# 802.11i

Giulio Oliveira
Lucas Gomes
Walter Freitas Jr.

# Histórico

- 802.11-1997
  - Primeiro padrão de redes sem fio
  - Segurança através de WEP
    - Wired Equivalent Privacy
  - WEP demonstra falhas em 2001 envolvendo o seu uso do RC4-Stream Cipher
  - Atualmente ele pode ser quebrado em alguns minutos usando hardware padrão e softwares livres

# Histórico

- Pré 802.11i – WPA (Wi-Fi Protected Access)
  - Projeto de Implementação
    - WPA implementou um subset das especificações do padrão 802.11i
  - Substituiu WEP com WPA-TKIP em 2003
    - Compatibilidade reversa, maioria dos wireless cards podem ser atualizados via firmware
  - Suscetibilidade a quebra descoberta
    - Envolve o uso da cifra RC4 pelo algoritmo TKIP.

# WPA2

- 802.11i – WPA2
  - Implementação total do padrão
    - Adotado em 2004
  - Substituiu WPA com WPA2-AES (Advanced Encryption Standard) in 2004
    - Compatível com WPA
  - AES-CCMP
    - Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
  - Provê RSN (Robust Security Network)

# Introdução

- A criptografia em WPA2 é feita via AES ou TKIP, e a autenticação usa um dos 2 modos a seguir (de acordo com o padrão 802.1x):
- O modo pessoal utiliza uma PSK (Chave pré-compartilhada) e não requer uma autenticação separada dos usuários
- O modo empresarial requer que os usuários sejam autenticados separadamente com o uso do EAP (Extensive Authentication Protocol)

# Introdução

| | 802.1x Dynamic WEP | Wi-Fi Protected Access (WPA) | Wi-Fi Protected Access 2 (WPA2) |
|---|---|---|---|
| Access Control | 802.1X | 802.1X or Pre-Shared Key | 802.1X or Pre-Shared Key |
| Authentication | EAP methods | EAP methods or Pre-Shared Key | EAP methods or Pre-Shared Key |
| Encryption | RC4 | TKIP (RC4) | AES / TKIP |

# Introdução

- WPA2 estabelece uma comunicação segura em 4 etapas:
- Fase 1: O AP e o cliente estabelecem uma política de segurança, de acordo com o RSN (método de autenticação e pré-autenticação)
- Fase 2: Geração da Master Key (MK)
- Fase 3: Criação de Temporal Keys em intervalos regulares
- Fase 4: Todas as chaves geradas na fase 3 são utilizadas pelo protocolo CCMP para prover integridade e confidencialidade de dados

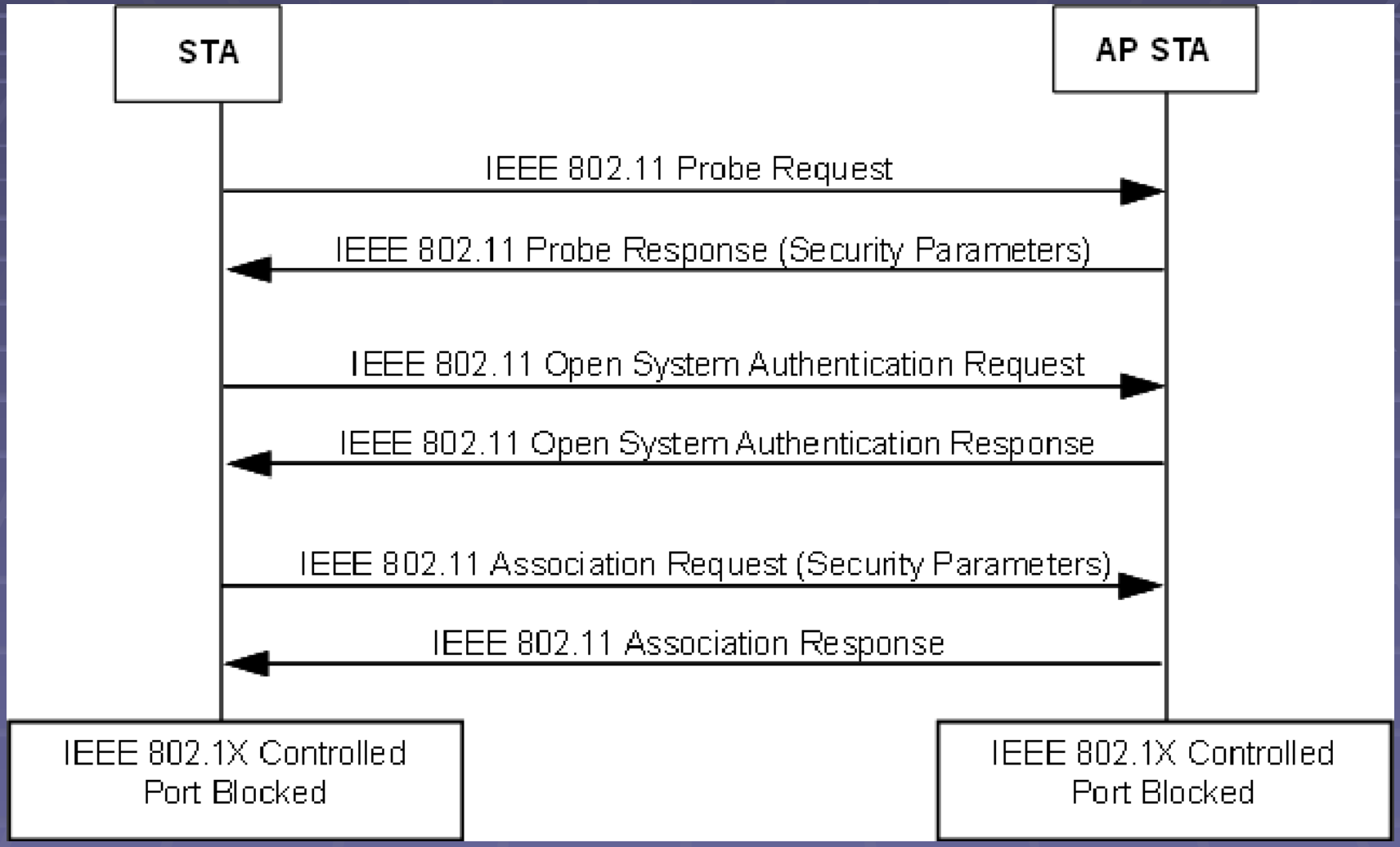
# Robust Security Network via padrão 802.1X

- RSN é um elemento que negocia dinamicamente a autenticação e o algoritmo de criptografia a ser usado na comunicação entre os clientes e os APs.
- A cada ameaça descoberta, novos algoritmos podem ser adicionados (future-proof).
- Usa o AES, junto do padrão 802.1x e o EAP

# Robust Security Network via 802.1X

- Três atores são utilizados para executar o protocolo 802.1X
  - Um client (STA/Supplicant)
  - Um wireless access point (AP STA ou Autenticador)
  - Um servidor de autenticação (opcional) (AS)

# Robust Security Network via 802.1 X



# Robust Security Network via 802.1X

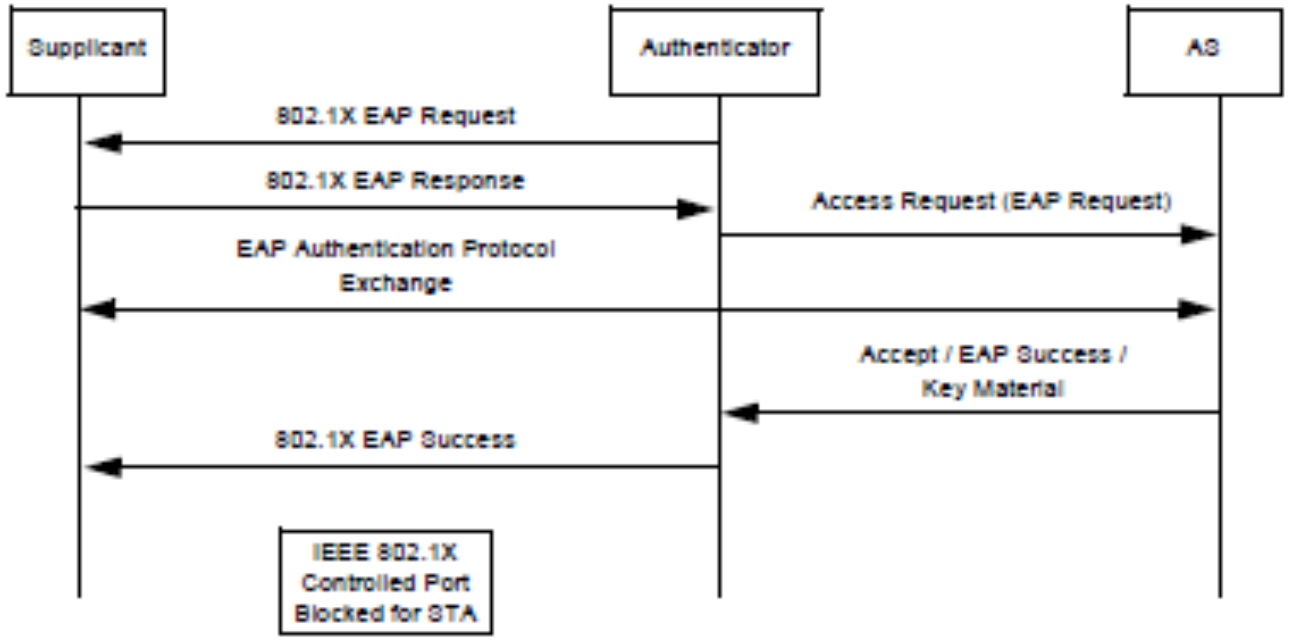



Figure 11b—IEEE 802.1X EAP authentication

# Robust Security Network via 802.1X

- **Master Session Key – MSK ou MK**
- Chave simétrica que é a fonte da geração das chaves subsequentes nas decisões de acesso
- Somente o cliente e o AS têm posse dela
- A decisão para autorização é baseada no MK

# Robust Security Network via 802.1 X

- PMK – Pairwise Master Key
  - Derivado da  Master Key
  - Enviado do AS para o Autenticador
  - PMK é permanente por toda a sessão e é utilizado para gerar chaves de criptografia, e não para criptografar os dados
    - Deve ser gerado um Pairwise Transient  Key para criptografia de dados.
      - Isto é feito usando o 4-way handshake

# Robust Security Network via 802.1X

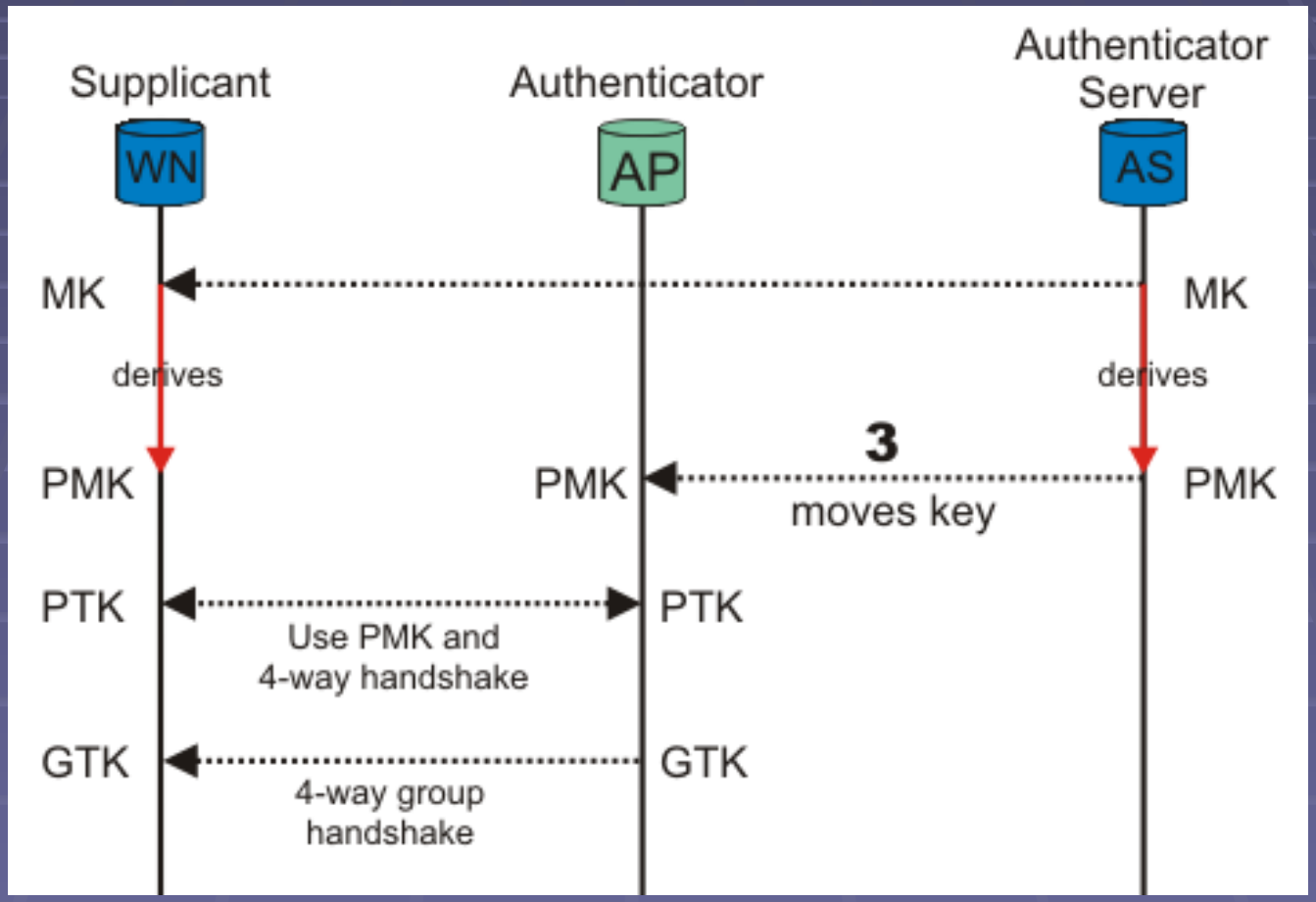
- PTK – Pairwise Transient Key
- Derivado da PMK
- Criptografa frames unicast com o cliente

- GTK – Groupwise Transient Key
- Derivado pela GMK (Group Master Key)
- Criptografa frames de broadcast/multicast neste específico

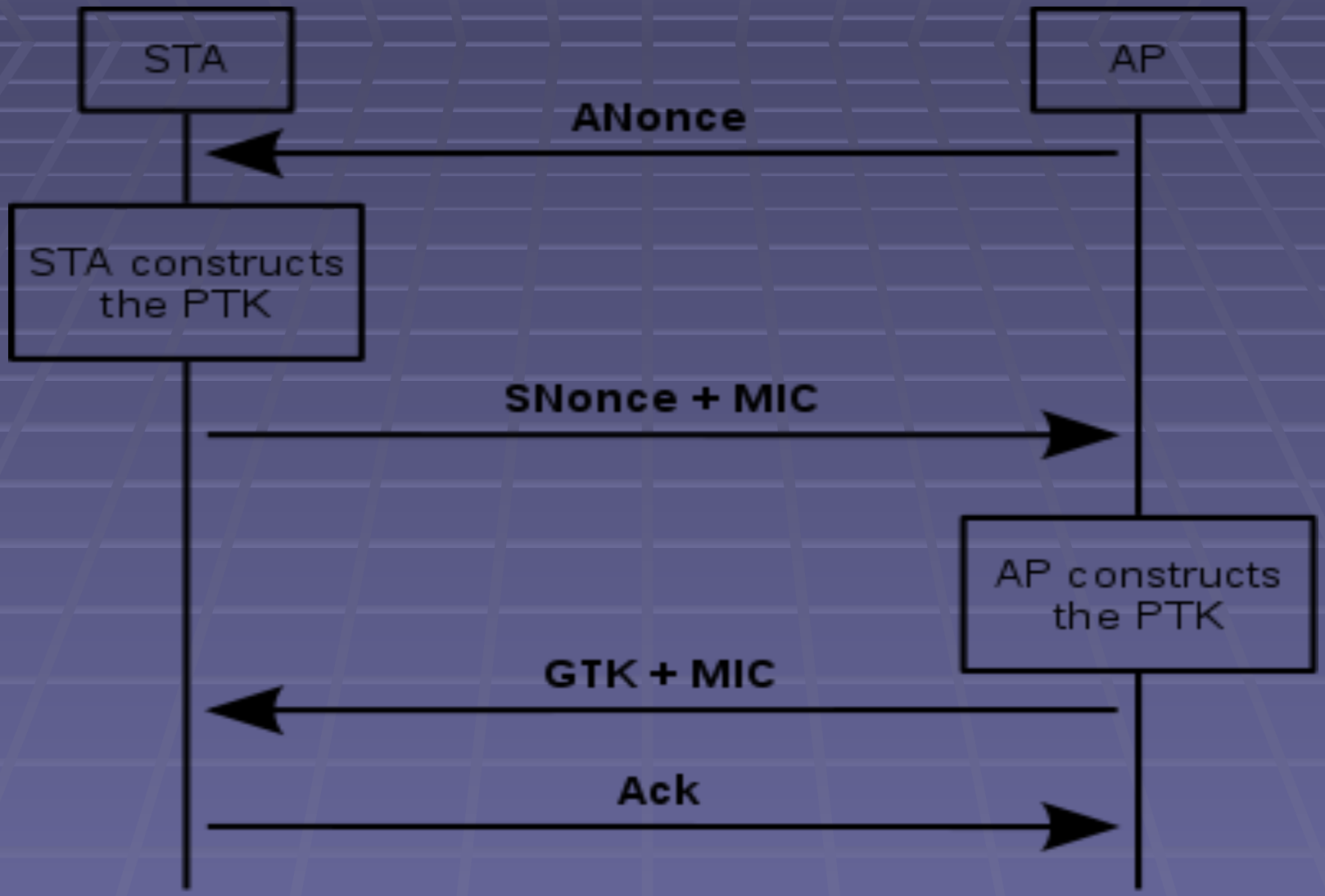
# Robust Security Network via 802.1 X

- 4-Way Handshake
- AP envia ANonce (valor aleatório) para estação,  que gera o PTK baseado nesta e em outras informações
- Estação devolve com SNonce + MIC (mensagem criptografada) para que o AP (autenticador) também construa o PTK
- AP envia GTK + MIC para transmissões criptografadas em broadcast / multicast
- ACK para confirmação da instalação do PTK e GTK

# Robust Security Network via 802.1X



# Robust Security Network via 802.1X



# Robust Security Network via 802.1 X

- Nonce
  - Um valor que não deve ser reutilizado com uma dada chave, incluindo todas as reinicializações do Sistema através do tempo.
- Message Integrity Code (MIC)
  - Provê uma integridade das mensagens mais segura contra ataques, substitui o CRC utilizado no WEP

# WPA2-PSK – Modo Pessoal

- Modo de chave pré-compartilhada
  - Tráfego de rede criptografado utilizando uma PMK de 256 bits
  - Usuário entra com chave (Pairwise Master Key)
    - 64 dígitos hexadecimais
    - 8-63 caracteres printáveis ASCII

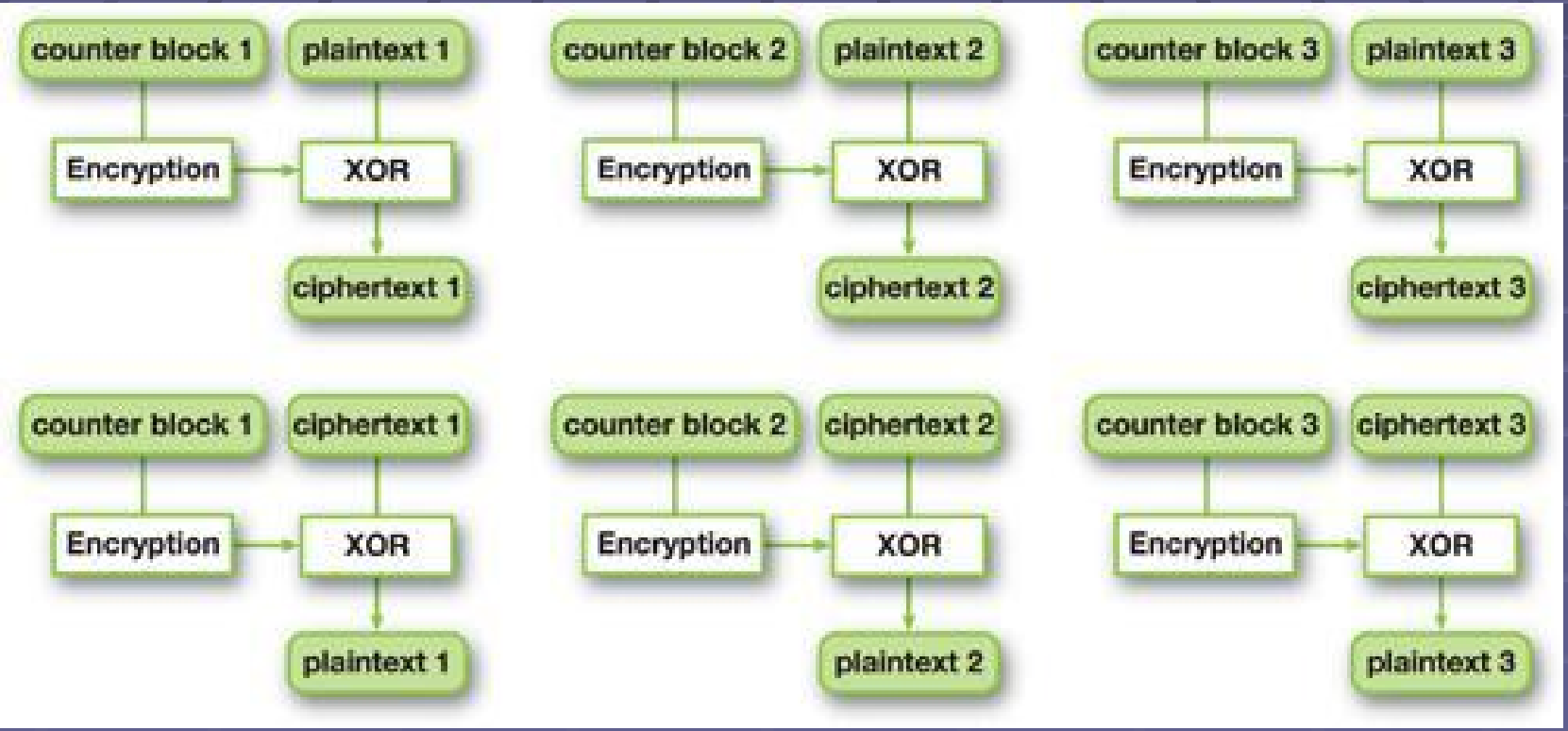
# WPA2-PSK – Modo pessoal

- Autenticação, Conexão, e Estabelecimento do PTK e GTK.
  - Procedimento semelhante a quando o AS está presente, exceto que o PSK é usado como PMK.

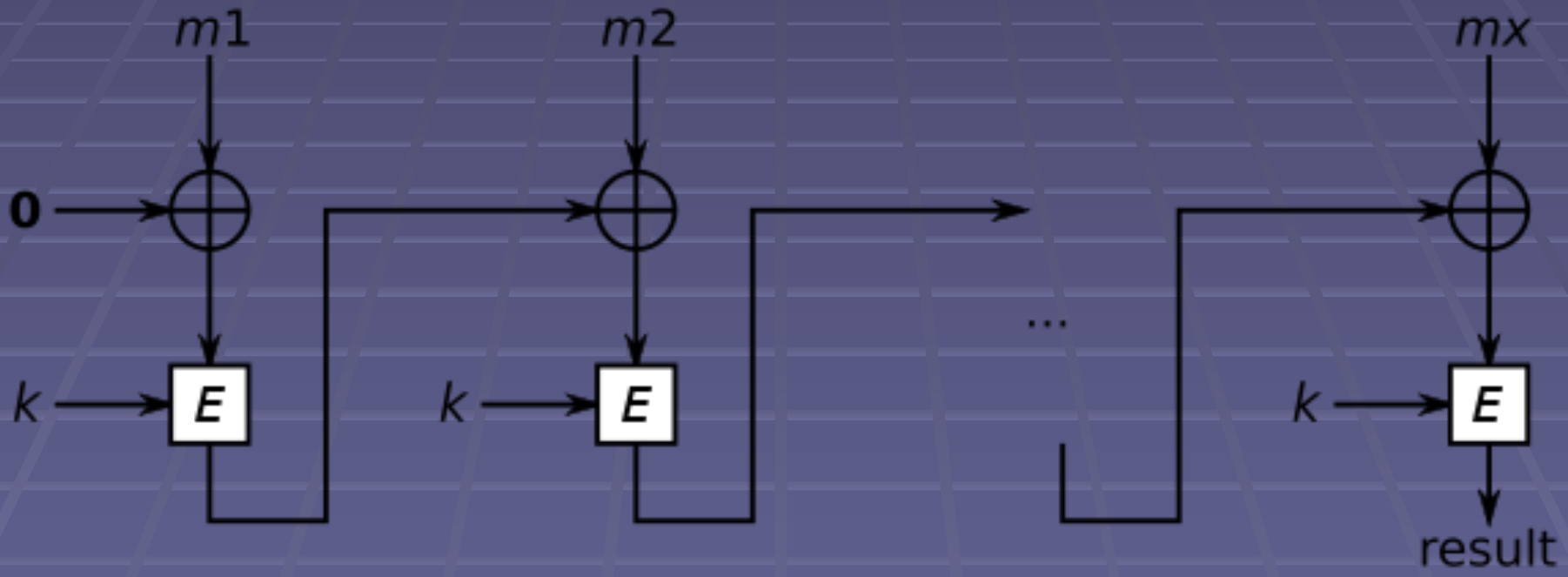
# Criptografia de Dados via AES-CCMP

- (AES-Counter Mode CBC-MAC Protocol) Algoritmo de criptografia usado no protocolo de segurança do 802.11i. Faz uso da cifra de bloco AES.
- AES-CCMP incorpora 2 técnicas criptográficas sofisticadas (counter-mode e CBC-MAC) e as adapta aos frames Ethernet para prover um protocolo robusto de segurança entre a estação móvel e o AP.
- AES por si só é uma cifra muito forte, e o counter mode torna difícil para um interceptador observer padrões, além do método de integridade de mensagem CBC-MAC assegura que mensagens não foram adulteradas.

# Counter Mode (CTR Mode)



# CBC-MAC



Obrigado pela atenção!!!