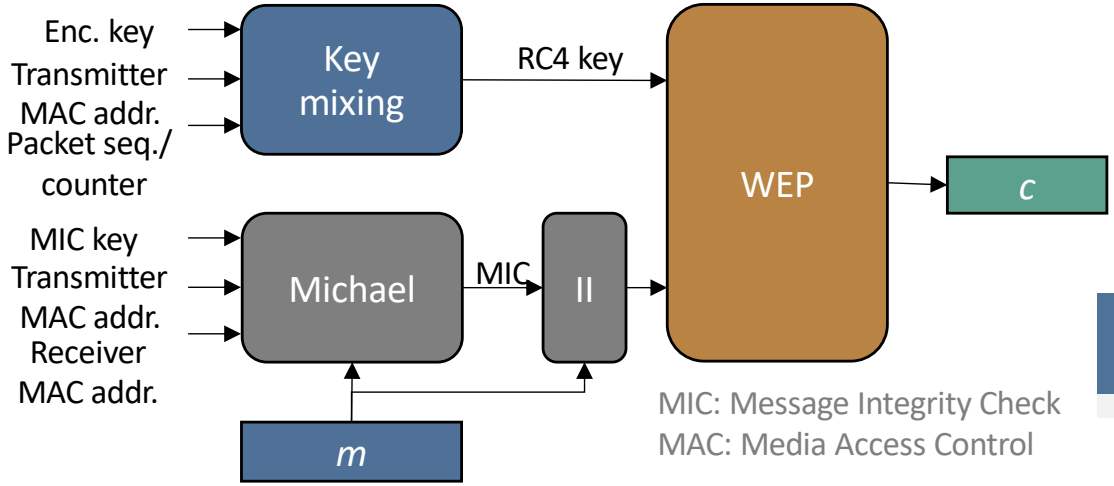
deprecated
(2014)

IEEE 802.11i-draft
(2003)

| Sizes | |
|---|---|
| | *Packet seq.: 48 bits* |
| | *MIC: 64 bits* |

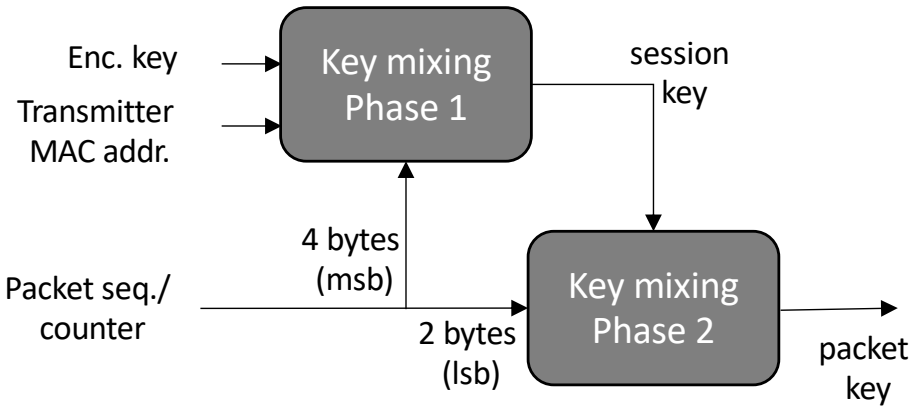



MIC: Message Integrity Check
MAC: Media Access Control

KCK: Key Confirmation Key
KEK: Key Encryption Key
TK: Temporal Keys



## *Key Mixing*




- + *Integrity*: MIC instead of CRC
- + *Lengths*: larger (e.g., Packet seq. vs. IV)
- + *Key management*: key per package (packet no. to avoid replay attacks)
- − *Attacks*

## *Temporal Key Integrity Protocol (TKIP)*

***Pairwise Master Key - PMK (256 bits)***

*Pairwise Transient Key PTK (512 bits)*

| *EAPOLMICKey (128 bits)* (KCK) | *EAPOLEncKey (128 bits)* (KEK) | *DataEncKey (128 bits)* | *DataMICKey (128 bits)* (TK) |
|---|---|---|---|

TKIP Pairwise Key Hierarchy

$$PTK = f(PMK, NonceAP, NonceSTA, MAC_{AP}, MAC_{STA})$$

***Group Master Key - GMK (128 bits)***

*Group Transient Key GTK (256 bits)*

| *DataEncKey (128 bits)* | *DataMICKey (128 bits)* |
|---|---|

TKIP Group Key Hierarchy

$$GTK = f(GMK, NonceAP, MAC_{AP})$$