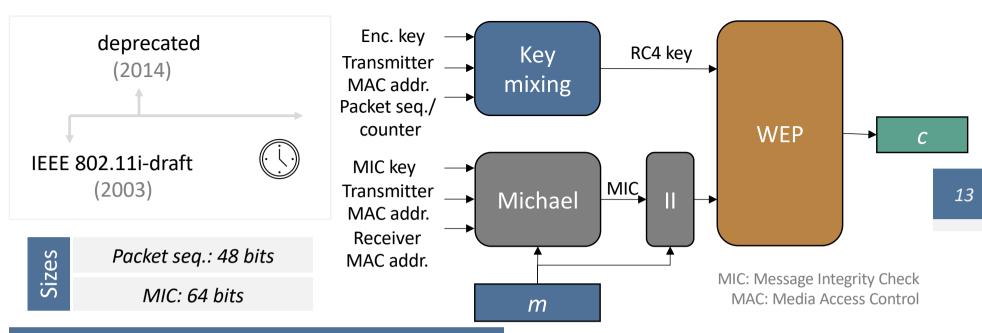
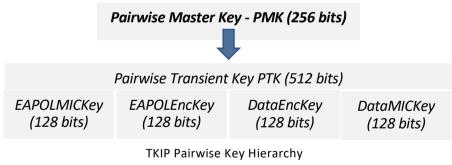
www.ruxandraolimid.weebly.com/pagesonsecurity



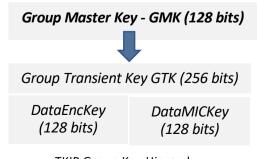
Key Mixing session Enc. kev Key mixing key Transmitter Phase 1 MAC addr. 4 bytes (msb) Key mixing Packet seq./ 2 bytes Phase 2 counter packet (Isb) key Integrity: MIC instead of CRC

- 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)



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



TKIP Group Key Hierarchy $GTK = f(GMK, Nonce_{AP}, MAC_{AP})$ **Pages on SecuRity** by Ruxandra F. Olimid