无线局域网安全技术

提纲

- 0. 基础无线局域网络结构
- 1. 有线等效保密协议-WEP
- 2. 802. 11i 加密机制
- 3. 802. 11i 的鉴别机制-802. 1X
- 4.Wi-Fi Protected Access---WPA

0 基础无线局域网络结构

- WLAN是指一个无线站点（如接入点AP，Access Point）充当中心站，所有无线节点对网络的访问均由其控制的网络。

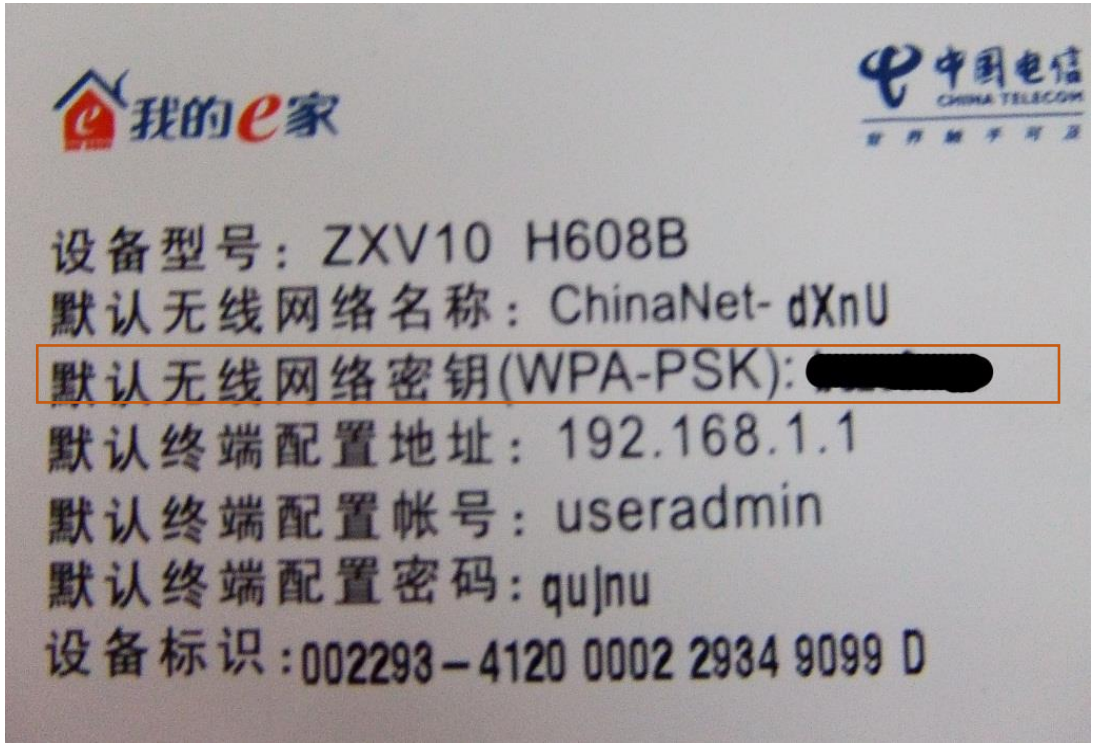
- 接入点为通信的中心，为无线节点提供连接，是非对等的；为了与接入点关联，必须将无线节点的服务集标识符（SSID）配置成接入点的SSID。

- 常用在企业、家庭以及小型/家庭办公室（SOHO）无线联网环境中

无线网络的开放性，安全问题严重！！！

0 基础无线局域网络结构

- **WPA**: Wi-Fi Procted Access
- **PSK**: Pre-shared Key预共享密钥



1.有线等效保密协议-WEP

WEP（**Wired Equivalent Privacy**），有线等效保密协议

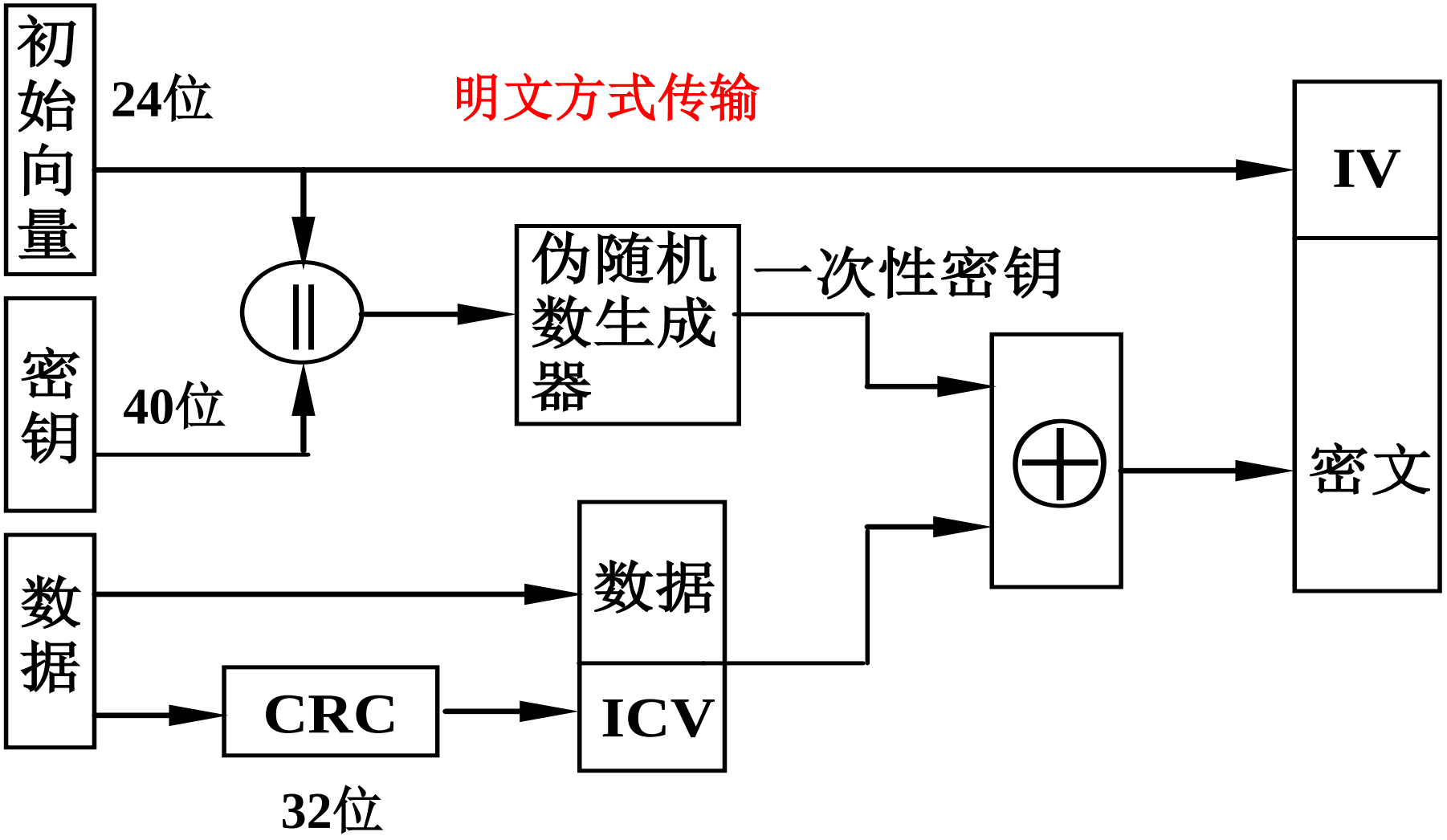
- **802.11b**中定义的最基本安全加密
- 采用**RC4**流加密算法
- **目标**：提供访问控制和保护隐私的功能
  - **访问控制**—**防止没有WEP秘钥的非法用户访问网络**
  - **保护隐私**---通过**加密**手段保护无线局域网上传输的数据，防止数据被攻击者窃听，防止数据被攻击者中途恶意篡改或伪造

1.有线等效保密协议-WEP

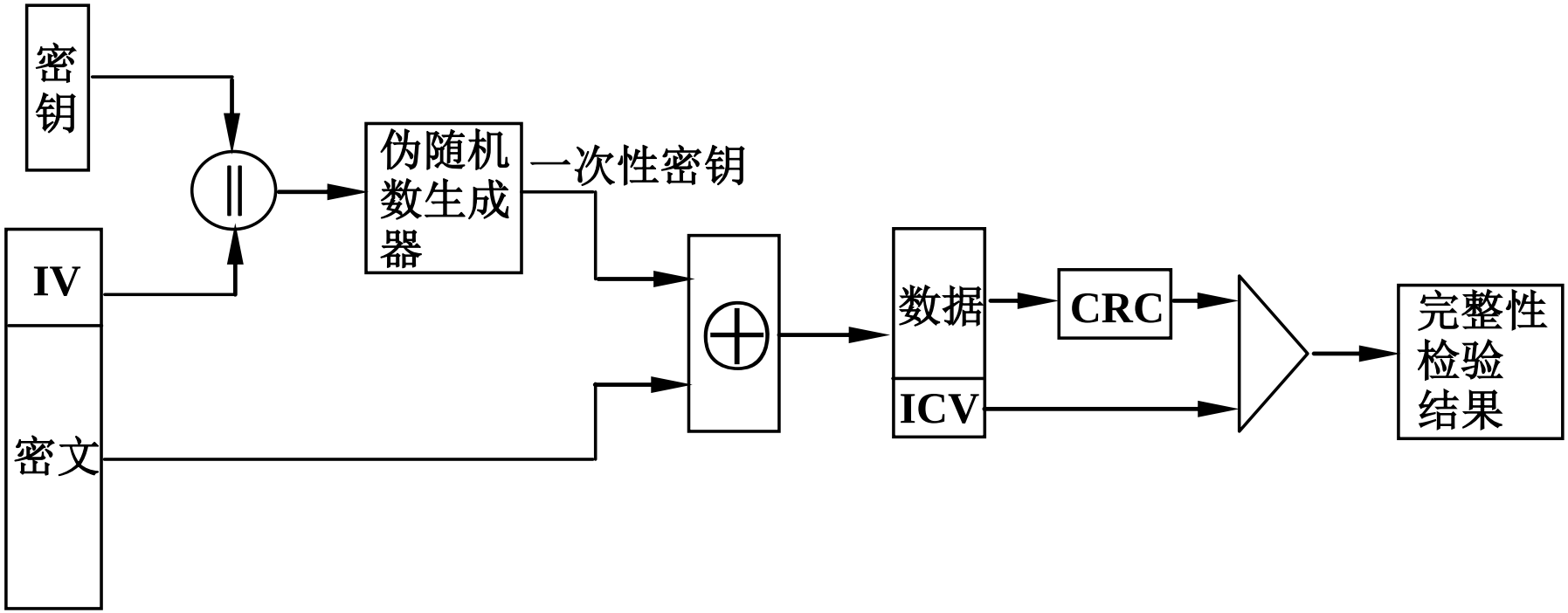
关注问题：

- IV、密钥、随机数种子、CRC、一次性密钥分别多少位？
- 发送端发送给接收端的有哪些信息？分别是密文形式还是明文形式？
- 为什么每一次加密，就都要变一下IV？
- WEP加密过程、WEP解密过程？

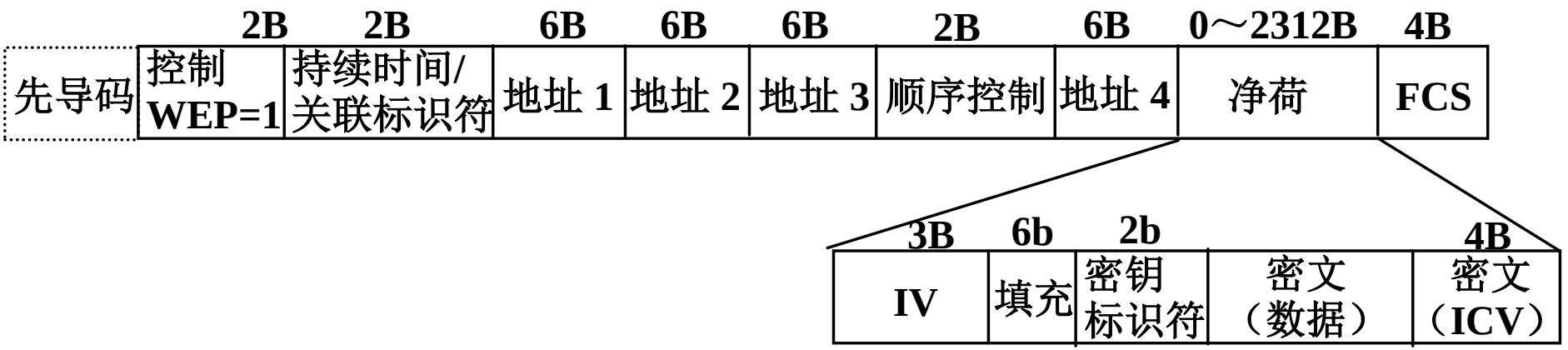
1.1 WEP加密过程



1.2 WEP解密和完整性检测过程



1.3 WEP帧结构



WEP支持64位和128位加密

- 64位加密有时称为40位加密
- 128位加密有时称为104位加密

1.4WEP鉴别机制

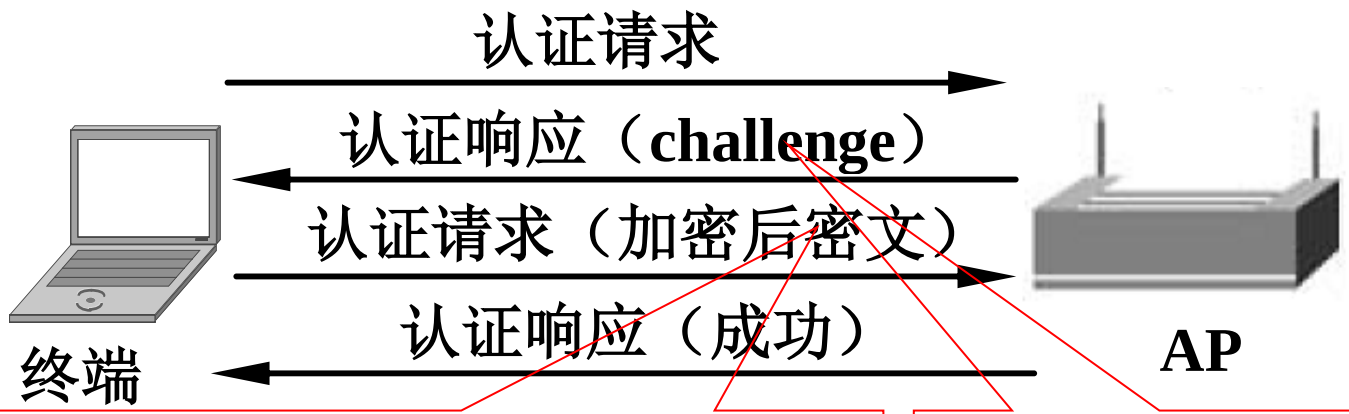
WEP认证方式

1. 开放系统认证

2. 共享密钥认证

- 采用标准的挑战/响应机制，以共享秘钥来对客户端进行认证
- 对128字节的challenge进行如下面的加密和解密流程，完成认证。

1.4 WEP鉴别机制--共享密钥认证四次握手

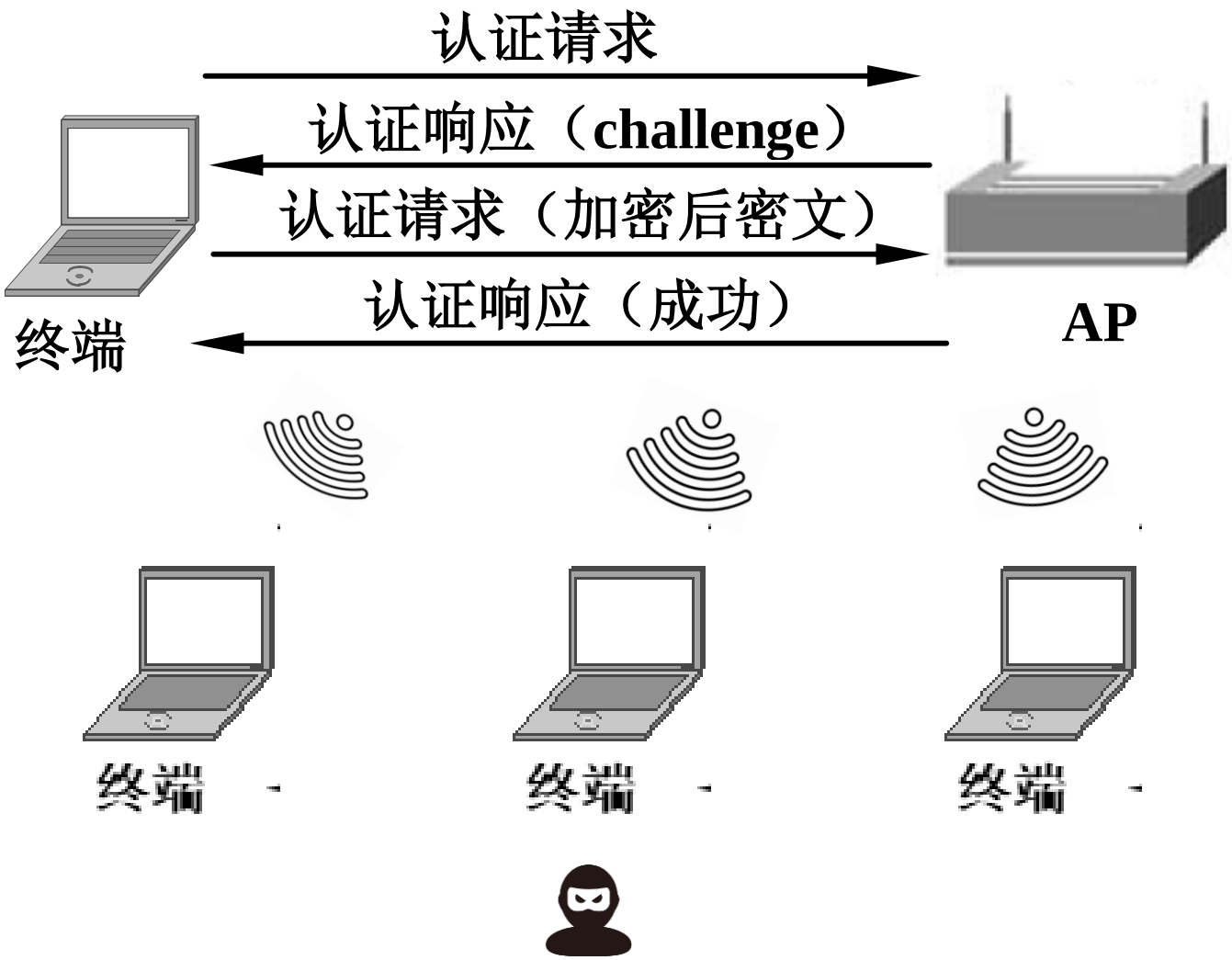


密文＝（challenge‖ICV）⊕K；
K是一次性密钥，以IV和密钥为伪随机数种子生成的伪随机数，其长度＝128＋4（单位字节）。

challenge是128字节长度的随机数。

1.4 WEP鉴别机制

终端共享相同密钥，静态配置



你发现什么问题了吗？

1.5 WEP的安全缺陷

- 静态密钥管理缺陷。
  - 所有终端共享相同密钥，静态配置。
- 共享密钥认证机制的安全缺陷；
  - 攻击者可以获取到当前使用的一次性K，因为challenge，IV都是明文传输的。
- 一次性密钥字典
  - IV是24位，有限穷举空间为2^24，固定字典时间为1220s
- 完整性检测缺陷。
  - CRC算法的缺陷。

攻击者：
实现身份认证通过和密钥窃取攻击。

新的安全技术的提出

- 由于WEP的安全漏洞，IEEE 802.11i工作组和生产厂商Wi-Fi联盟以及我国都提出了新的安全体系：

  IEEE 802.11i

  WPA（Wi-Fi联盟，WEP到IEEE 802.11i的过渡方案）

  WAPI（无线网鉴别和保密基础结构，我国）

新的安全技术的提出-802.11i

解决了WEP中安全问题

1．加密机制

2^{48}？？

基于用户配置密钥，且密钥采用动态配置机制；一次性密钥的数量增加到2^{48}个，且BSS中的每一个终端拥有独立的2^{48}个一次性密钥，以此避免出现重复使用一次性密钥的情况。

2．完整性检测机制

完整性检验值具有报文摘要的特性，并使用加密的消息鉴别码（MAC）。

3．鉴别身份机制

802.1X作为鉴别协议，针对用户的，双向鉴别机制。

2 802.11i加密机制

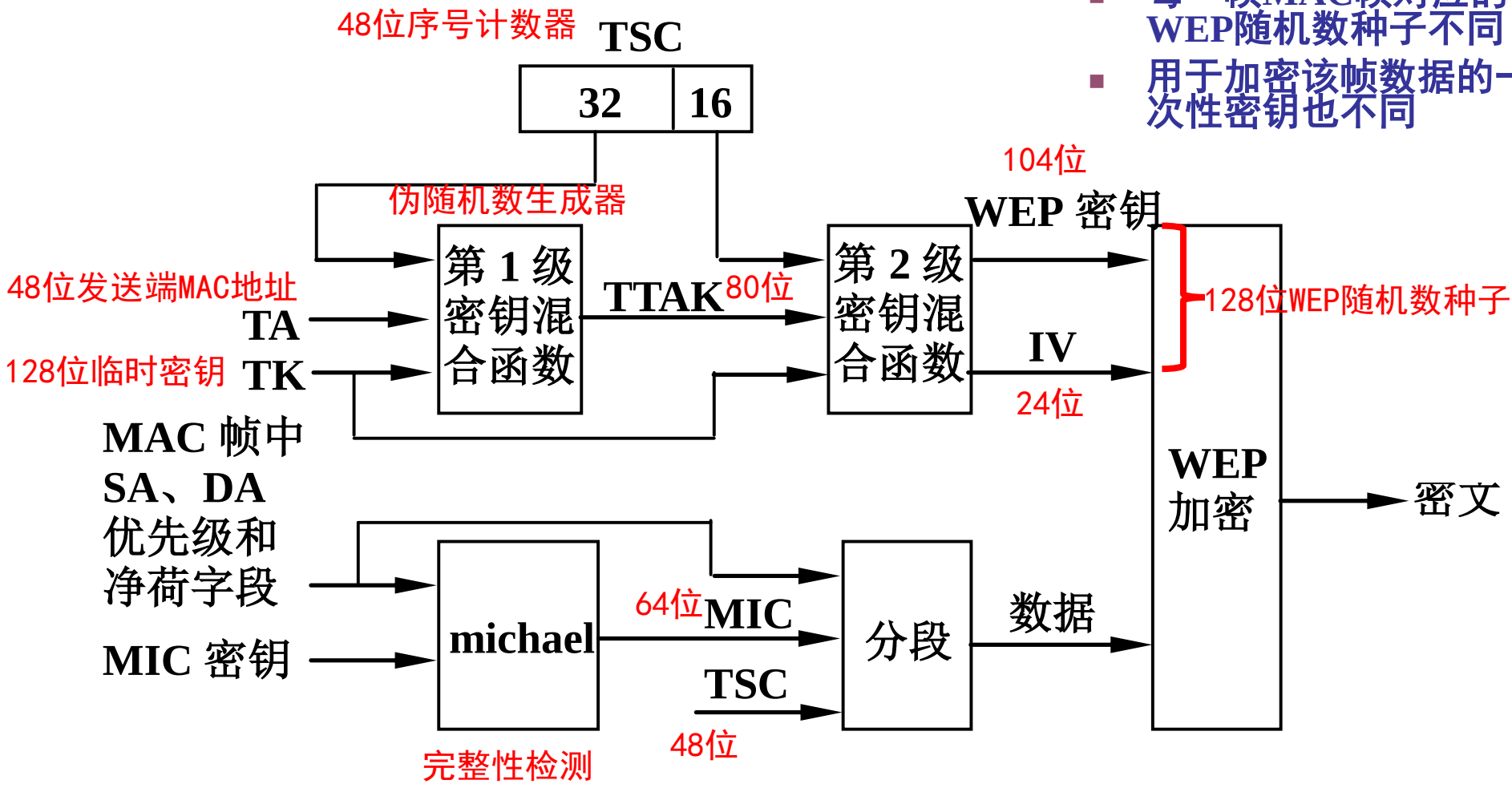
802.11i加密机制主要有：

- 临时密钥完整性协议（TKIP-Temporal Key Intergrity Protocol）

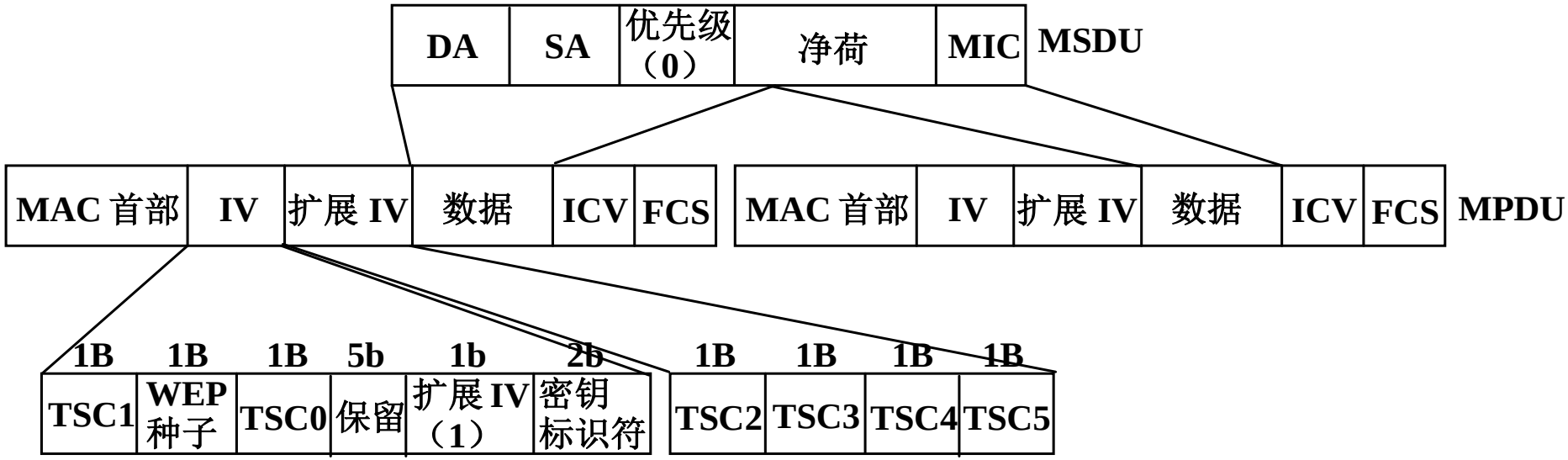
- CCMP（CTR with CBC-MAC Protocol）

2.1 TKIP-兼容WEP

- 每一帧MAC帧对应的WEP随机数种子不同
- 用于加密该帧数据的一次性密钥也不同

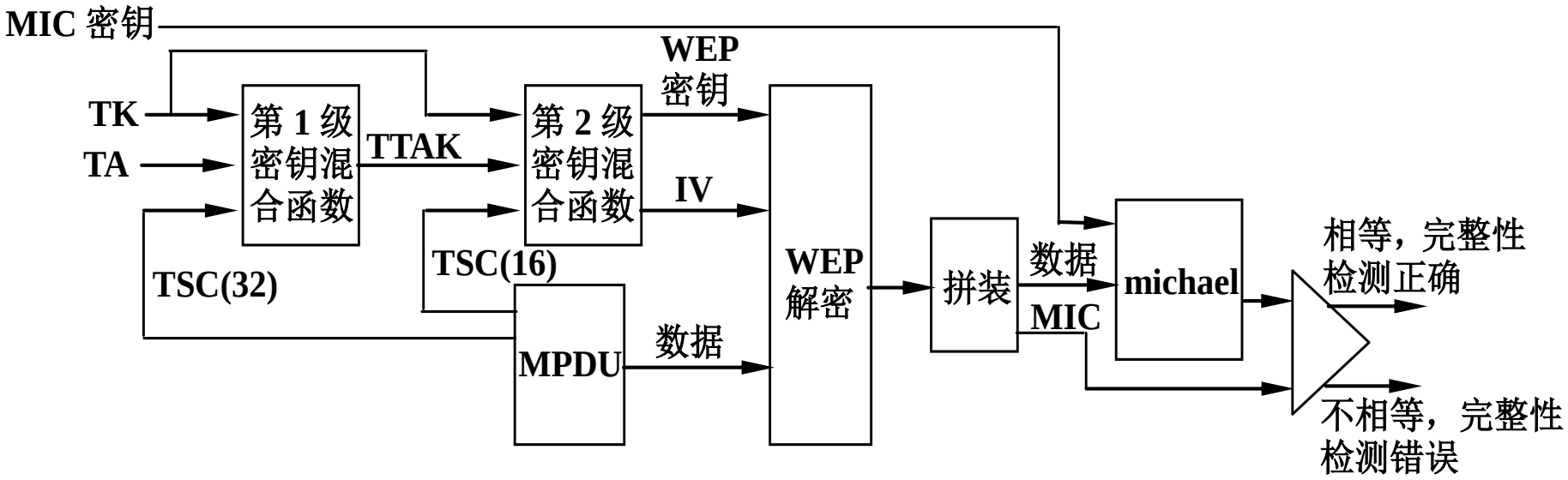


2.1 TKIP-兼容WEP



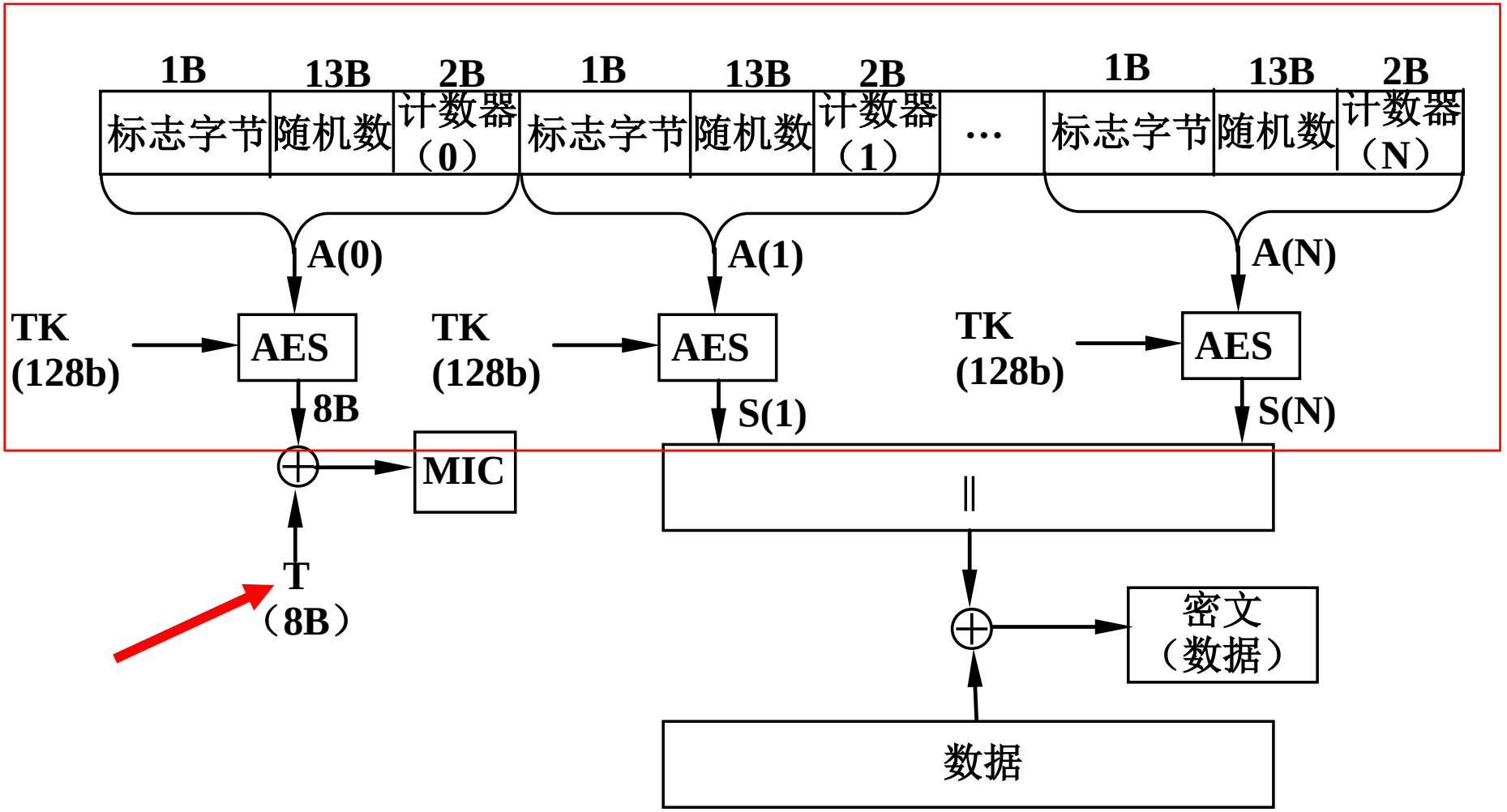
MAC帧格式和TKIP MPDU封装过程

2.1 TKIP-兼容WEP



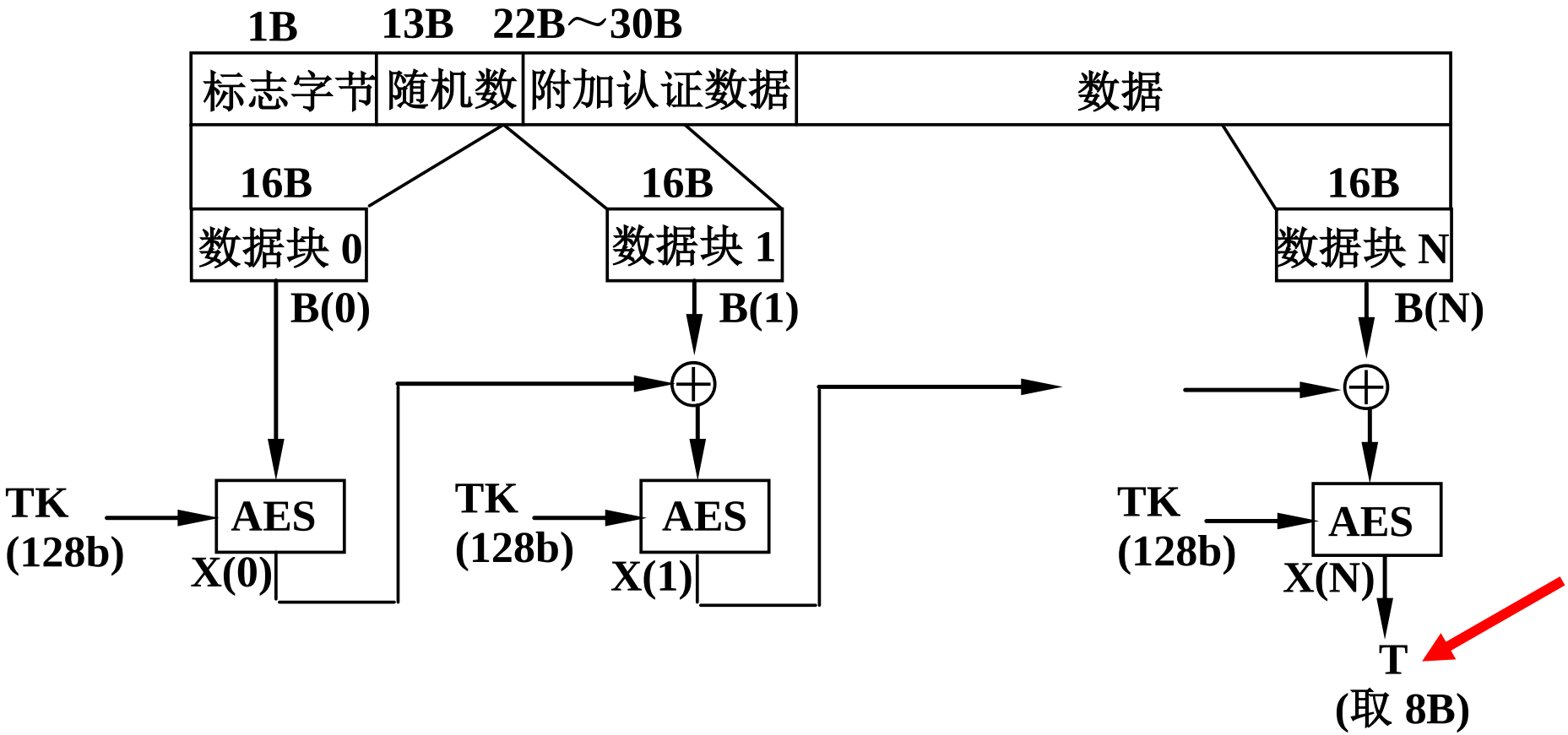
TKIP解密过程

2.2 CCMP之CTR加密



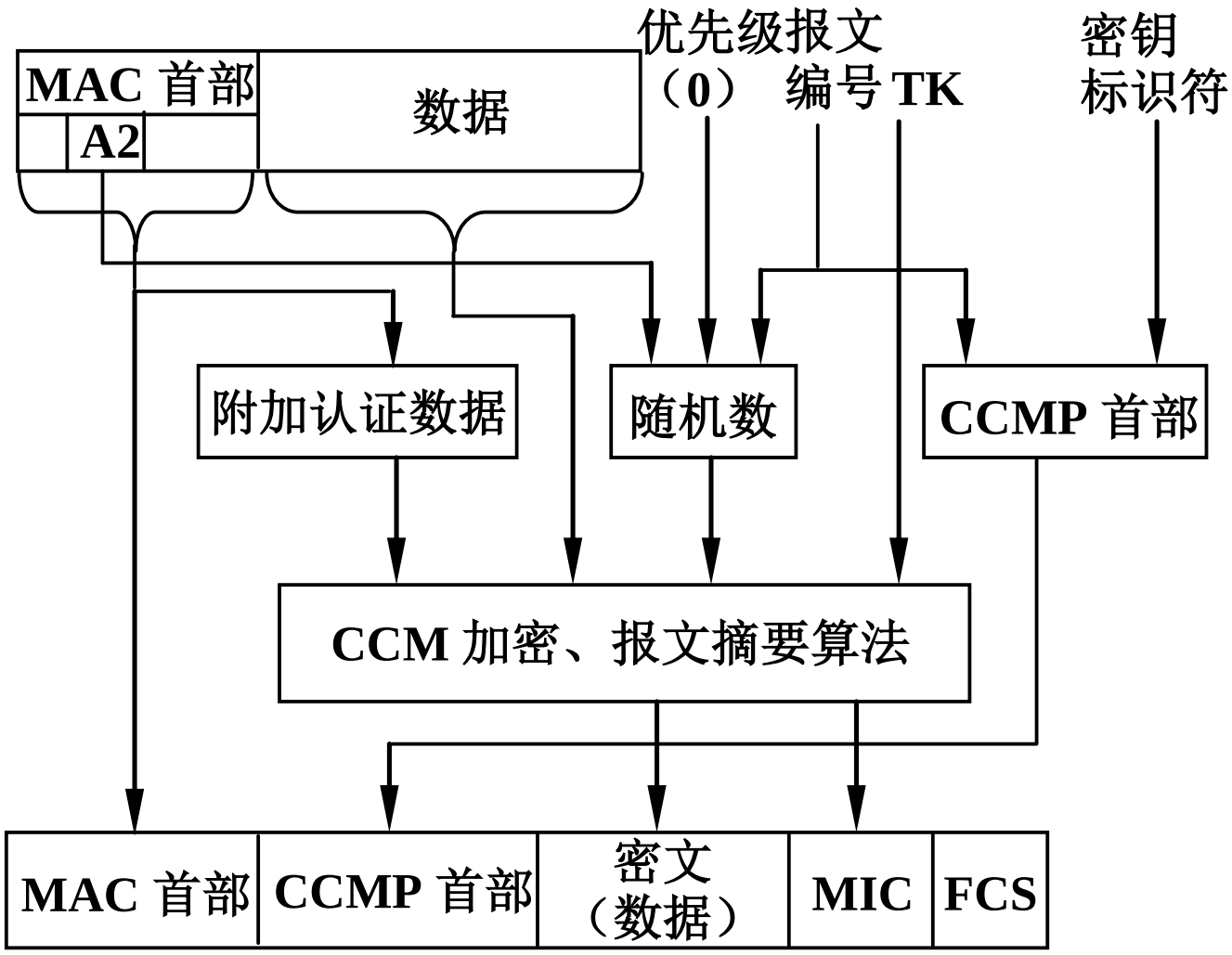
CCMP数据加密过程

2.2 CCMP之 CBC-MAC过程



CCMP计算MIC (T) 过程

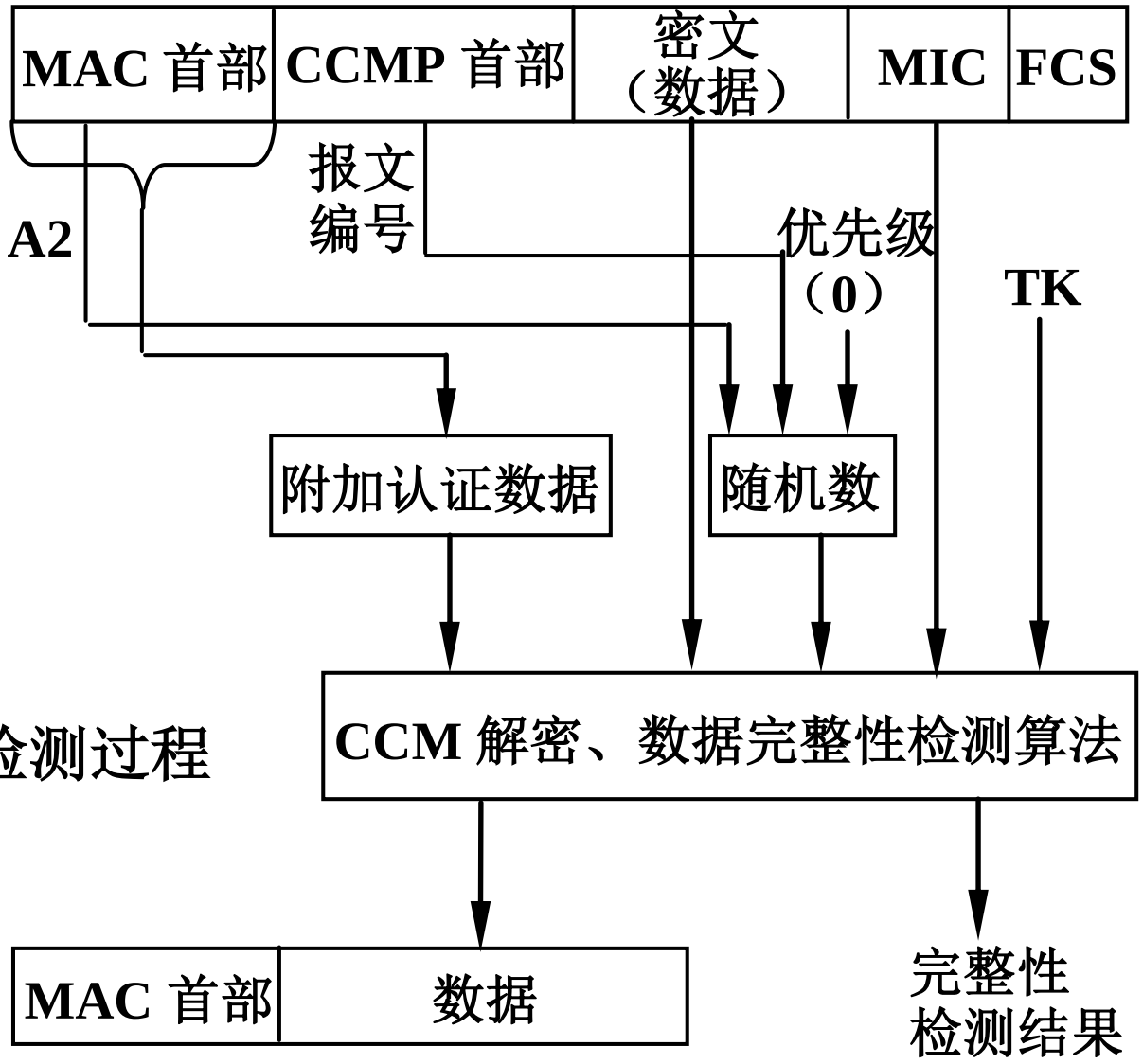
2.2 CCMP



CCMP加密和计算MIC过程

2.2 CCMP

CCMP解密和完整性检测过程



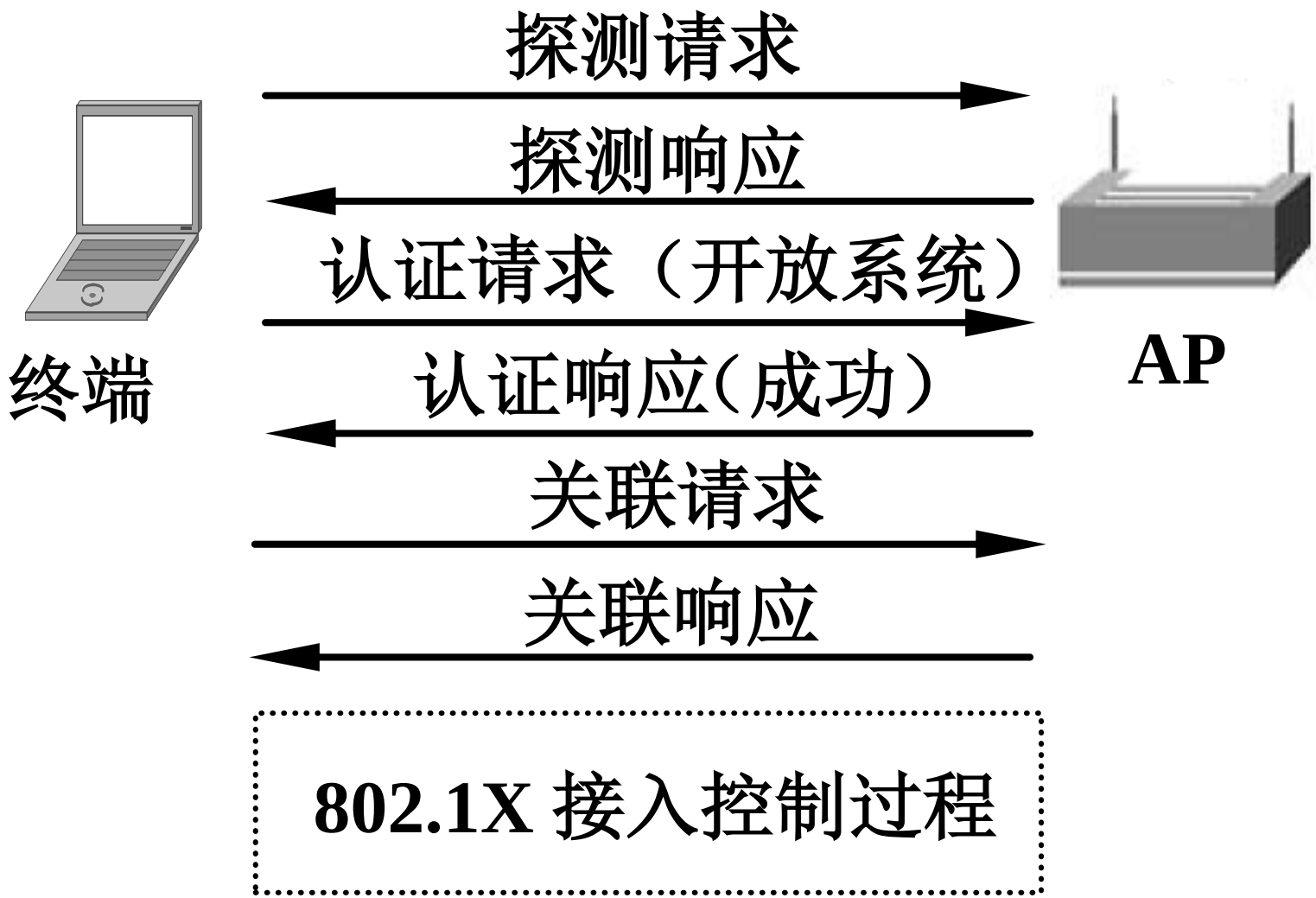
3 802.11i的鉴别机制-802.1X

802.11i的安全性基于以下特点：

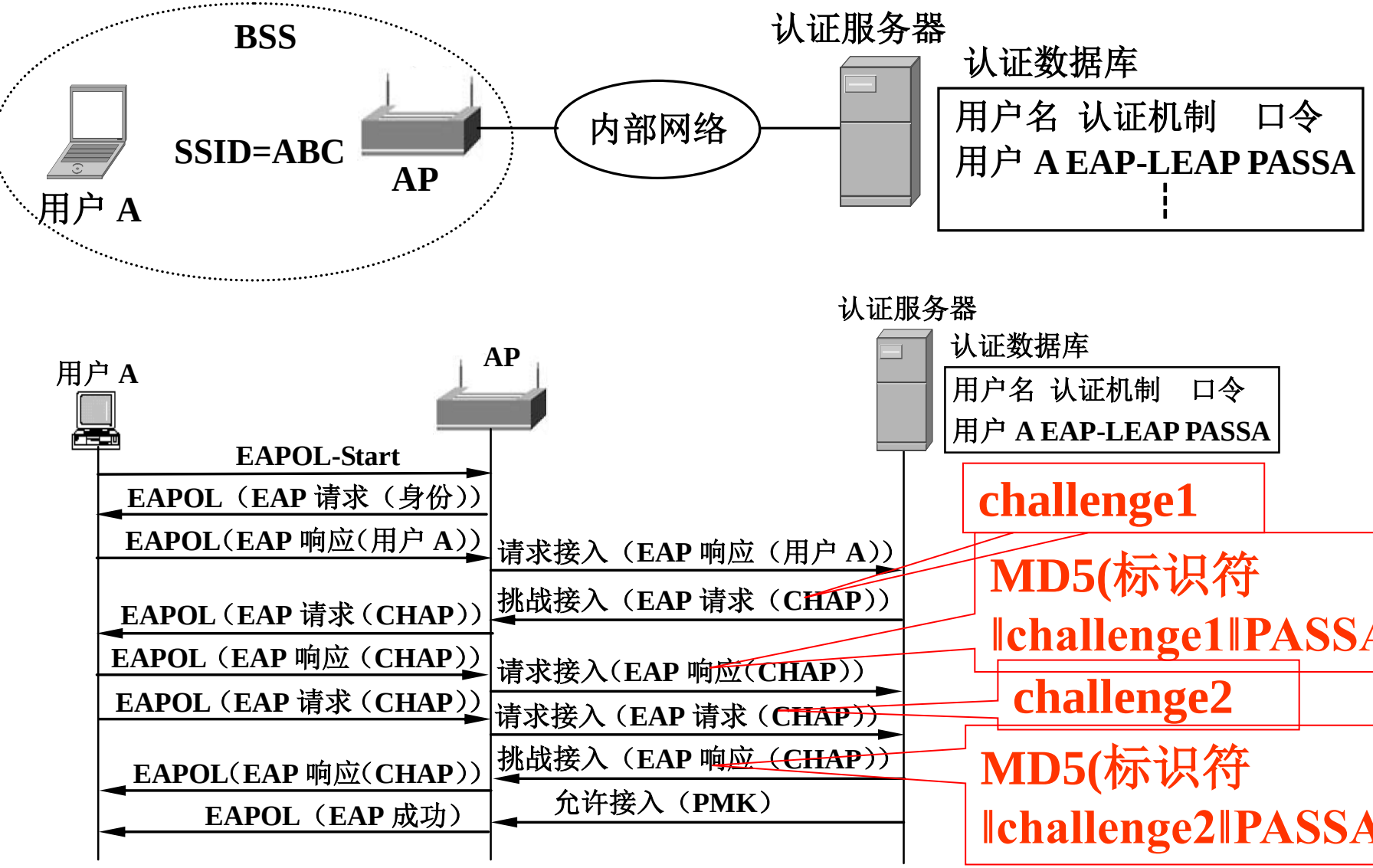
- 基于用户身份认证，不是基于终端，因此，同一用户可在不同的AP和BSS建立安全关联；
- 和AP建立安全关联，并在建立安全关联时分配临时密钥TK，TK只在安全关联存在期间有效；

- 802.1X完成双向的、基于用户的身份认证，并分配临时密钥TK；
- 安全关联指在正常建立的关联的基础上由802.1X完成双向的、基于用户的身份认证，并分配临时密钥TK的关联。

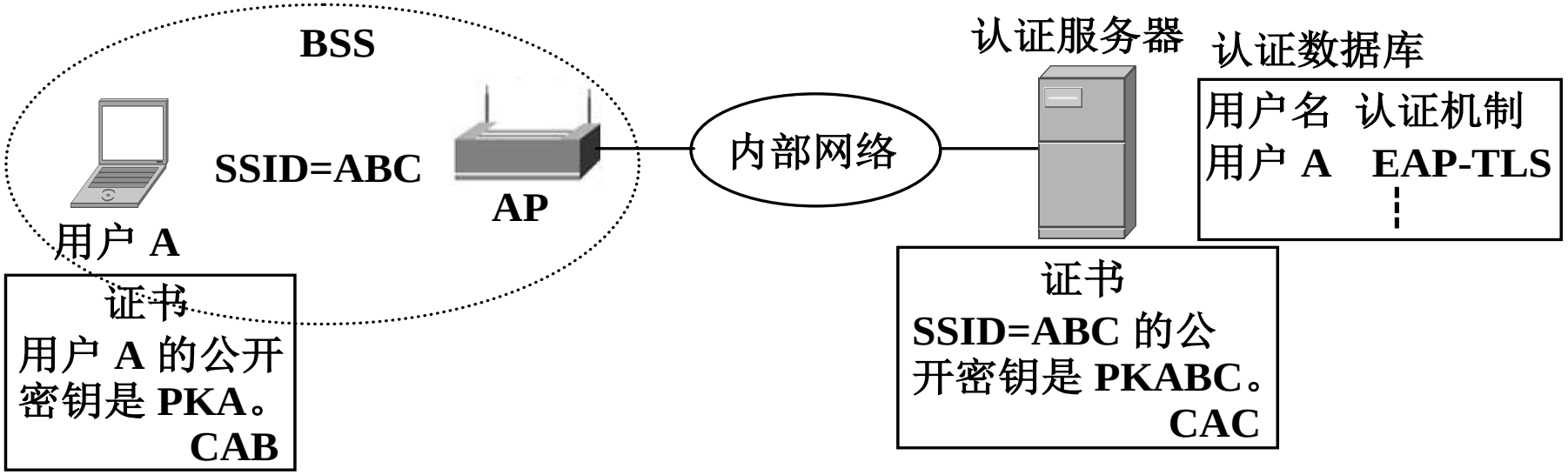
3.1基于802.1X建立安全关联



3.2 双向CHAP鉴别（基于802.1X）

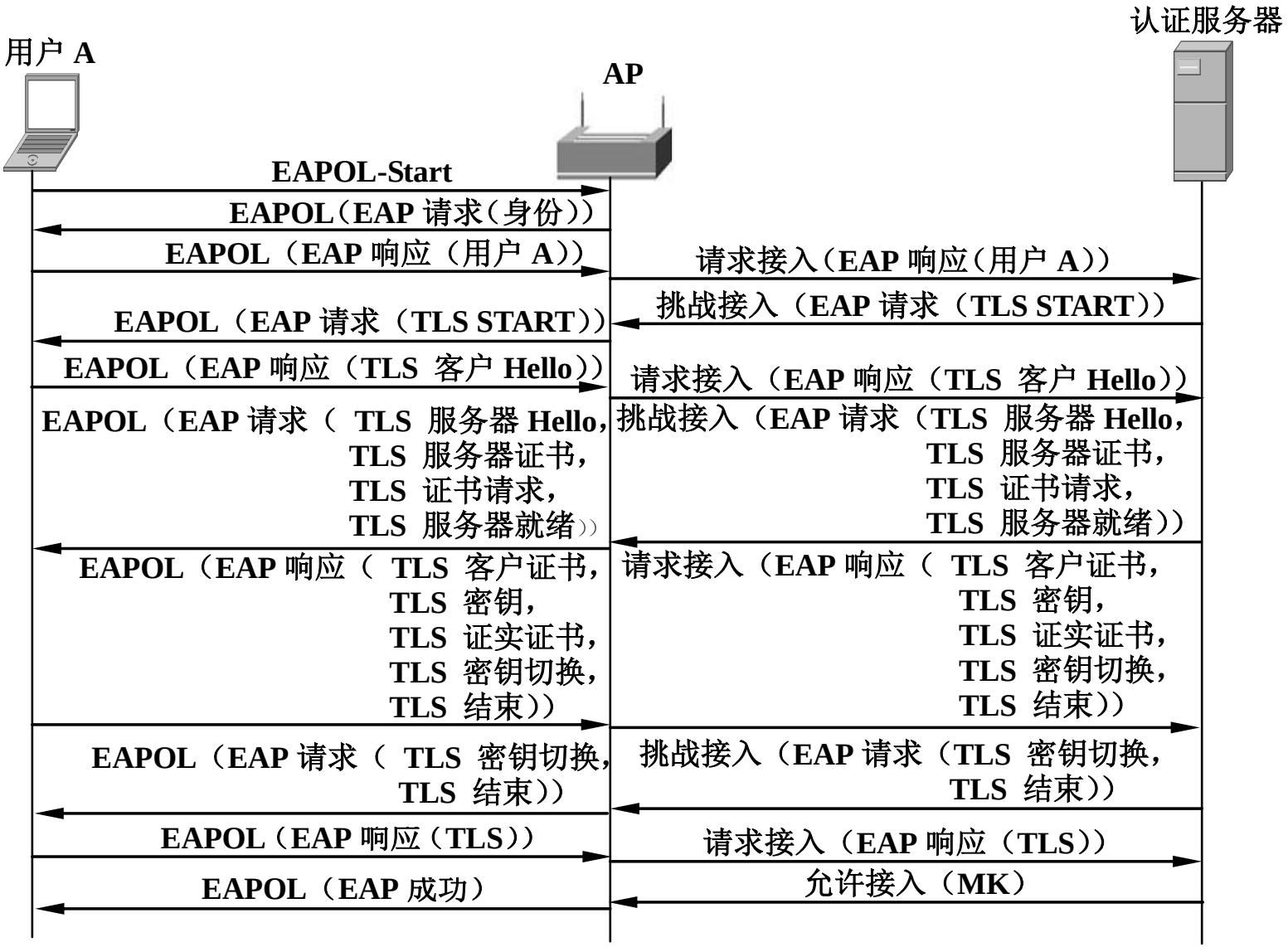


3.3 双向TLS鉴别（基于802.1X）

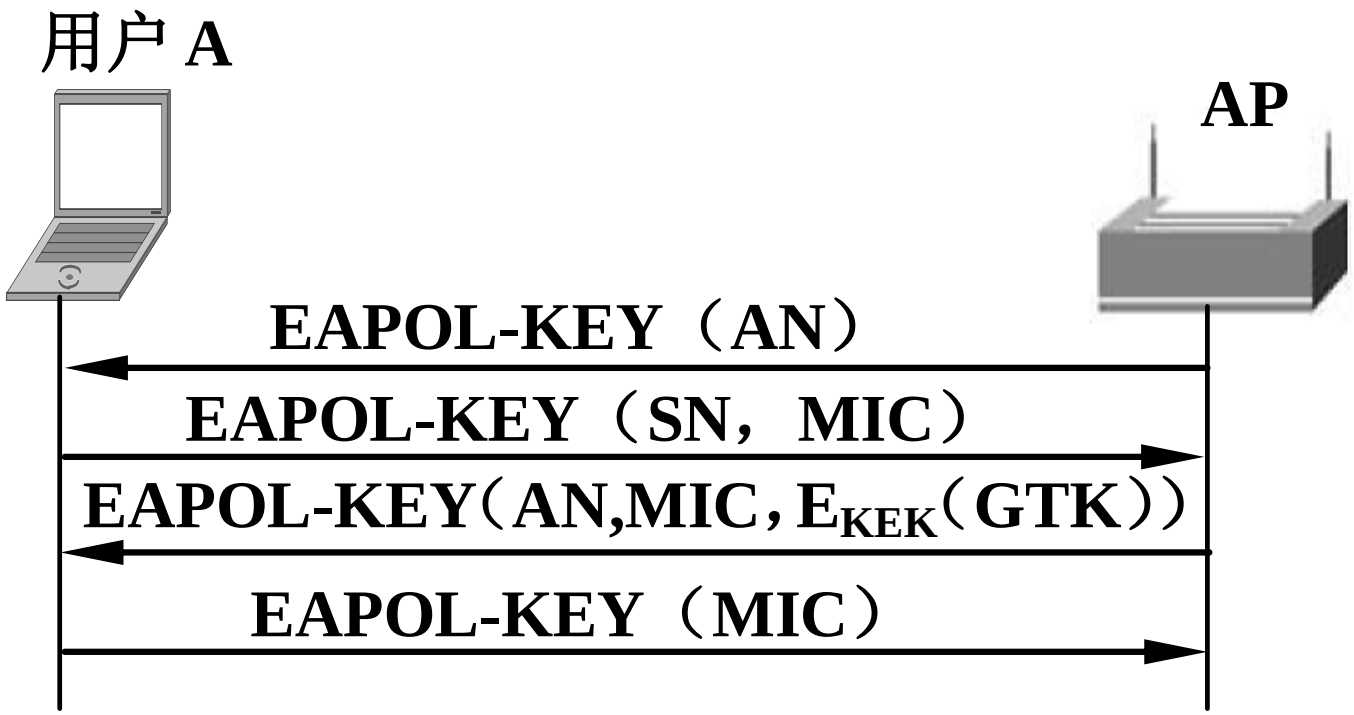


双向TLS鉴别的网络结构

3.3 双向TLS鉴别（基于802.1X）

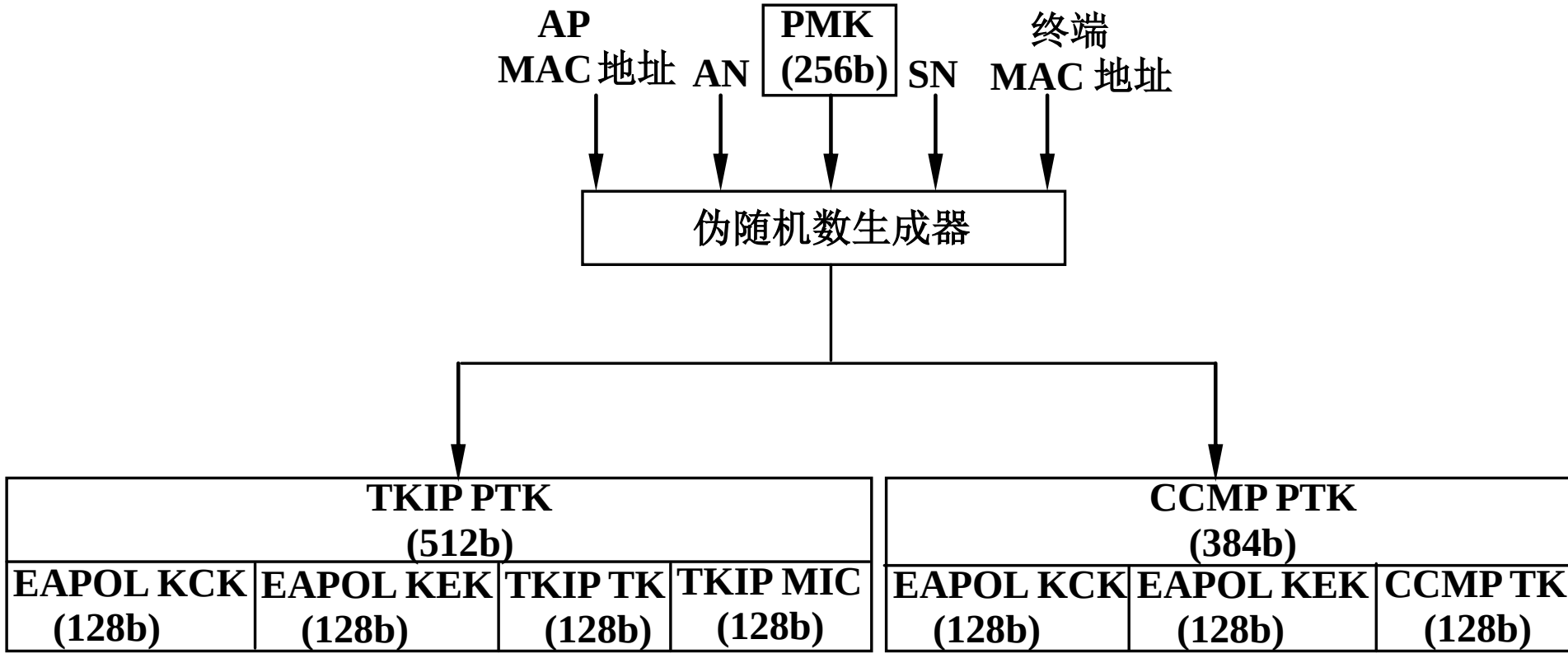


3.4 动态密钥分配机制



- 8021.1X动态密钥分配机制

3.4 动态密钥分配机制



证实密钥和加密密钥（密钥生成过程中的）　加密密钥　证实密钥

4.Wi-Fi Protected Access---WPA

- WIFI联盟2003年在802.11i草案的基础上发布的加密标准

➢ **家庭/个人 WPA-PSK (Pre Shared Key)**

- 预共享密钥（PSK）
- TKIP加密算法

（临时秘钥完整性协议）

➢ **商业/企业 WPA-Enterprise**

- 802.1X Radius
- 可扩展认证协议 EAP

WPA使用动态的密钥加密算法
它会不断地变化并使得破解入侵
无线网络比WEP更困难

➢WPA 企业版需要一台具有 IEEE 802.1X 功能的 RADIUS (远程用户拨号认证系统) 服务器。

4.1 WEP与WPA比较

WEP缺陷	WPA改进
IV太短	**在TKIP中，IV大小增加一倍，已达48位**
ICV漏洞	CRC校验方式由Michael算法取代，计算粒度达到64位
密钥不更新	由主密钥派生出临时密钥以保证每个客户端均不同
无重放保护	使用TKIP算法将IV用做帧计数器以提供重放保护

4.2 WPA2

- WPA和WPA2都是基于802.11i的。
- 简单概括：
- **WPA = IEEE 802.11i draft 3 = IEEE 802.1X/EAP + WEP(选择性项目)/TKIP**
- **WPA2 = IEEE 802.11i = IEEE 802.1X/EAP + WEP(选择性项目)/TKIP/CCMP**

4.2 WPA2

- IEEE 802.11i标准2004年6月最终确认后发布的加密标准
- **WPA2**是WPA的升级版，现在新型的网卡、AP都支持WPA2加密。

  WPA2-PSK

  WPA-Enterprise

4.2 WPA2之个人模式

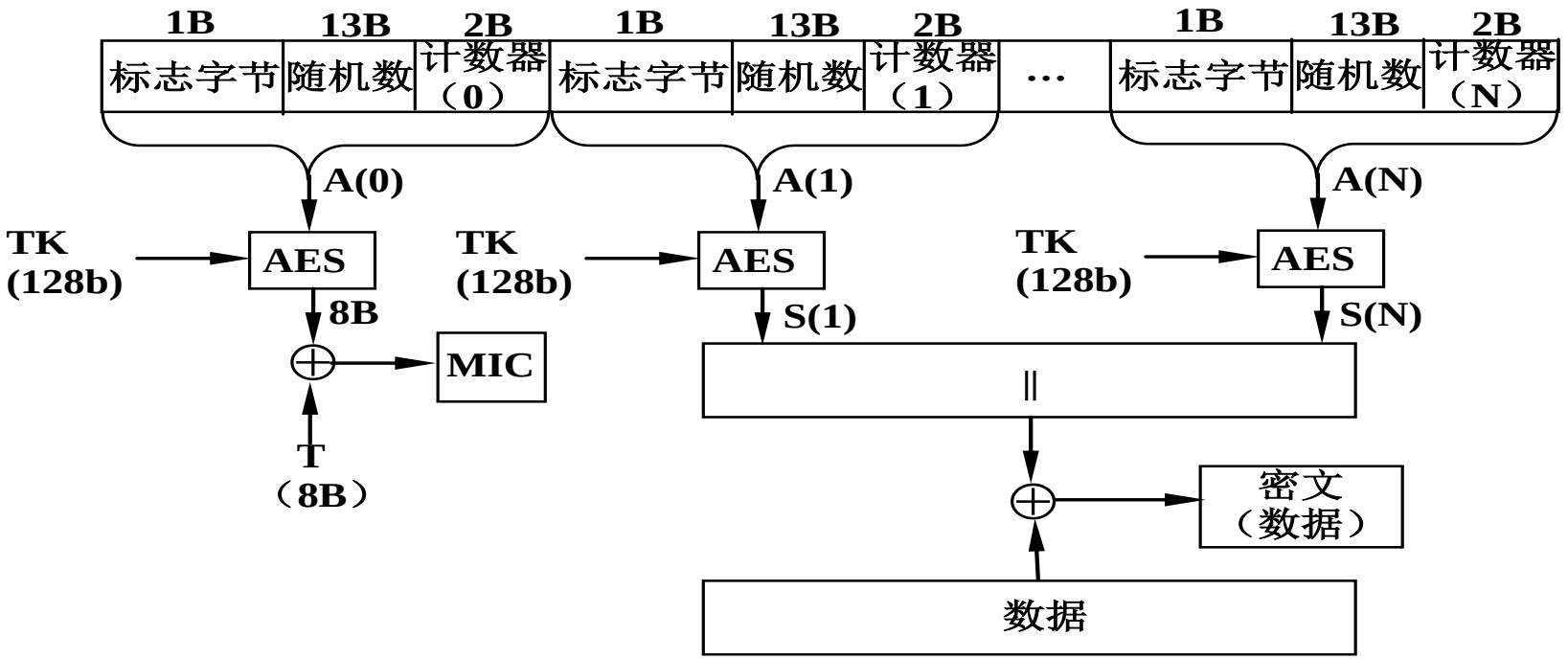
1．密钥导出PMK过程

PMK=PSK=pdkdf2_SHA1(passphrase，SSID，SSID length，4096)

2．由PMK(PSK)导出PTK的过程

WPA2个人模式下的PTK生成过程如3.4动态密钥分配机制。

课堂交流：CCMP加密结构



- CCMP加密时采用CTR加密模式，如图，并没有直接用AES对明文数据加密，而是使用计数器和临时密钥用AES加密产生的一系列数据流后再和明文数据异或，请查阅相关资料并结合实际应用需要分析其采用现有加密结构的原因？