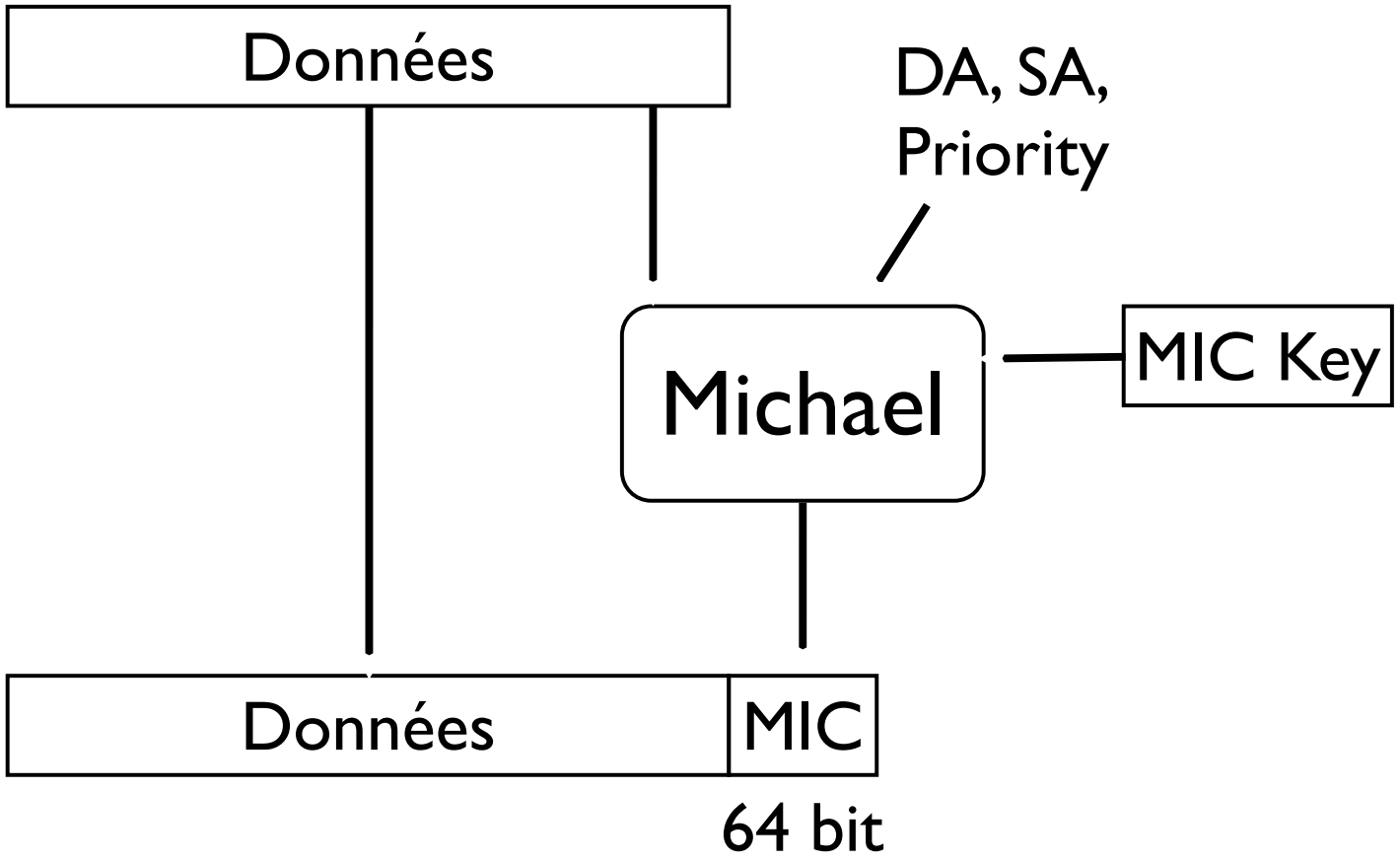
WPA

- Nouvel Integrity Check
  - Protégé cryptographiquement
  - 64 bits
- Utilise la PSK d'une manière très différente
- L'IV mesure maintenant 48 bits
  - Compteur de séquence
  - $2.81474977 \times 10^{14}$ combinaisons
  - La clé n'est jamais réutilisée, même si l'IV est réutilisé

Nouvel Integrity Check Value - MIC

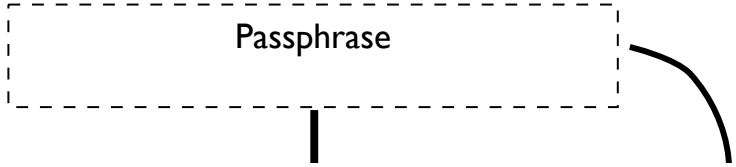


Les “clés” WPA (key)

- 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)

Dérivation des clés hiérarchiques



MASTER

TRANSIENT

TEMPORAL

Les “clés” WPA (key)

- Pairwisse Master Key (PMK)
- Pairwisse Transient Key (PTK)
- Key Confirmation Key (KCK)
- Key Encryption Key (KEK)
- Temporal Key (TK)
- Message Integrity Control Key (MIC)
- Group Master Key (GMK)
- Group Transient Key (GTK)
- Group Temporal Key (GTK)
- Group MIC Key (GMIC)

Dérivation des clés hiérarchiques de groupe

MASTER

TRANSIENT

TEMPORAL

L’utilisation des clés

Par paires		Groupe		Clés	
Chiffrement	Intégrité	Chiffrement	Intégrité	Chiffrement	Intégrité
TK	MICK	GTK	GMIC	KEK	KCK

4-way handshake

Pairwise Transient Key PTK
Vient de PMK, MAC1, MAC2, Nonce1, Nonc

Group Master Key GMK
(Généré aléatoirement par l'AP)

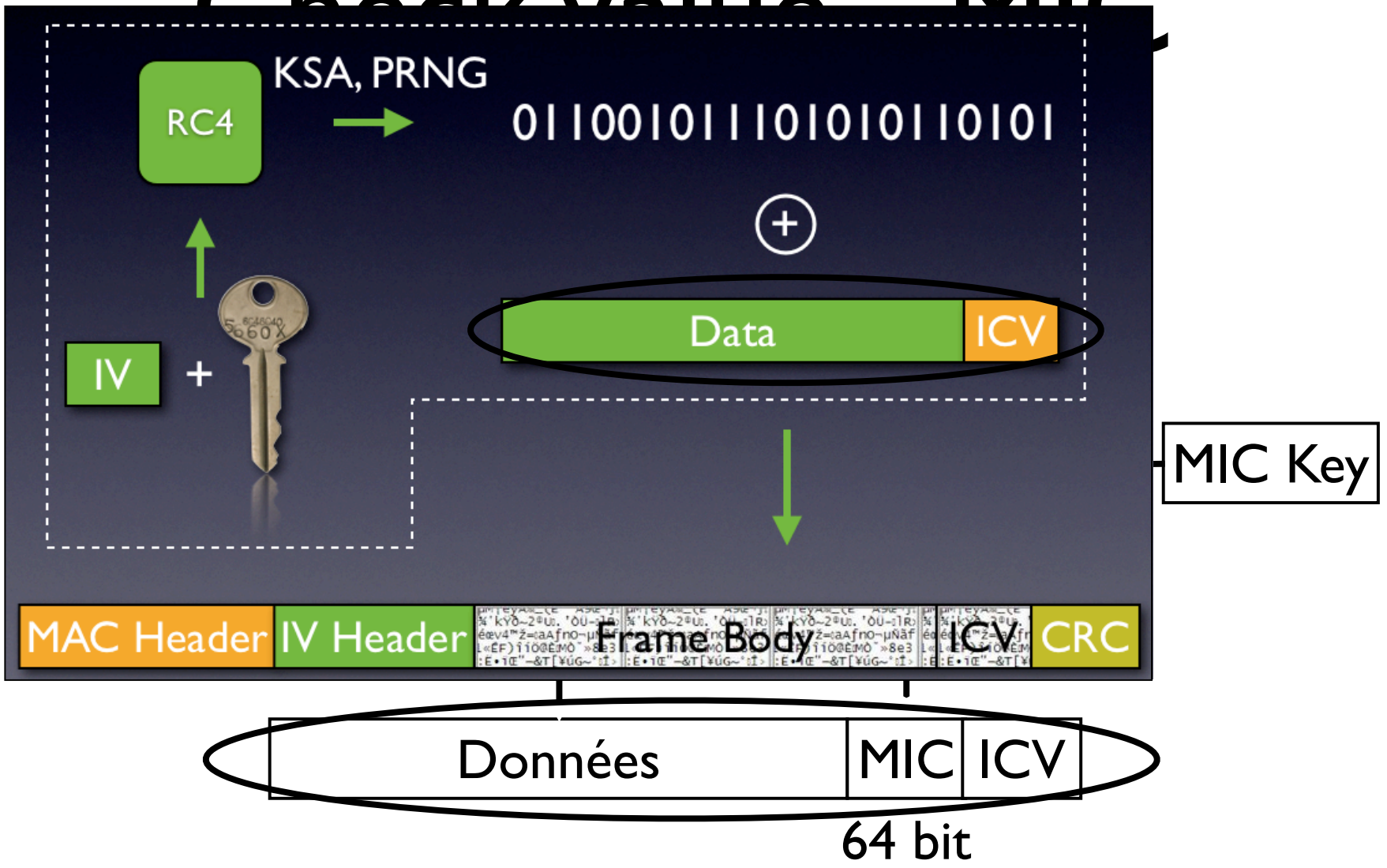
Nonce de l'authentificateur

Nonce du suppliant authentifié par la KCK

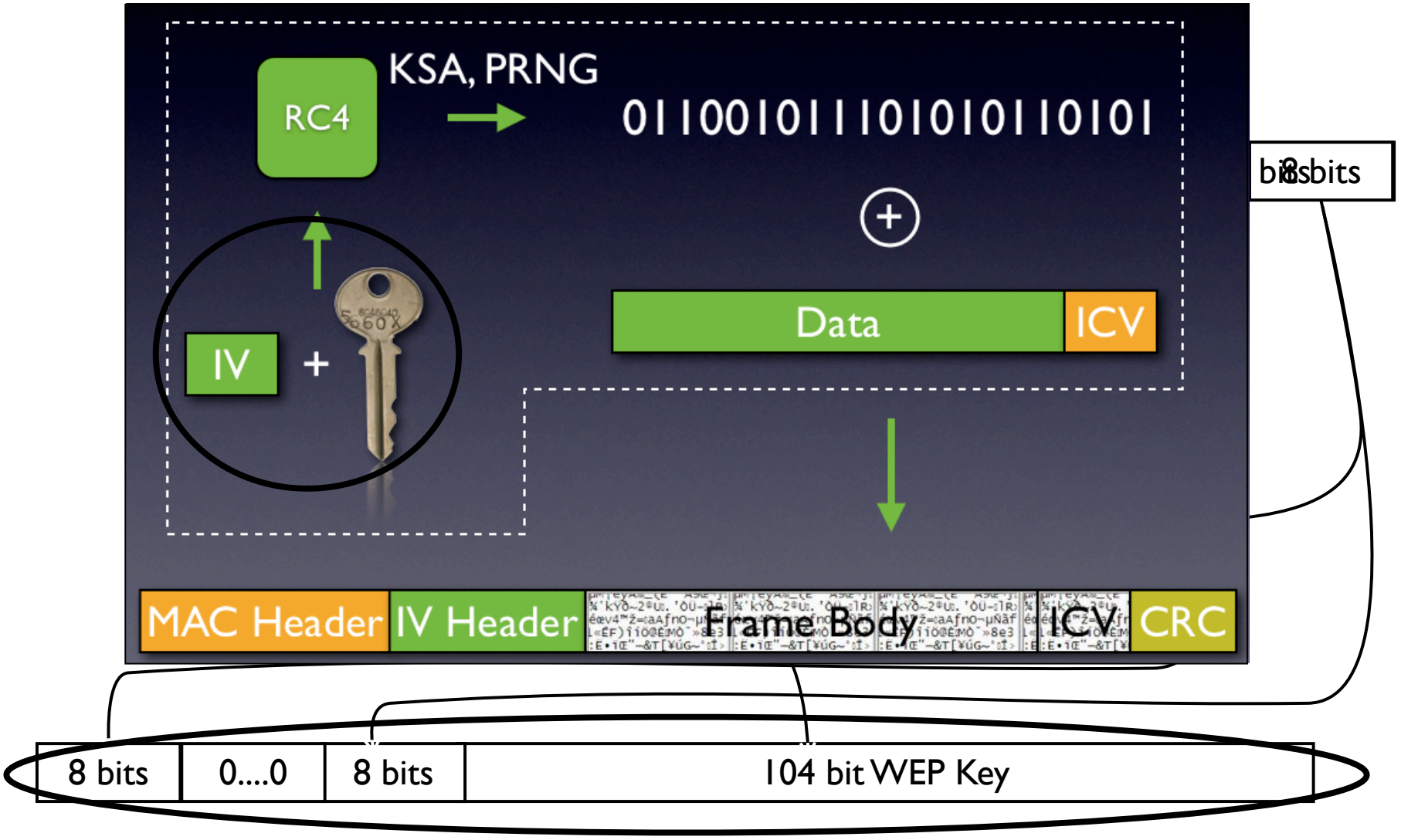
ACK contient GTK chiffré par KEK et authentifié par KCK

ACK authentifié par KCK

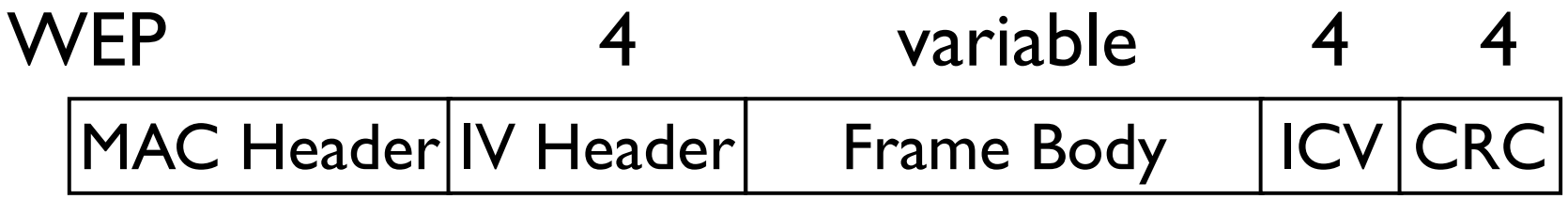
Nouveau Integrity CheckValue - MIC

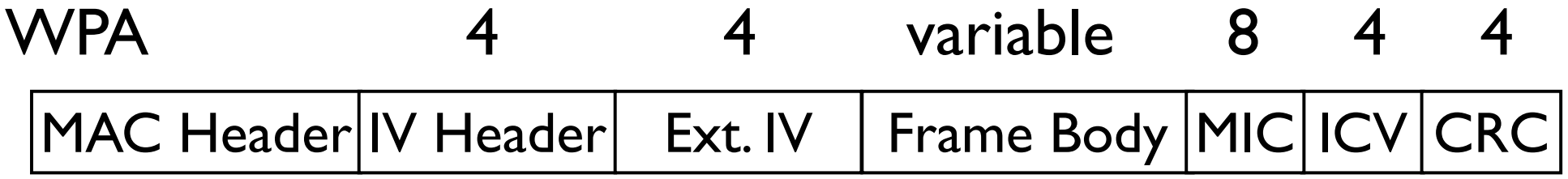


L'algorithm TKIP



WEP vs. WPA

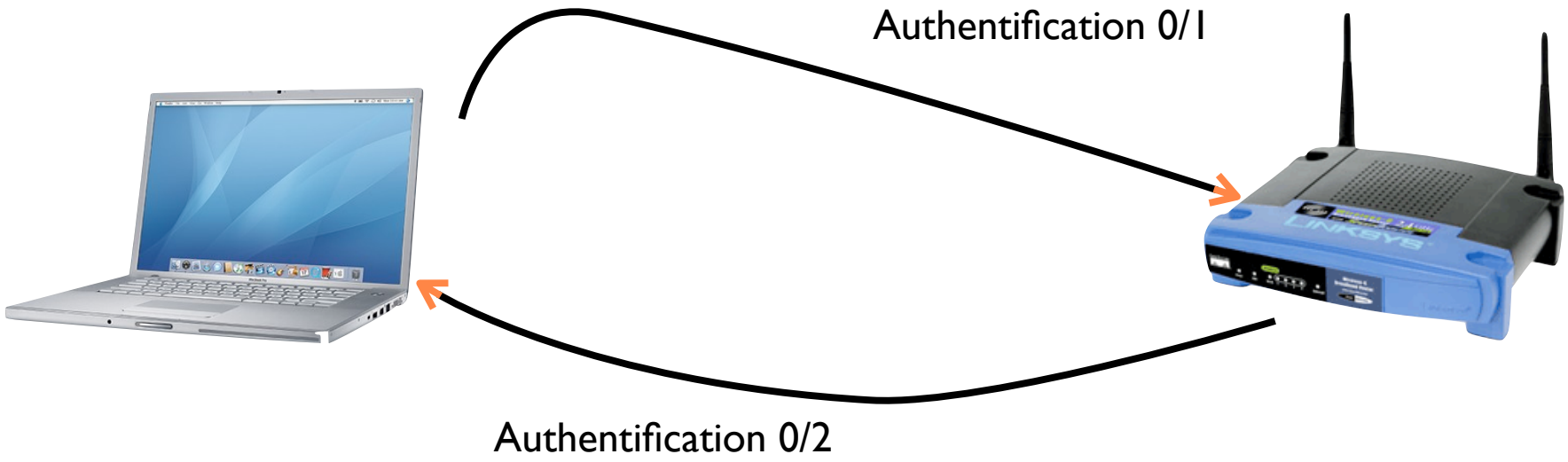

WEP
4
variable
4
4
MAC Header
IV Header
Frame Body
ICV
CRC


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

Améliorations de WPA par rapport à WEP

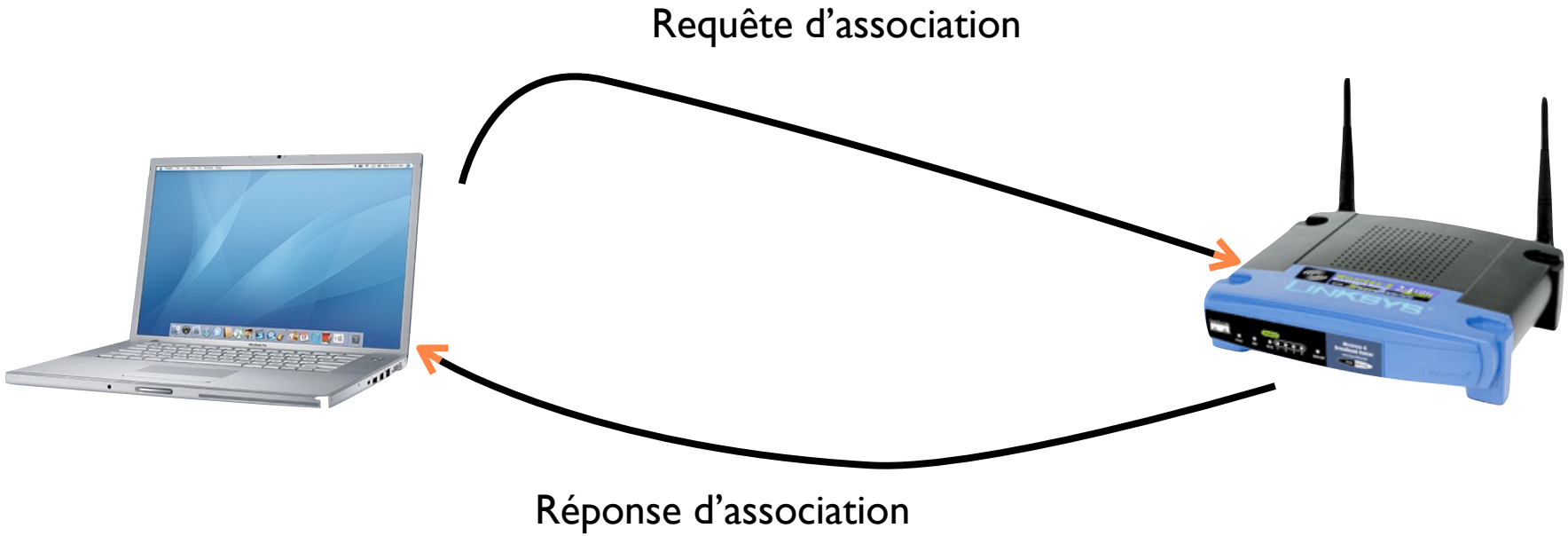
- TKIP (Temporal Key Integrity Protocol)
  - L'IV ne se répète pas
  - La clé dépend d'un numéro de séquence et de l'adresse de la STA source
  - Donc, la clé est différente pour chaque trame
  - Le MIC (Message Integrity Code calculé utilisant la méthode Michael) est significativement plus fort que l'ICV
- Méthode d'authentification améliorée

Commencer avec authentification ouverte



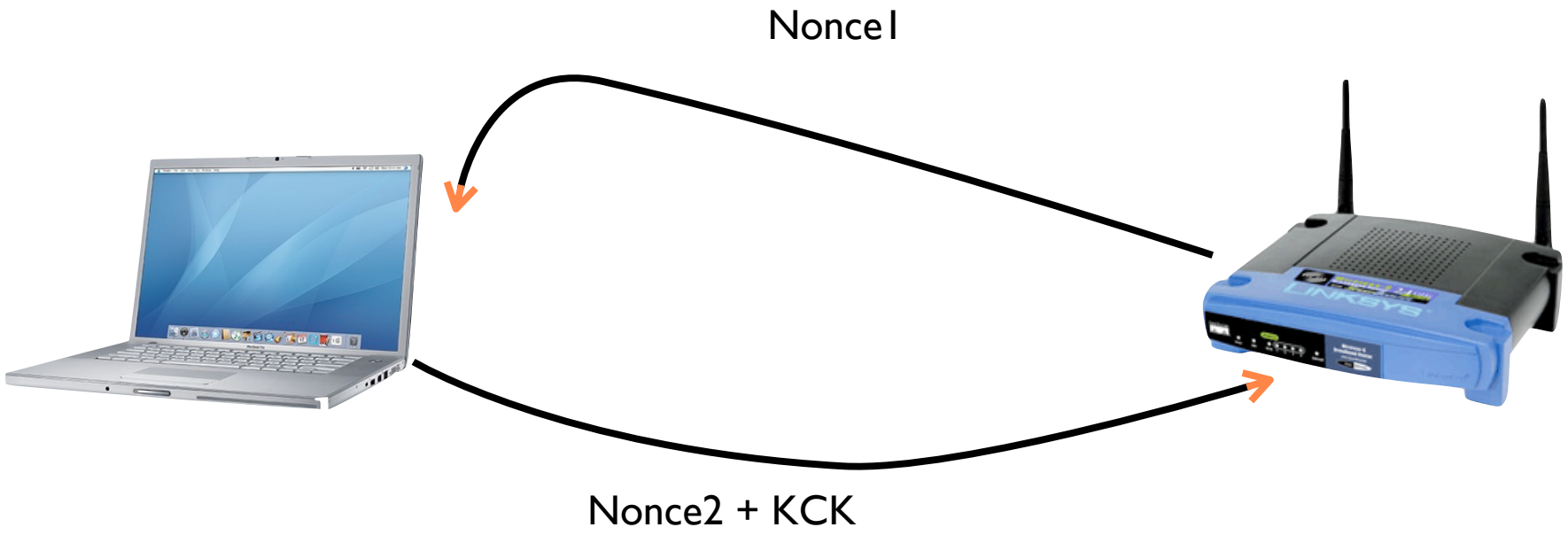
Association

... comme avant



Nouveau: échange de nonces

La station crée les clés à partir de :
La clé partagée secrète + Nonce1 + Nonce2

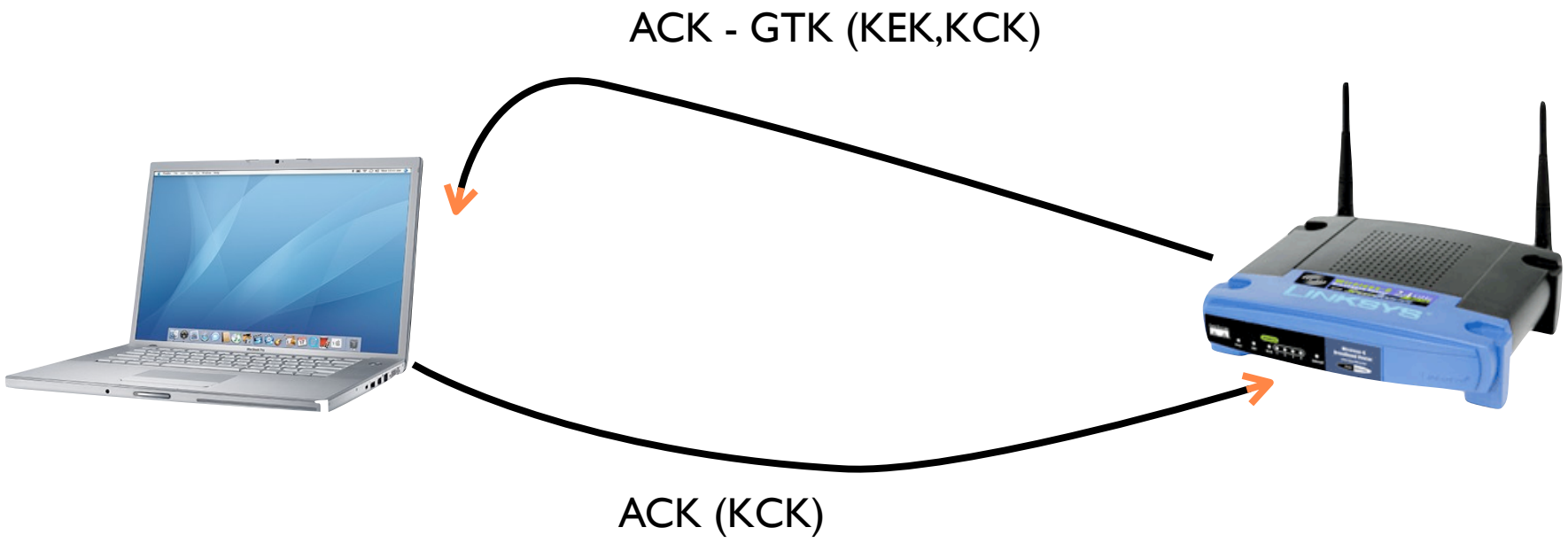


L'AP authentifie la STA utilisant le MIC
Il crée également les clés

Nouveau: échange de nonces

La station reçoit la GTK

L'AP est maintenant authentifié



Fin