... do not verify the MIC… no yet!
- Remember, the IV is now a sequence counter
  - The counter will be wrong
  - Ignore the frame