第11章
无线网络安全

中国科学技术大学
曾凡平
billzeng@ustc.edu.cn

课程回顾：第10章 Internet安全

10.1 OSI安全体系结构

- 安全攻击，安全服务，安全机制

10.2 IPSec协议

- IPSec体系结构，IPSec工作模式，AH协议

10.3 SSL/TLS协议

- SSL体系结构，SSL记录协议，SSL修改密码规范协议，
- SSL报警协议，SSL握手协议，TLS协议

10.4 安全电子交易

- SET的需求，SET系统构成，双向签名，支付处理

第11章 无线网络安全

11.1 IEEE 802.11无线网络安全

- IEEE 802.11无线网络背景
- WEP
- 802.11i

11.2 移动通信系统的安全

- GSM的安全
- GPRS的安全
- 第三代移动通信系统(3G)的安全

11.3 第四代移动通信系统(4G)的安全概述（补充）

11.4 第五代移动通信系统(5G)的安全概述（补充）

11.1 IEEE 802.11无线网络安全

11.1.1 IEEE 802.11无线网络背景

- **IEEE 802**是一个开发**局域网(LAN)标准**的委员会，**802.11**则是成立于1990年的工作组，负责开发**无线局域网(WLAN)**的协议与传输规范。
- 目前802.11有多种扩展名，一般以后缀字母区分。
- 其中IEEE 802.11是原始标准，规定了无线局域网的**物理层和MAC层**的内容；802.11a、802.11b、802.11g、802.11n、802.11ac等是物理层的相关扩展标准；其余几个重要标准的内容如表11-1所示。

IEEE 802.11系列部分标准

表11-1

标准名称	主要内容
802.11d	在媒体接入控制/链路连接控制 (MAC/LLC) 层面上进行扩展，对应 802.11b 标准，解决不能使用 2.4GHz 频段国家的使用问题
802.11e	在 802.11MAC 层增加 QoS 能力，用时分多址 (TDMA) 方案取代类似以太网的 MAC 层，并对重要的业务增加额外的纠错功能
802.11f	改进 802.11 的切换机制，以使用户能够在两个不同的交换分区 (无线信道) 之间，或在两个不同的网络接入点之间漫游的同时保持连接
802.11h	对 802.11a 的传输功率和无线信道选择增加更好的控制功能，与 802.11e 相结合，适用于欧洲地区
802.11i	消除 802.11 的最明显的缺陷: 安全问题
802.11p	针对汽车通信的特殊环境而制定的标准
802.11v	无线网络管理，面向运营商，致力于增强由 802.11 网络提供的服务

- (1)在无线局域网中，**需要认证技术，以验证节点的身份**。而在有线局域网中，“与网络相连”这个可见行为起了某种程度的认证作用。
- (2)**无线局域网需要隐私保护机制**。而在有线局域网中，“信息的接收节点必须与网络相连”提供了一定程度的隐私性。
- 与有线局域网相比，无线局域网对安全服务和机制有更高的要求。

IEEE 802.11定义的安全机制：数据保密和完整性、身份认证

- 1999年发布的802.11b标准里定义了**WEP(Wired Equivalent Privacy)协议**，为数据提供机密性和完整性保护，并基于WEP协议设计了共享密钥认证机制。
- WEP协议旨在提供和有线局域网同级的安全性，但此后的大量工作证明，WEP存在较大的安全缺陷。因此，IEEE于2001年成立了802.11i任务组，以制定新的安全标准，来增强无线局域网的安全性。
- 在802.11i完善之前，国际Wi-Fi联盟组织(Wi-Fi Alliance)提出了**WPA(Wi-Fi Protected Access)标准**，作为802.11i完备之前替代WEP的过渡方案。
- 2004年6月，完整的802.11i标准通过，Wi-Fi联盟也随即公布了与之相对应的**WPA第二版(WPA 2)**。

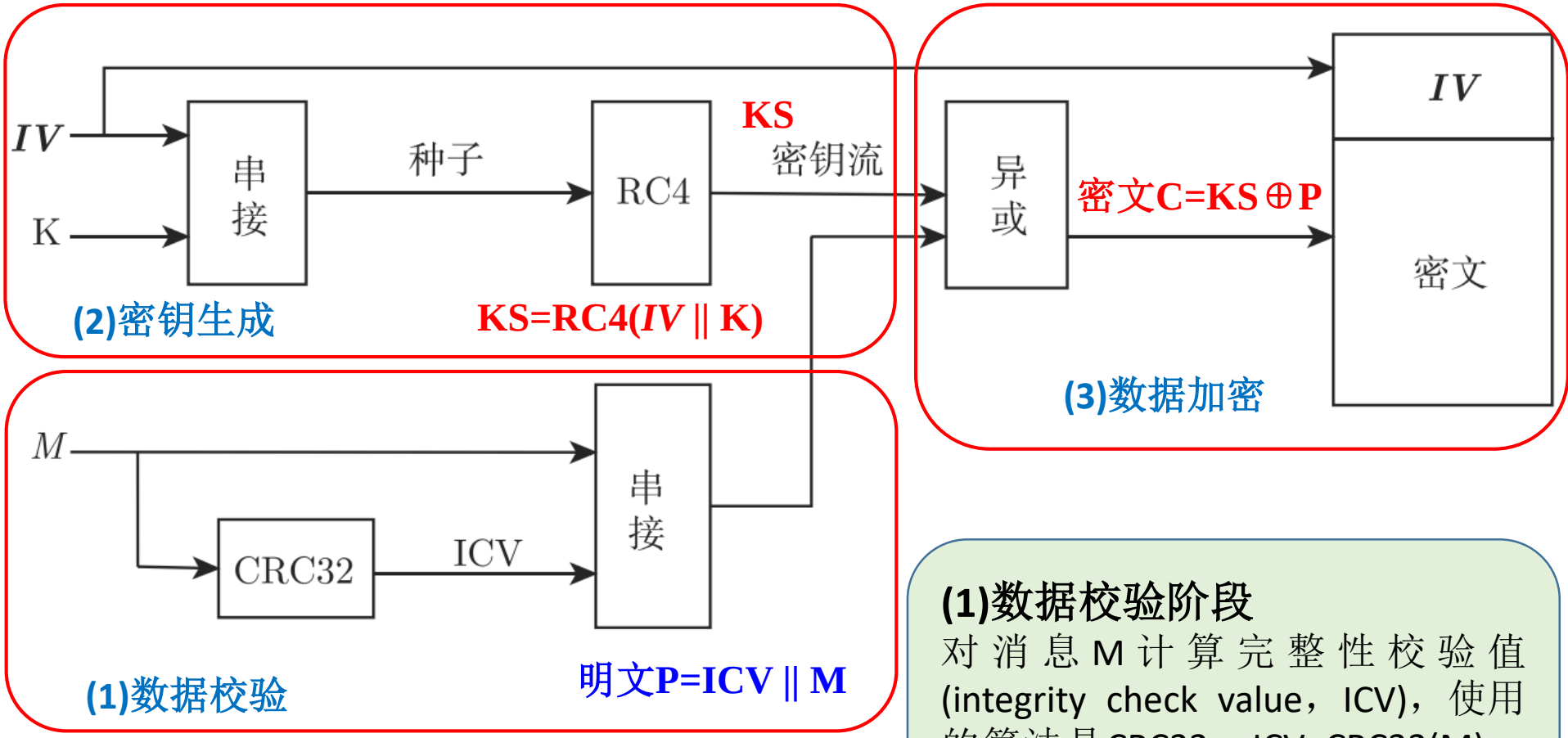
11.1.2 WEP

- **有线等效隐私**(wired equivalent privacy，WEP)以为无线局域网**提供与有线局域网相同级别的安全保护**为目的，用于保护无线局域网中的**数据链路层的数据安全**。WEP包含以下三个要素：共享密钥K、初始向量(initialization vector，***IV***)和RC4流密码算法。

1.WEP数据加密及解密

- WEP采用对称加密算法RC4。RC4算法是一种**对称流密码体制**，可以采用64比特或者128比特两种长度的密钥。IEEE 802.11b规定，WEP使用64比特的加密密钥。这64比特长的加密密钥由两部分组成：40比特的WEP用户密钥K和24比特的初始矢量***IV***。

WEP数据加密流程

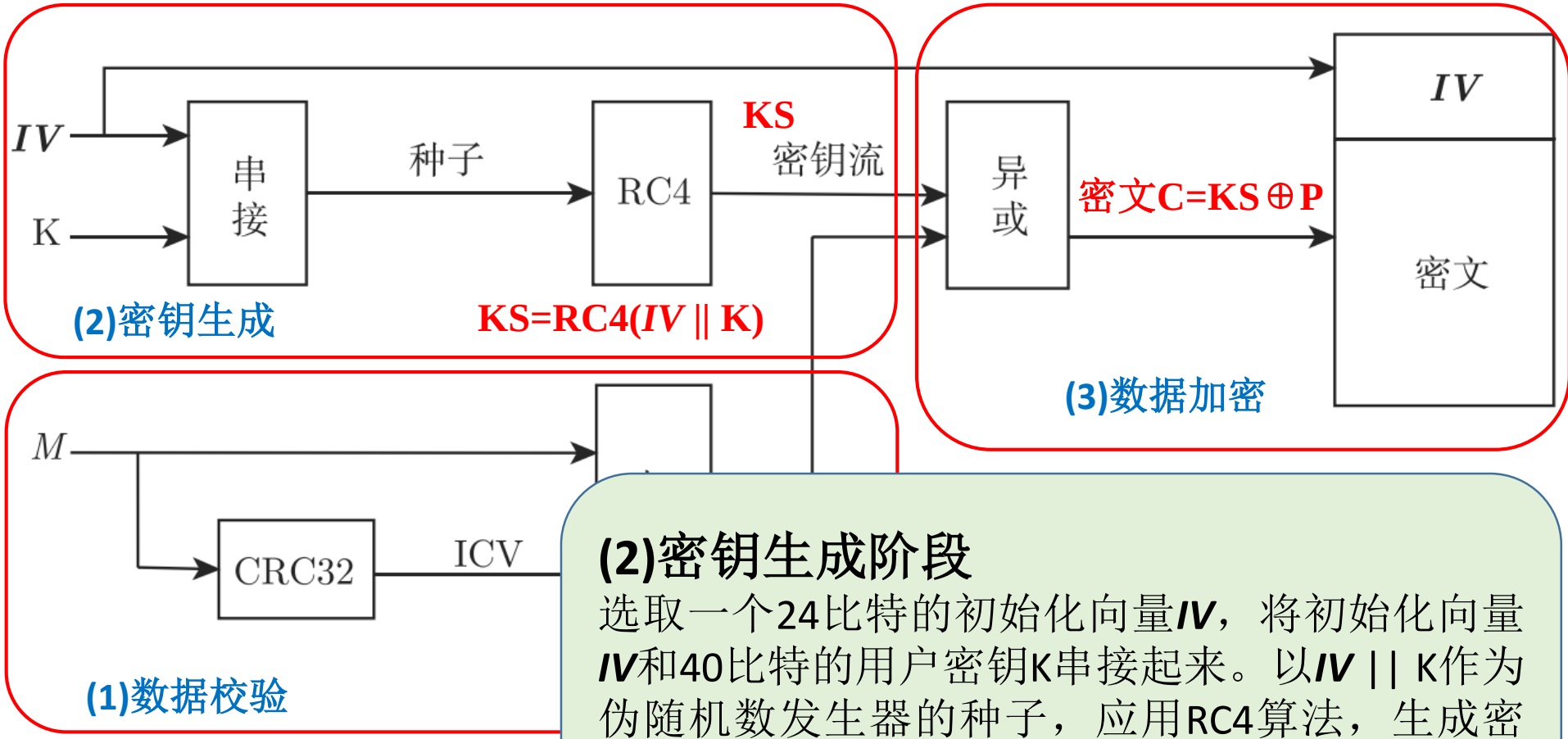


(1)数据校验阶段

对消息M计算完整性校验值(integrity check value，ICV)，使用的算法是CRC32：ICV=CRC32(M)。将ICV与M串接，得到明文P=ICV || M。

图11-1 WEP数据加密流程

WEP数据加密流程

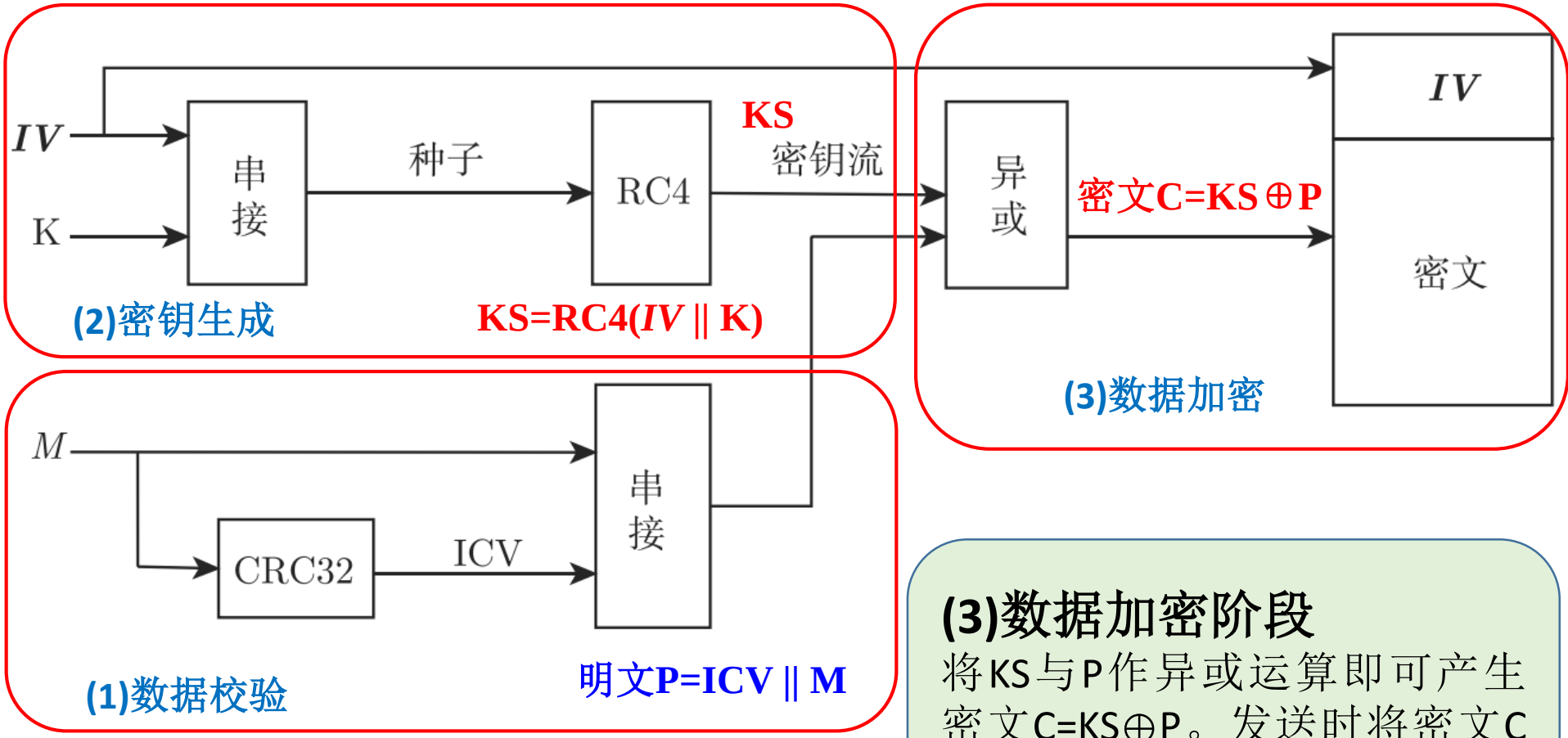


(2)密钥生成阶段

选取一个24比特的初始化向量***IV***，将初始化向量***IV***和40比特的用户密钥K串接起来。以***IV*** || K作为伪随机数发生器的种子，应用RC4算法，生成密钥序列(key sequence，KS)，即KS=RC4(***IV*** || K)，这是一个与P等长的伪随机序列。

图11-1 WEP数据加密流程

WEP数据加密流程



(3)数据加密阶段

将KS与P作异或运算即可产生密文C=KS⊕P。发送时将密文C和初始向量***IV*** 一起传输，即传输***IV*** || C。

图11-1 WEP数据加密流程

WEP的数据解密过程

(1)提取***IV***和密文C；

(2)将***IV***和密钥K一起送入，采用RC4算法的伪随机数发生器得到解密密钥流；

(3)将解密密钥流与密文相异或，得到明文消息M以及完整性校验值ICV；

(4)对得到的明文进行处理，采用相同的算法计算完整性校验值ICV；

(5)比较两个完整性校验值结果，如果相等则说明协议数据正确。

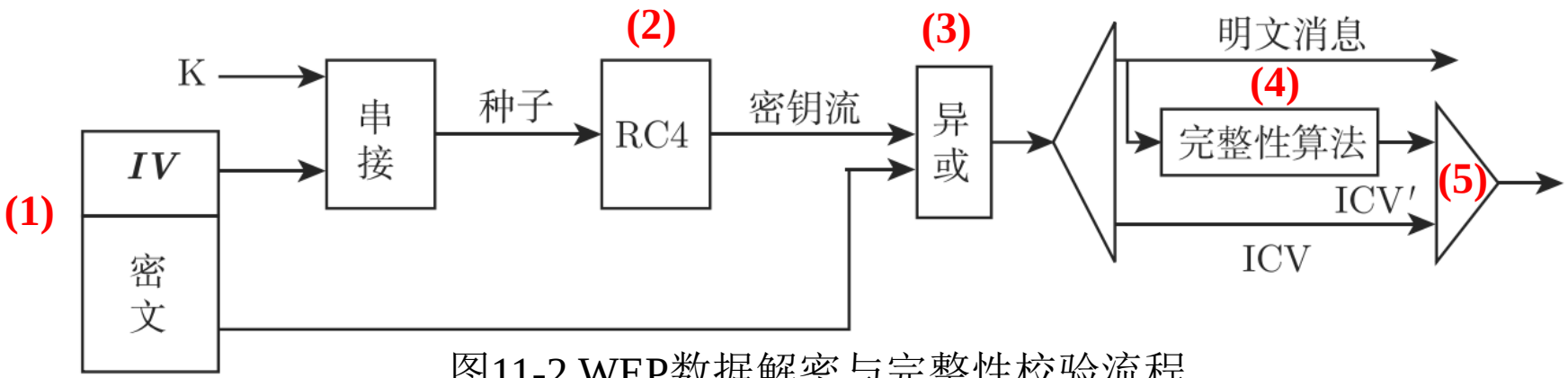


图11-2 WEP数据解密与完整性校验流程

WEP的MPDU
(MAC protocol data unit，MAC协议数据单元)结构

- IEEE 802.11b标准规定无线工作站和接入点可以共享的WEP加密密钥是有限制的，最多为4个。
- 在实际应用中，WEP帧中的Key ID决定具体使用哪个WEP用户密钥。
- WEP的MPDU(MAC protocol data unit，MAC协议数据单元)结构如图11-3所示。

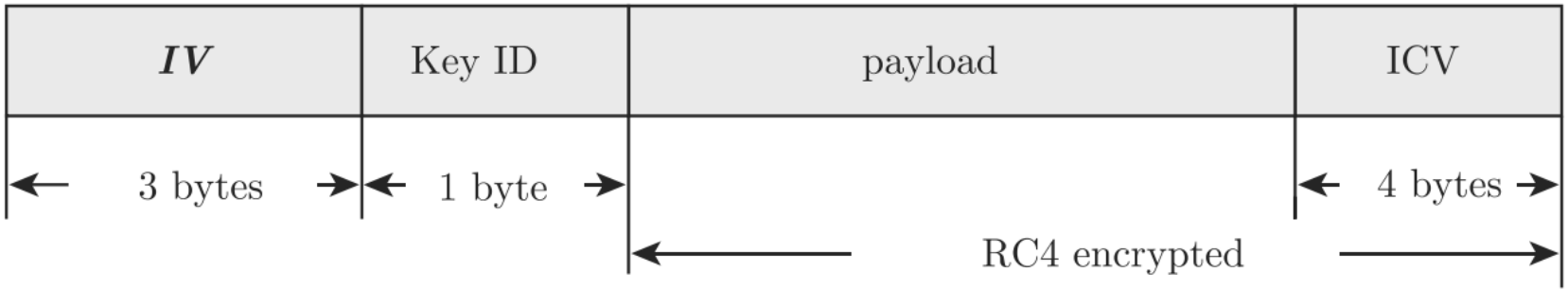


图11-3 WEP MPDU结构

2.WEP认证- 1)开放系统认证

- **开放系统认证是**IEEE 802.11的缺省认证方式。
- 这种认证经常被称为**“零认证”**，本质上是一种空认证机制，认证过程没有采用密码技术，甚至一个空的SSID就可以获得认证，安全性较差。
- **认证过程以明文方式进行**
  ① 无线站点发送一个包含自身ID的**认证请求**，其中未包含涉及认证的任何与客户端相关的信息。
  ② 若无线接入点的认证算法标识也为开放系统认证，则它返回一个包含认证成功或认证失败的**认证响应**。当无线站点收到包含认证成功的响应信息后，就表明通信双方相互认证成功。

2.WEP认证- 2)共享密钥认证

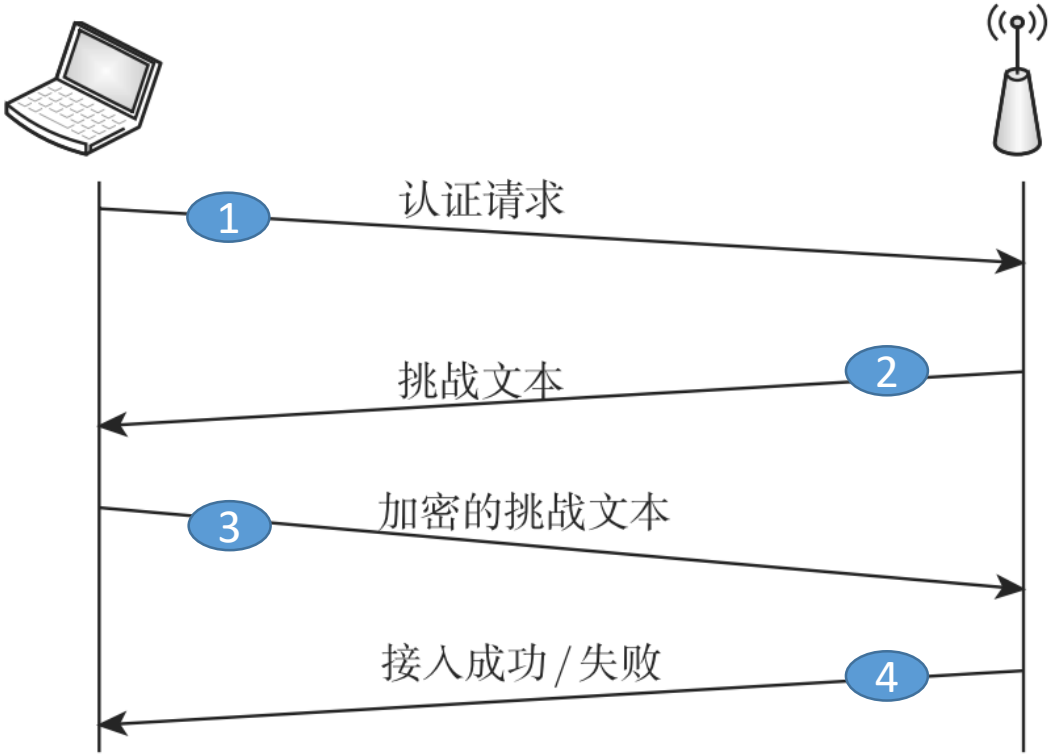


图11-4 共享密钥认证

- 采用挑战 / 响应方式，是基于共享密钥的身份认证机制
- 整个认证过程包括四步骤。

3.WEP密钥

- IEEE 802.11b以手工的方法将密钥输入到每个设备中。
- IEEE 802.11b允许最多4个密钥存储在每个设备上，每个WEP信息在传送时必须包括密钥编号(key ID)，只有发送设备和接收设备都采用相同的共享密钥，信息才能被正确地传送和解码。

- 现实当中，很多机构在设置了一个初始的WEP共享密钥后就永远不会变了，就必然会增加密钥丢失的可能性。这也会增加加密方案被破解的可能。

4.WEP的缺陷

1)静态共享密钥和*IV*重用

- WEP没有密钥管理的方法，使用静态共享密钥，通过***IV*** / shared key来生成动态密钥。静态密钥的安全强度是比较低的。
- 在WEP中，***IV***的取值空间为[0，2^{24} -1]。**当加密的数据包个数超过2^{24}时，*IV*必然发生重复**，如果此时没有更换密钥的话，便会出现若干个数据包用来加密的种子密钥发生重复，从而很容易被破解。
- 按照IEEE 802.11b中WLAN的最高传输速率11Mb/s来计算，传输1800字节大小的数据包，6小时后一定会出现重复。

4.WEP的缺陷- 2) CRC-32的漏洞

- WEP协议计算32位的循环校验(CRC)作为完整性校验值。
- CRC算法是线性的，所以CRC校验体现出了很强的数据关联性，违背了密码学的随机性原则，安全性也随之降低。
- 此外，CRC本身是一种简单的算法，加上之前提到的线性原则，攻击者只要在信息流中插入一定比特位后再调整CRC校验与其相符，就可以做到破解密钥。

4.WEP的缺陷- 3)认证的漏洞

- WEP协议中规定的身份认证是单向的，即只包含接入点对无线工作站的认证，而却没有无线工作站对接入点的认证，不能防止假冒接入点的问题。
- WEP协议中规定的共享密钥认证也容易导致认证伪造。因为在认证过程中，接入点发送给无线工作站的“挑战文本”是以明文方式发送的，而无线工作站发回给接入点的消息为加密之后的。如果攻击者同时截获了明文和密文，就很容易根据**RC4(IV，K)=C⊕P**恢复出密钥序列，从而获得认证数据中的有用信息，以此通过接入点的验证而获得网络资源的访问。
- 此外，WEP协议本身没有抗重放保护机制，因此对加密的报文可以随意重放，接收方无法识别该报文是发送方发送的还是攻击者重放的。

11.1.3 802.11i

- 因为WEP协议存在重大安全缺陷，IEEE成立了安全任务组，制定了802.11i安全标准，以解决无线局域网的安全问题。
- IEEE 802.11i关注**无线接入点(access point，AP)**和**无线工作站点(station，STA)**之间的安全通信，引入了**健壮安全网络RSN(robust security network)**的概念，定义了以下安全服务。
  A. **认证：**定义用户和网络的交互，以提供相互认证，并生成用于STA和AP之间无线通信的短期密钥。
  B. **访问控制：**对认证功能的增强，能与多种认证协议协同工作。
  C. **带消息完整性的机密性：**MAC层数据与消息完整性校验码一起加密以提供机密性和完整性。

IEEE 802.11i强安全网络操作的5个阶段

(1)发现阶段：STA和AP建立连接，决定保护通信机密性和完整性的协议、认证方法、密钥管理方法等。

(2)认证阶段：一个STA与一个AP相互认证，目的是只允许授权STA访问网络，并且向STA保证连接的是一个合法网络。STA和AP还产生一个共享的主密钥。

(3)密钥管理阶段：AP和STA执行一系列操作，由认证阶段生成的主密钥来产生各种密钥并保存于AP和STA。

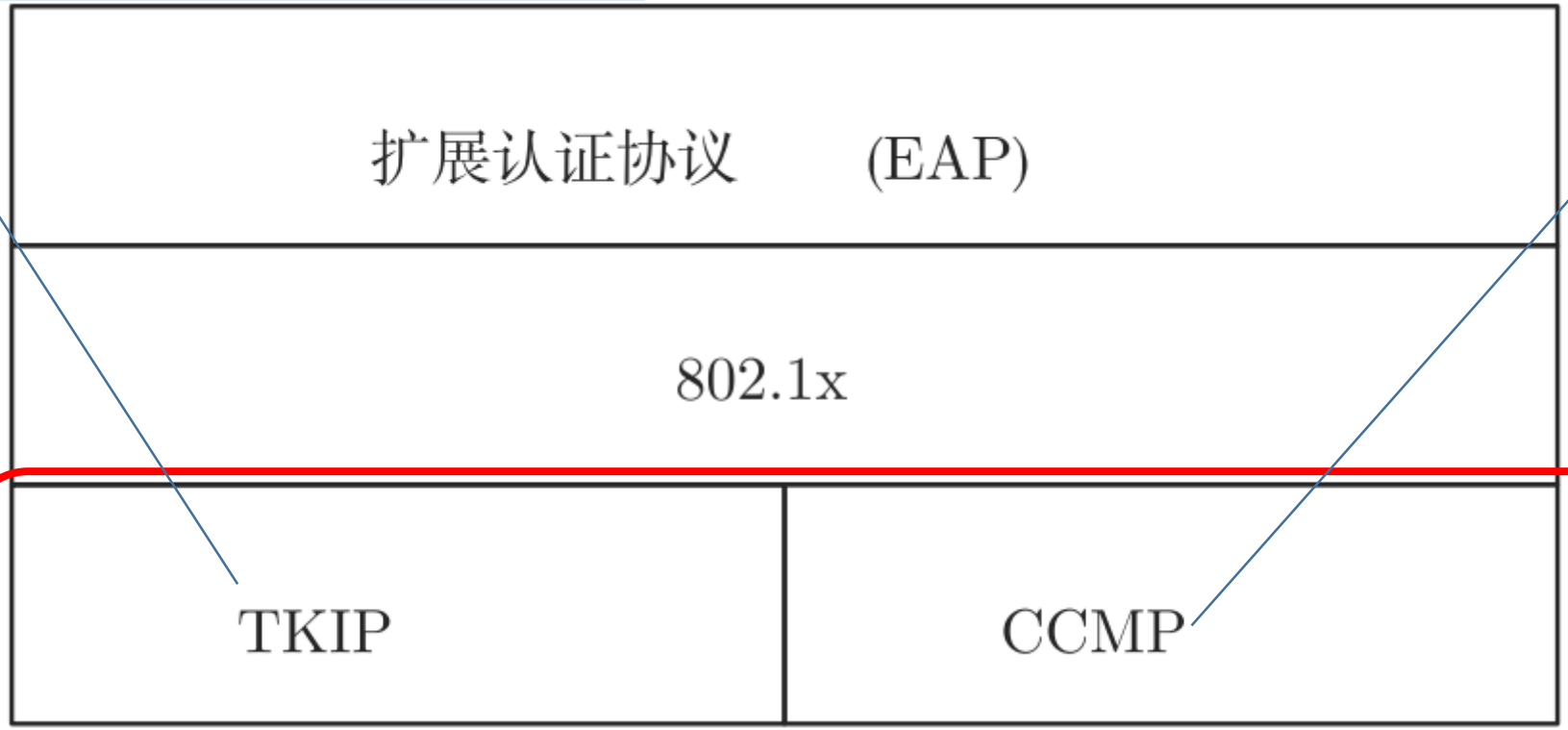
(4)安全通信阶段：AP和STA交换数据帧，交换的数据得到安全保护，以保证机密性和完整性。

(5)连接终止阶段：AP和STA拆除安全连接。

802.11i协议结构

TKIP(temporal key integrity protocol)

CCMP(counter-mode/CBC-MAC protocol)



两种数据加密机制，增强了WLAN中的数据加密和认证性能

图11-5 IEEE 802.11i协议结构

IEEE 802.11i支持的安全协议

① 加强的加密算法CCMP或TKIP，其中**必须实现基于AES的CCMP**。

② 动态的会话密钥。

③ 具有密钥管理算法。

④ 基于802.1x的、无线接入点和无线工作站点的**双向增强认证机制**。

⑤ 支持快速漫游和预认证。

⑥ 支持独立基本服务集(independent basic service set，IBSS)。

1. TKIP(数据加密和完整性)

- TKIP(temporal key integrity protocol)是一种对传统设备上的WEP算法进行加强的协议，目的是在不更新硬件设备的情况下，提升系统的安全性。
- TKIP与WEP 一样基于RC4加密算法，但相比WEP算法，**将密钥的长度由40位增加到128位，初始化向量的长度由24位增加到48位，解决了WEP密钥长度太短的问题**。

- TKIP对WEP进行了改进，引入了四种新机制以提高加密强度。

TKIP引入了四种新机制以提高加密强度

(1)每包一密钥(per-packet key)：

- 每个MAC数据包使用不同的密钥加密，该加密密钥通过将多种因素混合在一起而生成，安全强度大大提高。

(2) 消息完整性校验码(message integrity code，MIC)：

- TKIP实现了一个64位的消息完整性检查(MIC)，防止伪造的数据包被接受。

TKIP引入了四种新机制以提高加密强度

(3)具有序列功能的初始化向量*IV*：

- 利用TKIP传送的每一个数据包都具有独有的48位序列号，这个序列号在每次传送新数据包时递增，并被用作初始化向量和密钥的一部分，确保了每个数据包使用不同的密钥。

(4)密钥生成及定期更新功能：

- 解决了密钥管理的问题。

略

TKIP 的加密过程

TA：Transmit Address，一般是指AP的mac地址
TK：temporary key
TSC：TKIP sequence counter
MIC：message integrity check
MSDU：MAC service data unit

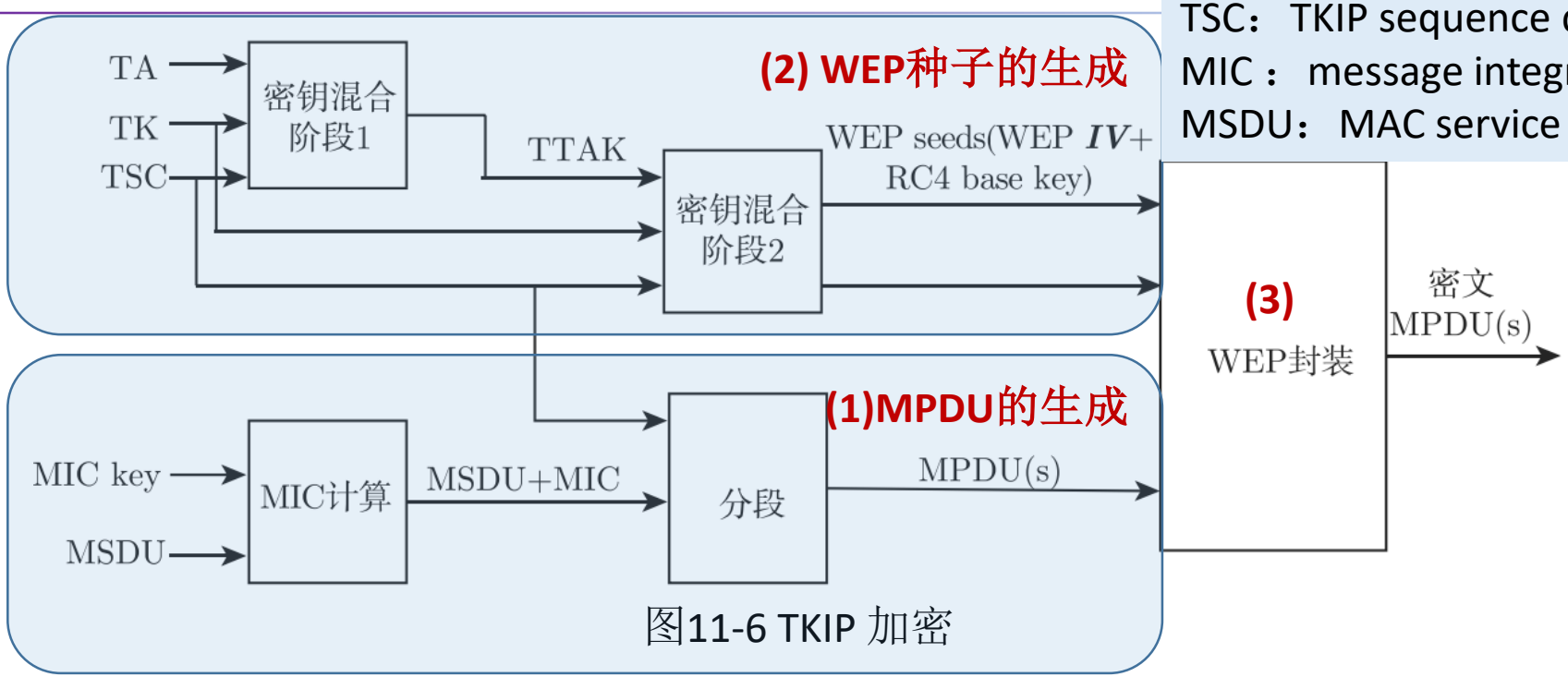


图11-6 TKIP 加密

TKIP 的加密过程包括以下几个步骤。

(1) MPDU(MAC protocol data unit, MAC 协议数据单元)的生成

(2) WEP 种子 (WEP seeds) 生成

(3) WEP 封装

略

TKIP MPDU 结构

- TKIP重用了WEP的MPDU格式，但扩展了4个字节，用作扩展***IV***字段，同时增加了8字节的MIC字段。
- MSDU-MIC可以封装在一个单一的MPDU，如果不行，则被分段，成为适当大小的多个MPDU，MIC可能只在最后的MPDU中出现。
- TKIP的MPDU结构如图11-7所示。

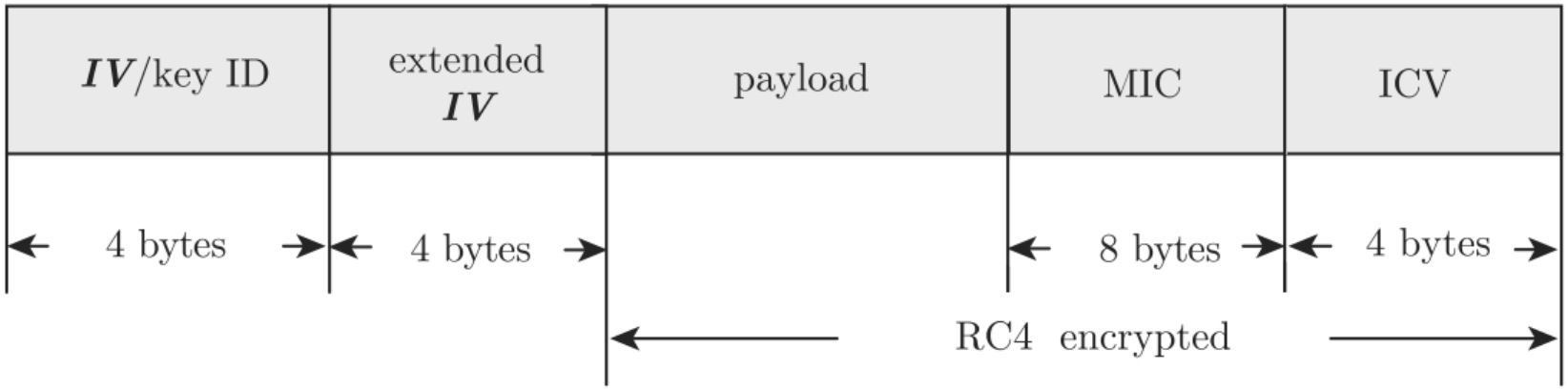


图 11-7 TKIP MPDU 结构

略

TKIP解密过程

- (1)在WEP解封一个收到的MPDU前，TKIP从IV中提取TSC和key ID。如果 TSC超出了重放窗口，则该MPDU被丢弃；否则，根据key ID定位TK，通过两个阶段的混合函数计算出WEP seed，计算过程和加密过程中的完全相同，不再赘述。
- (2) TKIP把WEP seed分解成WEP IV和RC4 base key的形式，把它们和MPDU 一起送入WEP解密器进行解密。
- (3)检查ICV，如果结果正确，则该MPDU将被组装入MSDU。
- (4)如果MSDU重组完毕，则检查MIC。如果MIC检查正确，TKIP把MSDU送交上一层；否则，MSDU将被丢弃。

TKIP从如下几个方面加强了WEP协议

(1) WEP缺少防止消息伪造和其他主动攻击的机制，TKIP中设计MIC以保证MSDU数据单元的完整性，从而可以有效抵抗这类攻击。

(2) TKIP中使用两个阶段的**混合加密函数**计算得到WEP seed。这个种子包括了WEP ***IV***，与TSC一一对应。同WEP中的静态密钥和24位的***IV***相比较，混合函数把密钥和数据包的属性结合起来，**可以有效地抵抗重放攻击，使密钥更安全**。

(3) TKIP**使用TSC**给它所发送的MPDU来排序，接收者会丢掉那些不符合序列的 MPDU。这提供了一种较弱的**抵抗重放攻击**的方法。

- 因为TKIP的总体安全性仍是取决于WEP核心机制，而WEP算法的安全漏洞是由于机制本身引起的，因此，**TKIP只是一种过渡算法**。

2. CCMP协议

- CCMP (counter-mode/CBC-MAC protocol) 基于AES算法和CCM模式，由两个部分组成：

① 加密模式(CTR counter mode)，用于保证数据的私密性；

② 密码块链式消息认证码(CBC-MAC, cipher block chaining message authentication code)模式，用于数据完整性校验。

- CCMP是802.11i强制使用的加密方式，为WLAN提供了加密、认证、完整性和抗重放攻击的能力，**能解决WEP中出现的所有问题。**

略

CCMP MPDU结构

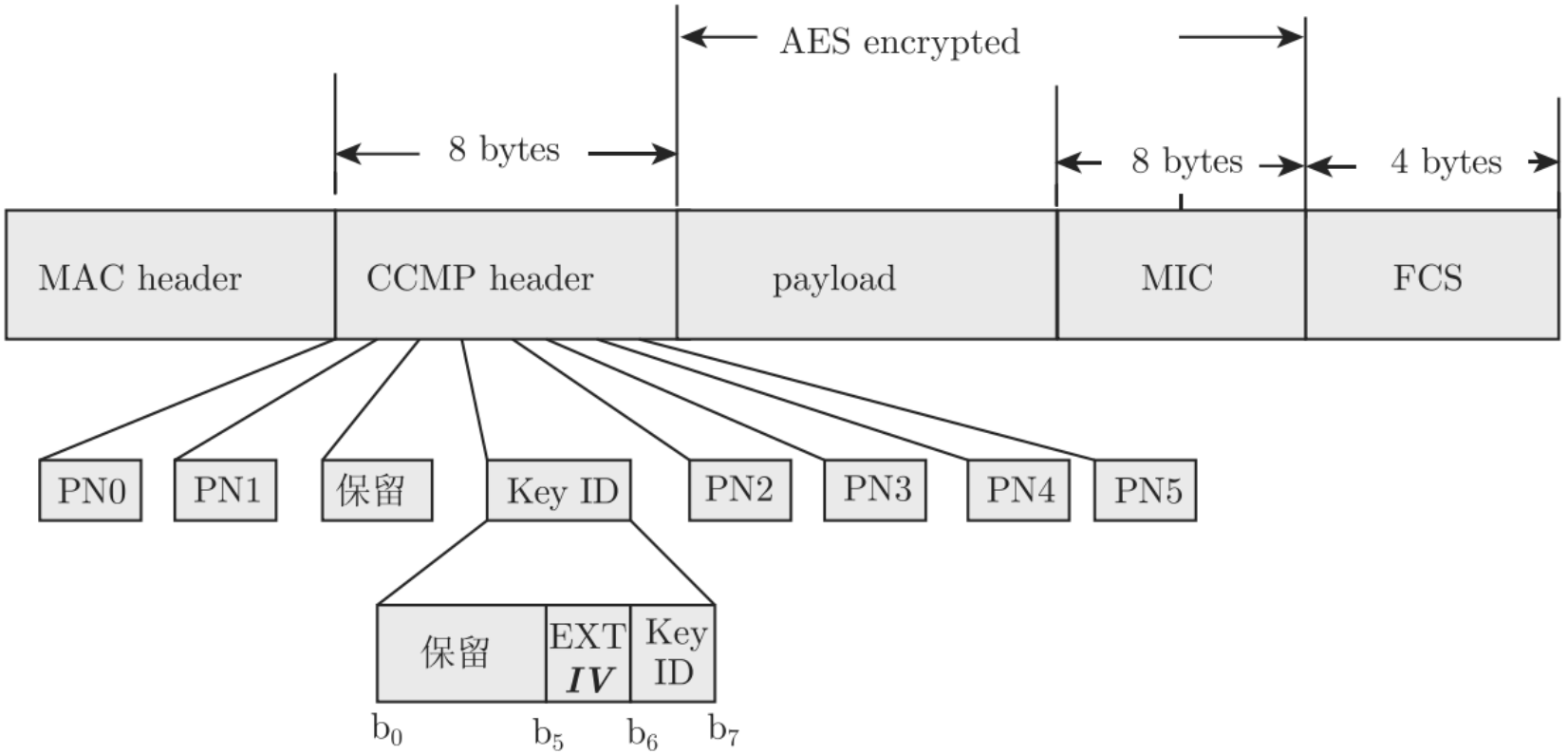


图11-8 CCMP MPDU结构

略

CCMP的正向封装过程实现了MPDU的加密和认证

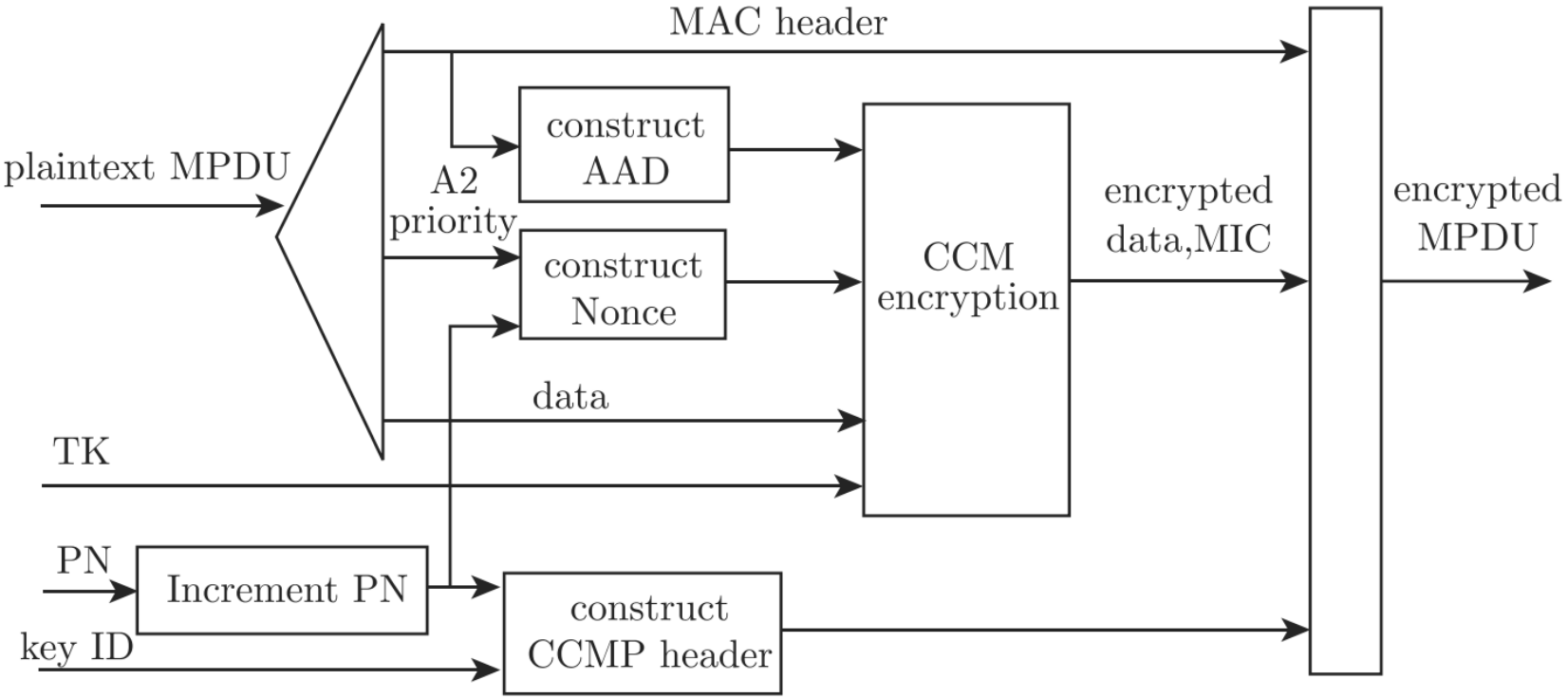


图11-9 CCMP封装过程

略

CCMP MPDU的解封装

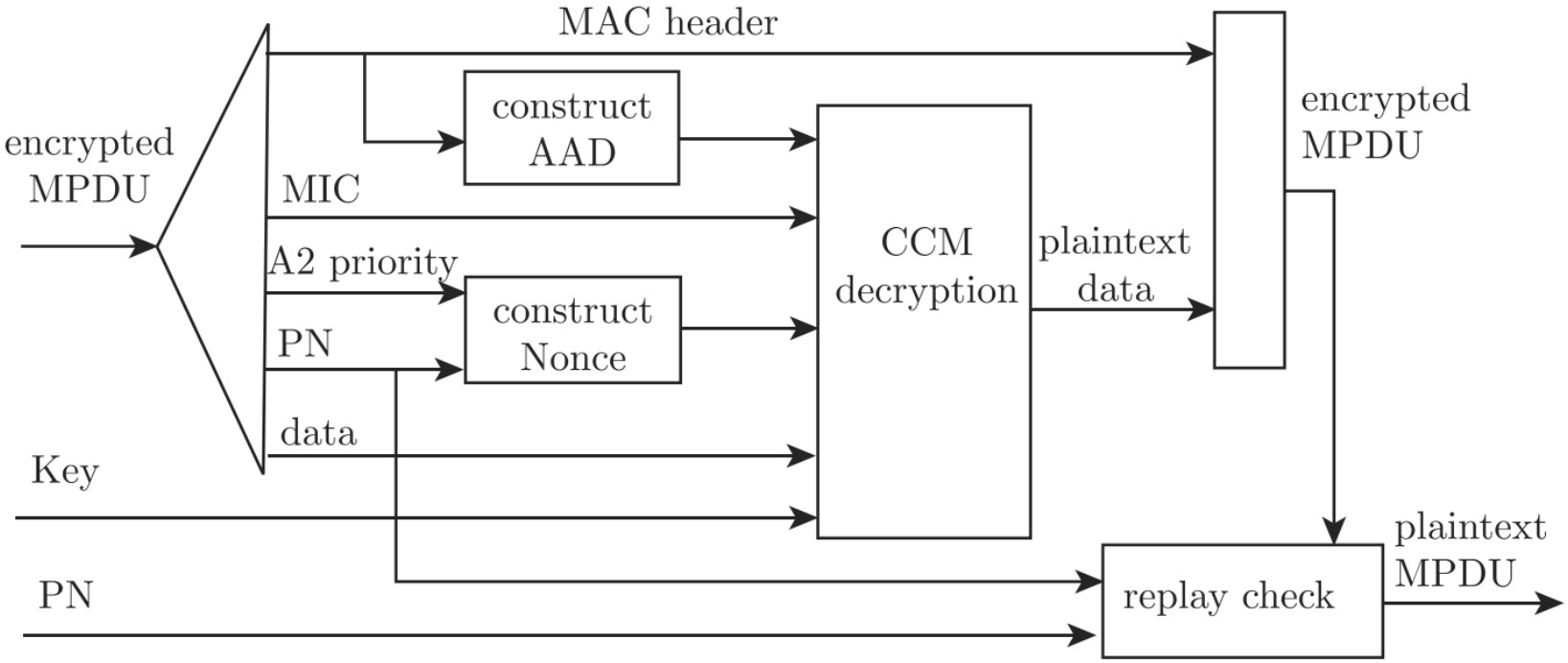


图11-10 CCMP解封装过程

3.认证协议

- 802.11i中的认证、授权和接入控制主要是由三个部分配合完成的，分别是802.1x标准、EAP协议和RADIUS协议。

1) 802.1x

- 802.1x的认证模型包含三个实体：
  - ① 请求者(supplicant)：STA
  - ② 认证者(authenticator)：AP
  - ③ 认证服务器(authentication server，AS)：
    - AS通常是网络中的一个有线连接的独立设备，但是也可以集成到AP中。

802.1x认证过程

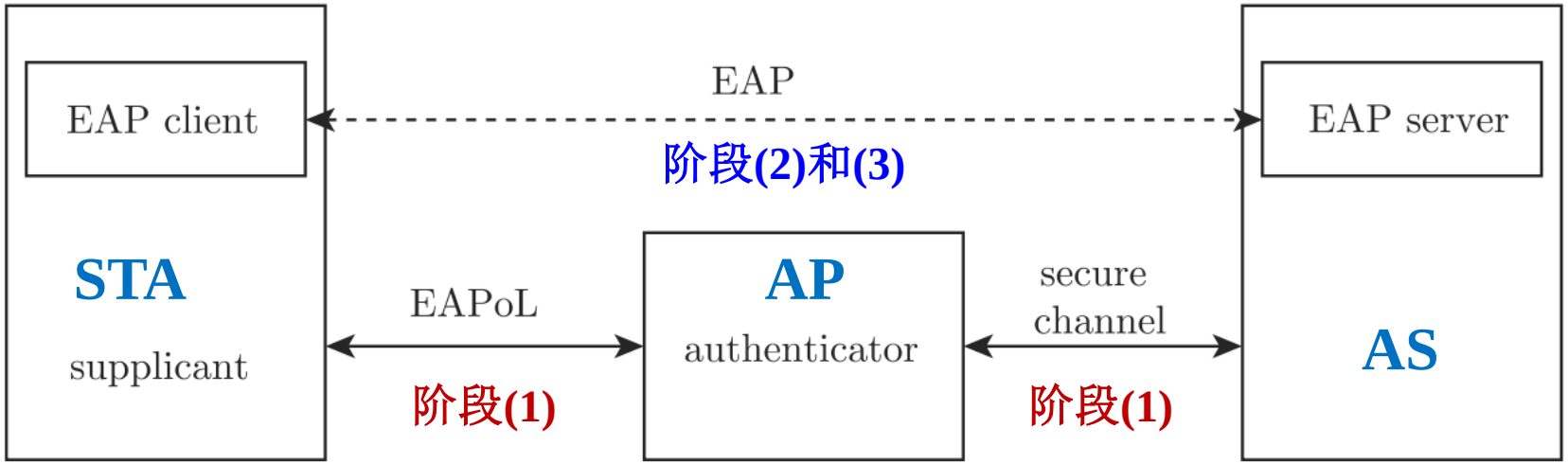
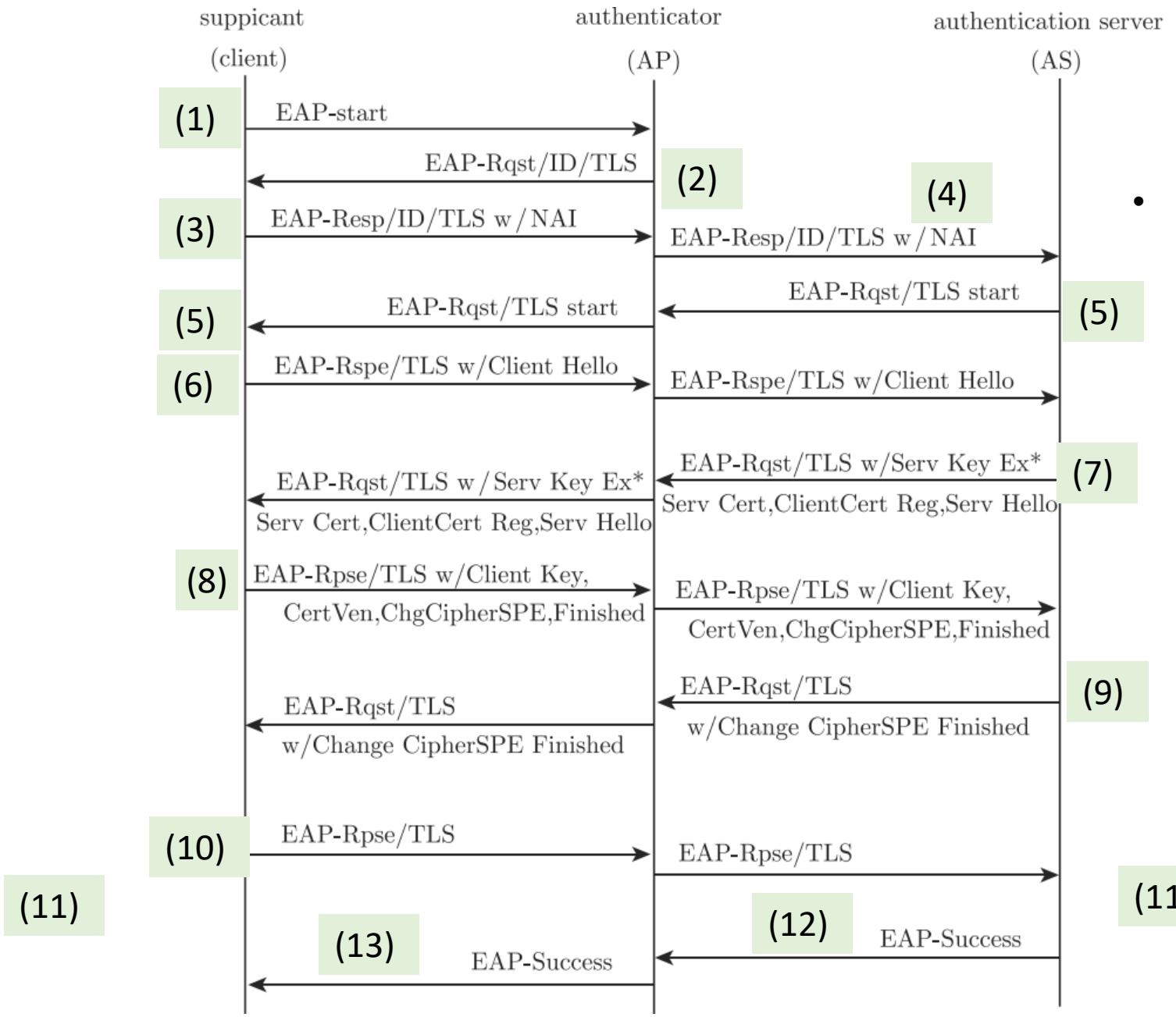


图11-11 802.1x认证结构

- (1)**连接到AS**：STA向它的AP发送一个请求以连接到AS。AP识别这个请求并给AS发送一个访问请求。
- (2) **EAP交换**：这个交换让STA和AS相互授权。
- (3)**安全密钥分发**：一旦认证完成，AS和STA产生一个主会话密钥(master session key，MSK)，此密钥也被称为AAA密钥(authentication、authorization、accounting)。STA和AP进行安全通信所需的加密密钥都从MSK产生。

2) EAP（extensible authentication protocol）

- EAP可以和802.1x很好地配合使用，因为802.1x专门定义了在LAN上运行EAP的报文格式EAPoL。EAPoL在原有的EAP报文外面增加了一层封装，使得EAP报文适合在局域网传输。
- **802.11i**并没有限制采用哪些协议作为上层认证协议，但规定了高层认证协议必须满足双向认证的要求，并**推荐采用EAP-TLS方法**。
- **EAP-TLS是一种基于TLS的认证方式**，认证服务器与请求者采用TLS协议协商会话密钥，该协议要求双方都要有公钥证书。



- 无线局域网环境下EAP-TLS认证过程

图11-12
802.1x认证结构

3) RADIUS

- RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证）协议是一个应用普遍的AAA（Authentication, Authorization, Accounting）协议，最初为拨号网络设计，基于IP网络。

- AP与AS之间的交互协议不是802.11i关注的重点，在此不再详述。

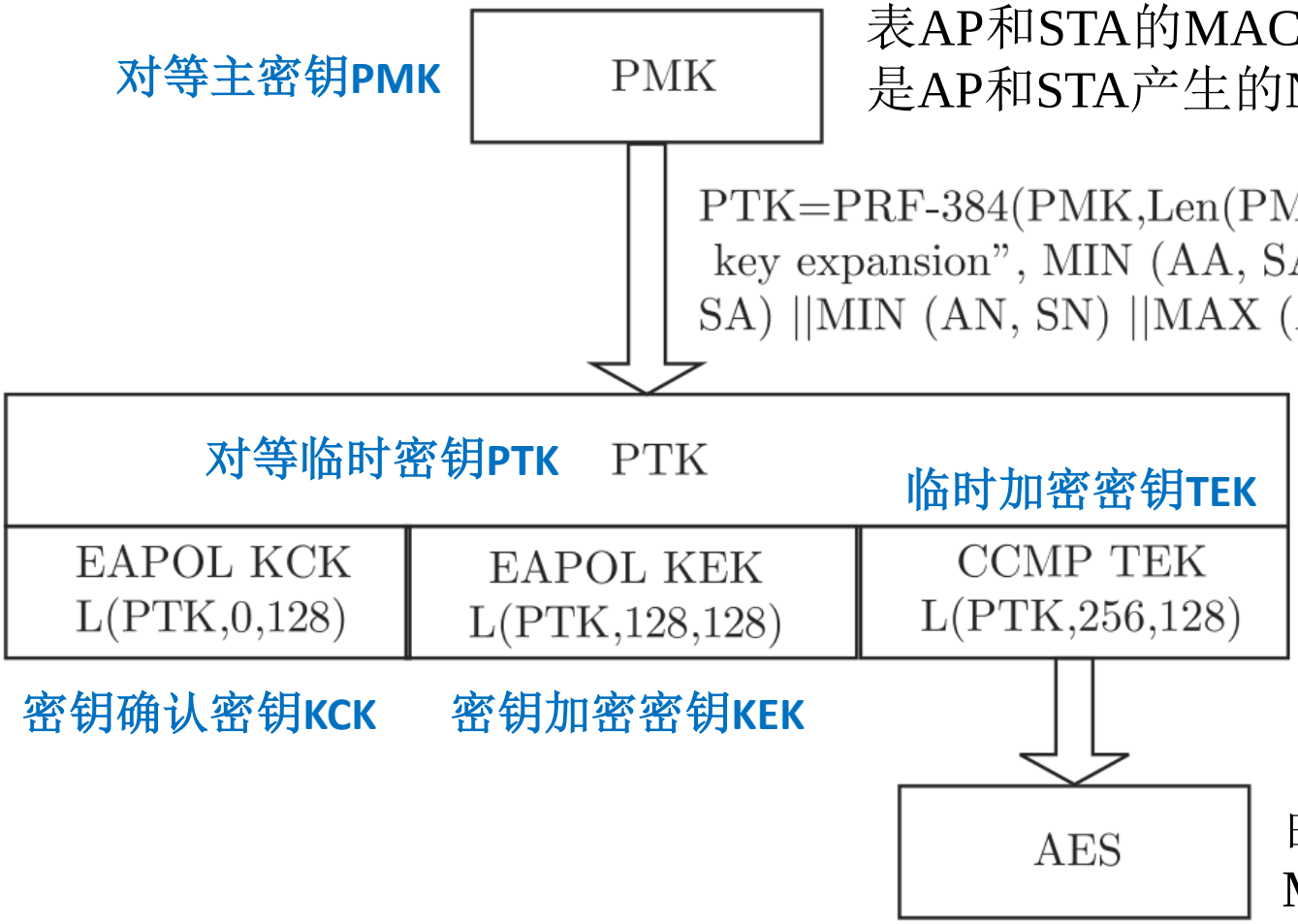
4.密钥管理

1)密钥层次

- 在802.11i中，存在多个层次的密钥。
- 认证成功后，无线工作站STA和认证服务器AS各自生成32字节的**对等主密钥(pairwise master key，PMK)**。PMK生成的方法与认证方式相关。如果是EAP认证，则由认证过程得到EAP主密钥(主会话密钥MSK)，再由MSK派生出对等主密钥PMK(通常是取MSK前面若干长度的比特组成PMK)。认证服务器AS将密钥材料安全地传送到认证者AP，从而使AP生成相同的PMK。
- **PMK处于密钥层次的第一级。**

AES密钥导出层次

Len()是求长度函数，AA和SA分别代表AP和STA的MAC地址，AN和SN则是AP和STA产生的Nonce(伪随机数)



由 TEK 根 据 CBC-MAC算法导出AES加密密钥

图11-13 AES密钥导出层次

4.密钥管理— 2)四步握手

图11-14 四步握手流程图

4.密钥管理— 3)组密钥更新

组密钥握手机制用来向STA发送新组密钥GTK

图11-15 组密钥更新流程图

5. RSNA建立过程

- IEEE 802.11i的**强安全网络连接(robust security network association，RSNA)**建立过程包含三个实体：申请者(STA)、认证者(AP)和认证服务器（如Radius服务器）。

大体上，RSNA建立过程可分成6个阶段。

(1)网络和安全能力发现：

(2) 802.11认证和连接：

(3) EAP/802.1x/RADIUS认证：

(4) 四步握手：

(5) 组密钥握手：

(6) 安全数据传输：

一个例子：华为路由器WS5200

11.2 移动通信系统的安全

- 移动互联网包括了以下几个要素：
  I. **无线移动通信网络**，包括2G、3G和4G等，提供接入服务；
  II. **公众互联网**，即Internet，提供内容服务；
  III. **移动通信终端**，包括手机和PDA等。

- 移动互联网十分严格地强调对用户隐私和用户行为的保护，比传统互联网具有更高的安全性要求。

11.2.1 GSM的安全(2G)

- 移动通信系统首先必须解决两个问题：

① **第一，对用户进行认证，防止未注册用户的欺骗性接入；**

② **第二，对无线路径加密，以防止第三方窃听。**

- 此外，移动台的位置更新过程也将成为系统的安全薄弱环节，因为这意味着即使是在非通话期间，也有可能对用户位置进行跟踪。因此，**移动通信系统还应能提供用户身份保护，防止用户位置泄露。**

1.GSM安全机制

- 每个GSM用户用**国际移动用户识别码IMSI**唯一标识，并由网络统一分配**用户认证密钥Ki**。**IMSI和Ki**一起构成了网络**籍以鉴别用户**的重要**“身份证件”**。
- 而GSM认证与加密方案的一个设计要点就是保证这一“身份证件”永远无需在无线路径上传输（除非是在网络数据库故障之类的特殊场合）。
- GSM的安全机制包括了以下几个方面的功能：

  ① 用户身份认证
  ② 用户身份保密
  ③ 用户数据保密以及信令数据保密

安全信息在整个系统中的分布情况

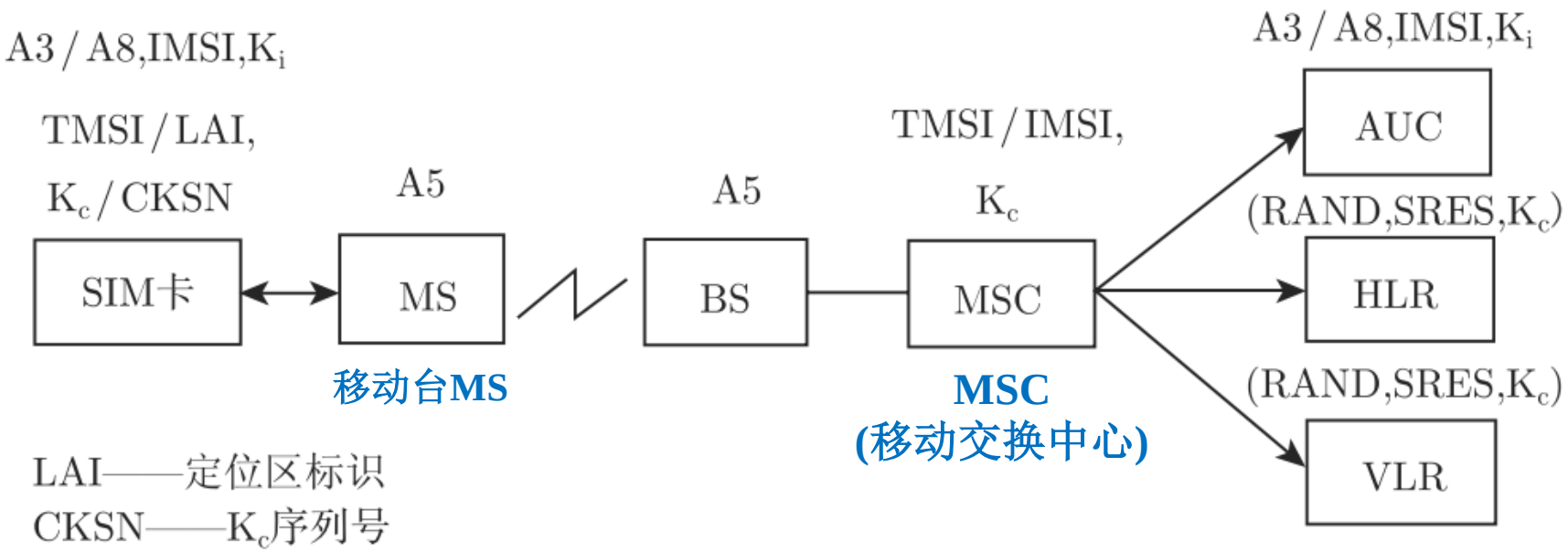


图11-16 安全信息在整个系统中的分布情况

- GSM在无线路径上的传输是以突发脉冲为传输单位的。一个普通突发脉冲包含114比特的用户数据，因此，在无线路径两端的加 / 解密操作都是在一个突发脉冲的114比特的基础上进行的。

A3/A8和A5算法的外部规范

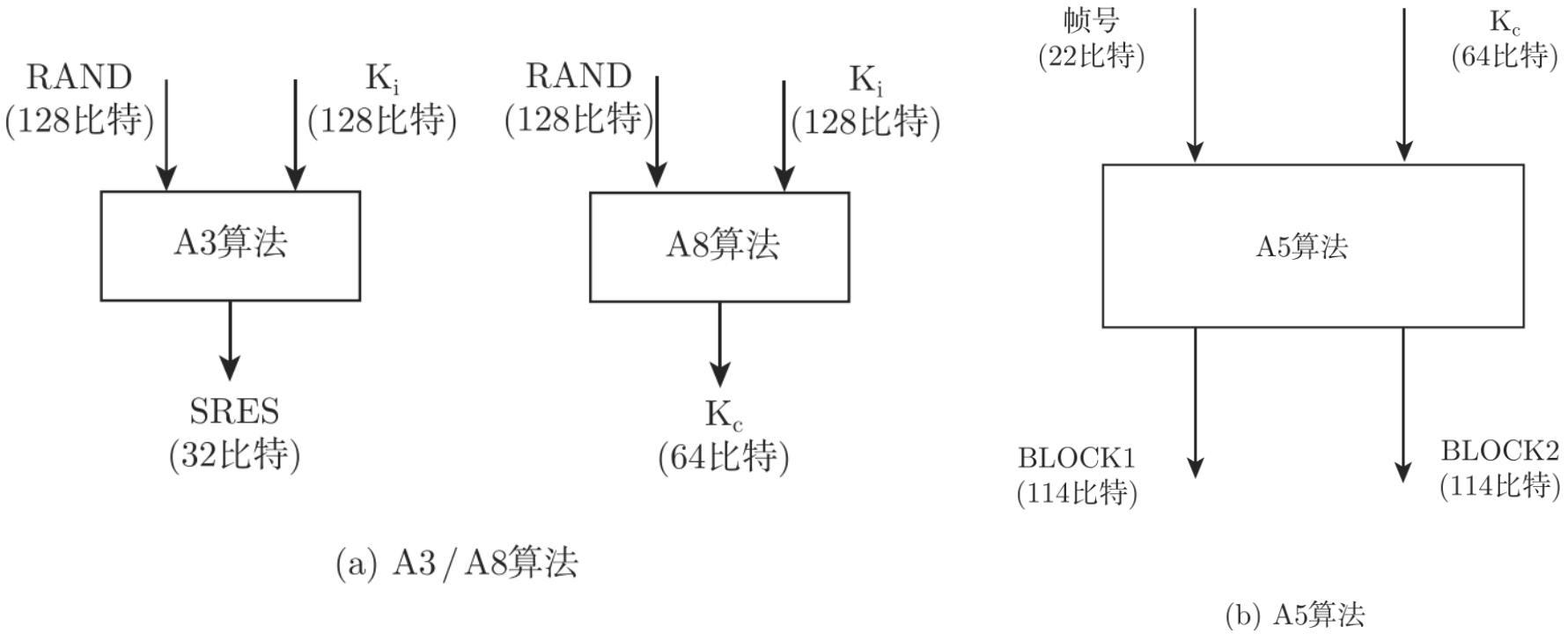


图11-17 A3/A8和A5算法外部规范

1.GSM安全机制— 1)用户身份认证

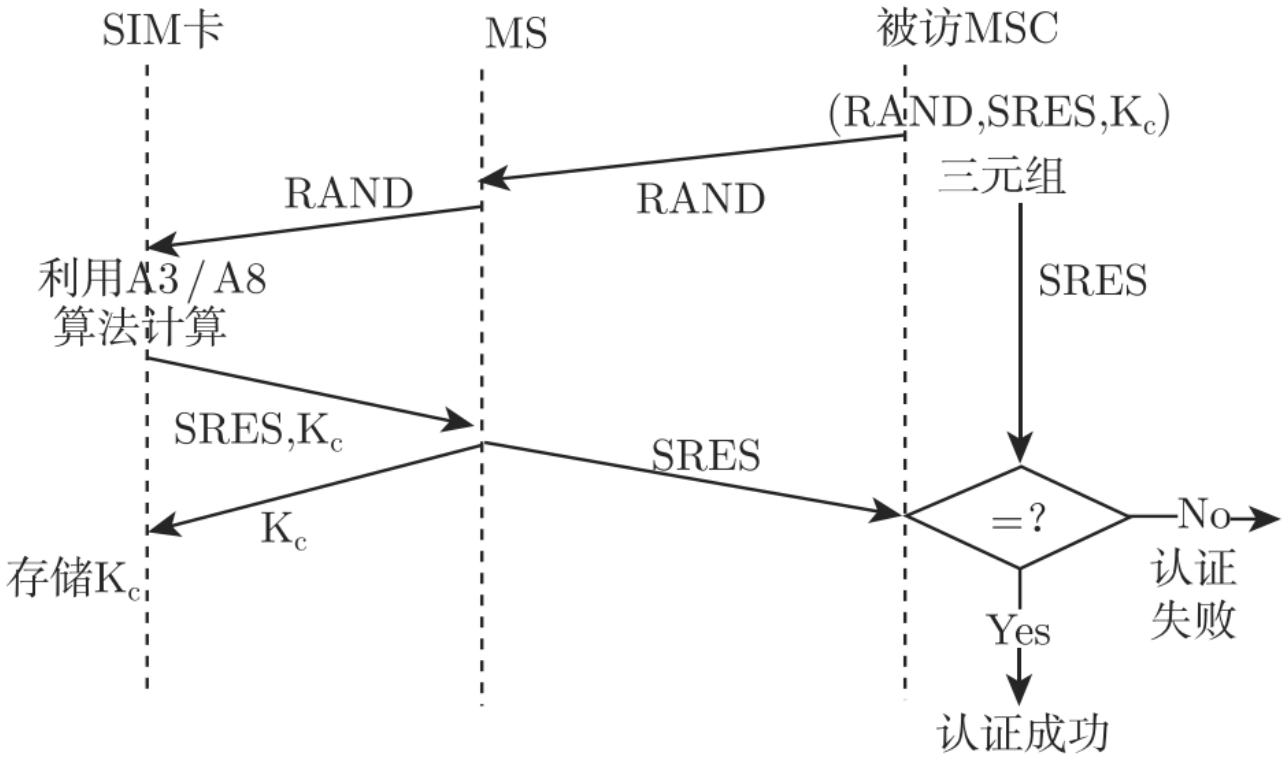


图11-18 GSM用户认证与密钥生成

1.GSM安全机制— 2)信令及数据保密

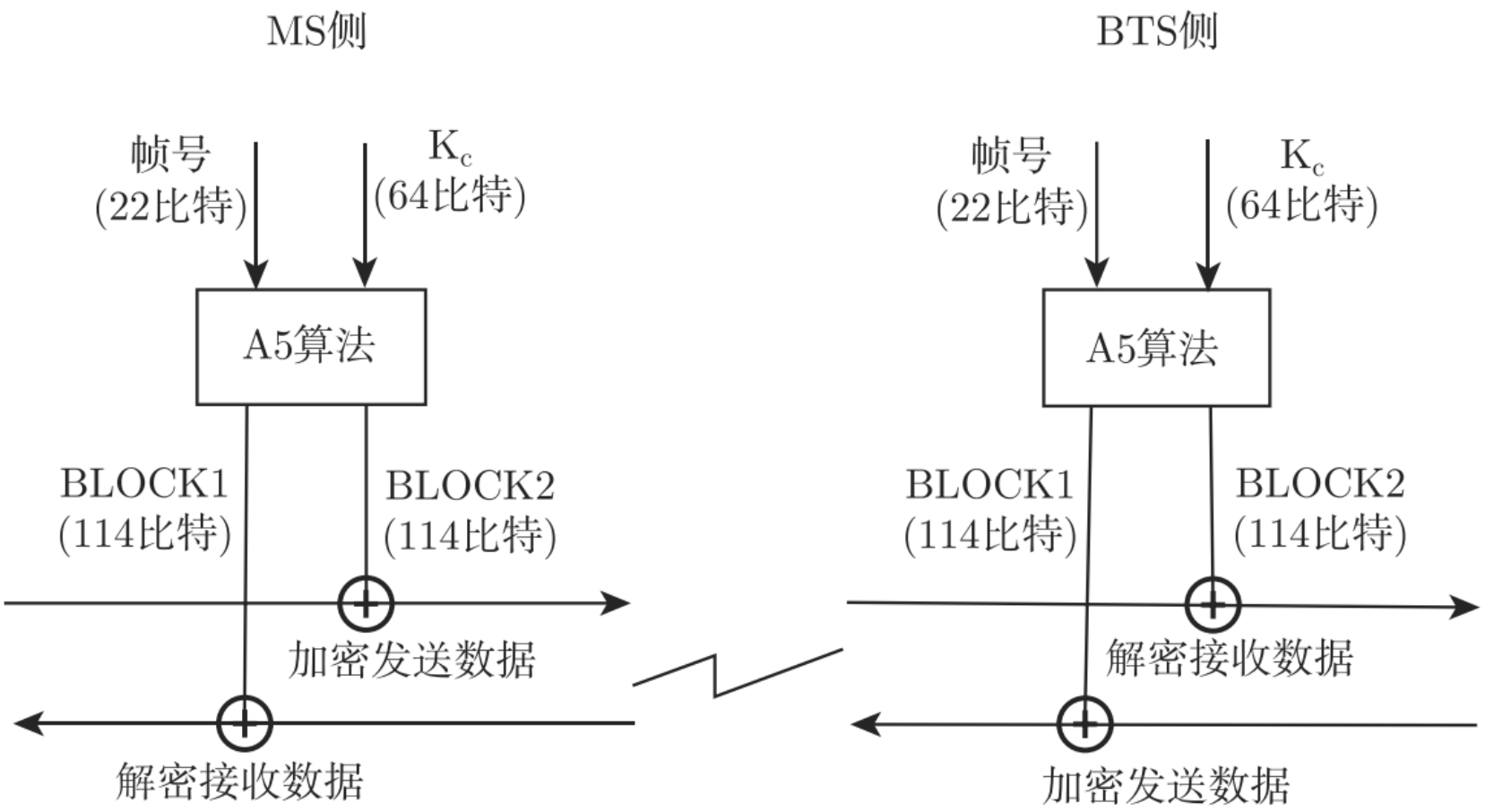


图11-19 GSM加密模式传输

1.GSM安全机制— 3)用户身份保密

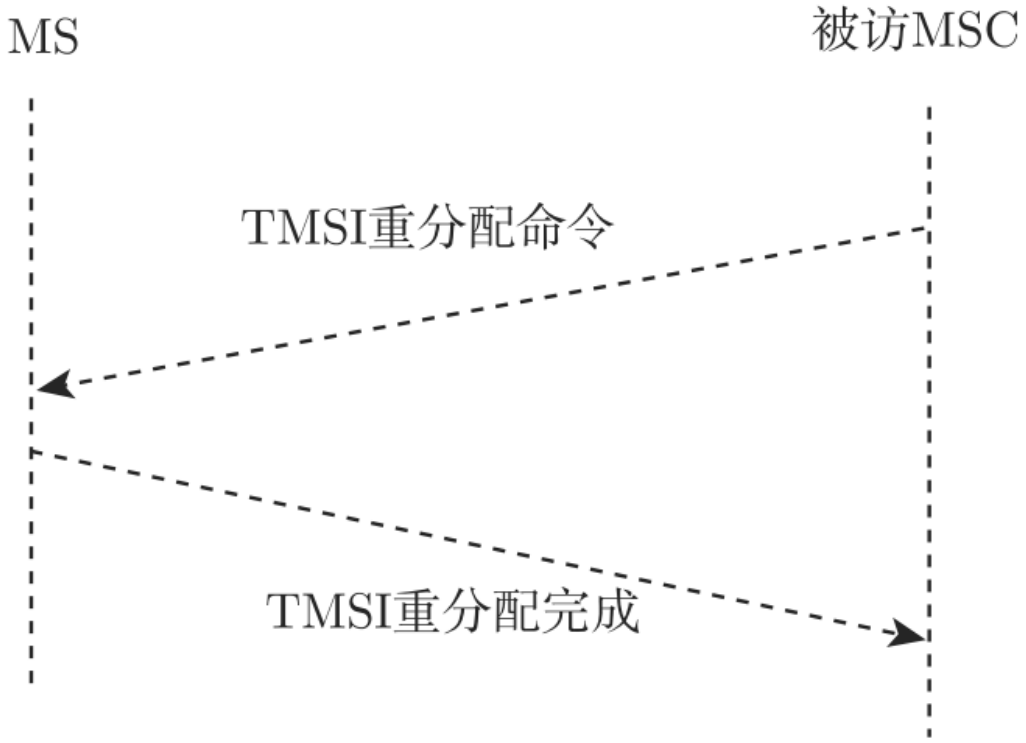


图11-20 TMSI的分配

GSM为每个用户分配临时移动用户识别码TMSI

2.认证方案

- GSM的认证方案采用了单钥体制，其认证协议为典型的“问—答”机制，并只对用户进行单向认证。
- 由于公钥体制具有较高的安全性，且更易于密钥的管理，较单钥体制有许多优点。目前限制公钥体制应用的主要因素是其计算量大。但随着公钥密码算法的发展（例如，算法所需计算量在通信双方的分布更加不均匀）以及移动台本身计算能力的提高，在未来的数字移动通信网（个人无线通信网）中，采用双钥体制将会是一种趋势。
- 通过采用更复杂的认证协议，双向认证也将成为可能。

3.加密算法A5

- 目前，所有国家都使用一种A5算法，该算法属于GSM MoU(理解备忘录)的财产，受版权保护。
- 由于保密原因，只有其外部规范是公开的，A5算法也因此成了众多密码学者研究分析的对象。
- 考虑到出口限制，A5算法还有A5/1和A5/2不同的版本，其中A5/2算法的强度稍弱些，可以理解为密钥长度自效位数的减少。
- 但即使是不采用任何A5算法，GSM也远比模拟蜂窝系统安全。

4.密钥长度

- 目前普遍的看法是采用128比特的密钥，像国际数据加密算法IDEA的密钥即为128比特，密钥长度为56比特的DES因此极有可能在不久后遭到淘汰。
- 相对而言，A5算法的密钥长度只为64比特，并且如果其有效密钥长度果真仅为40比特的话，则只能在短时间内对信息提供保护。
- **一般认为，普通蜂窝电话的内容受保护的时间应该在星期这个数量级上，因此在现阶段A5算法应该还是能胜任的。**

11.2.2 GPRS的安全

- 随着无线数据业务的迅速发展，移动数据业务已经从传统的电路交换方式发展为分组交换方式。
- **通用分组无线业务(GPRS, General packet radio service)**是一种新的数据业务，它可以在现有GSM网络基础上，通过增加一些网络节点给移动用户提供无线分组接入服务，提供端到端的、广域的无线IP连接。
- GPRS是GSM网络向第三代移动通信系统过渡的一项2.5代(**2.5G**)通信技术，在许多方面都具有显著的优势。
- GPRS的安全机制在GSM的基础上得到了加强，包括身份保密、身份认证、用户数据加密、信令数据加密以及其他由GPRS系统提供的GSM标准之外的安全机制。

1.GPRS网络结构

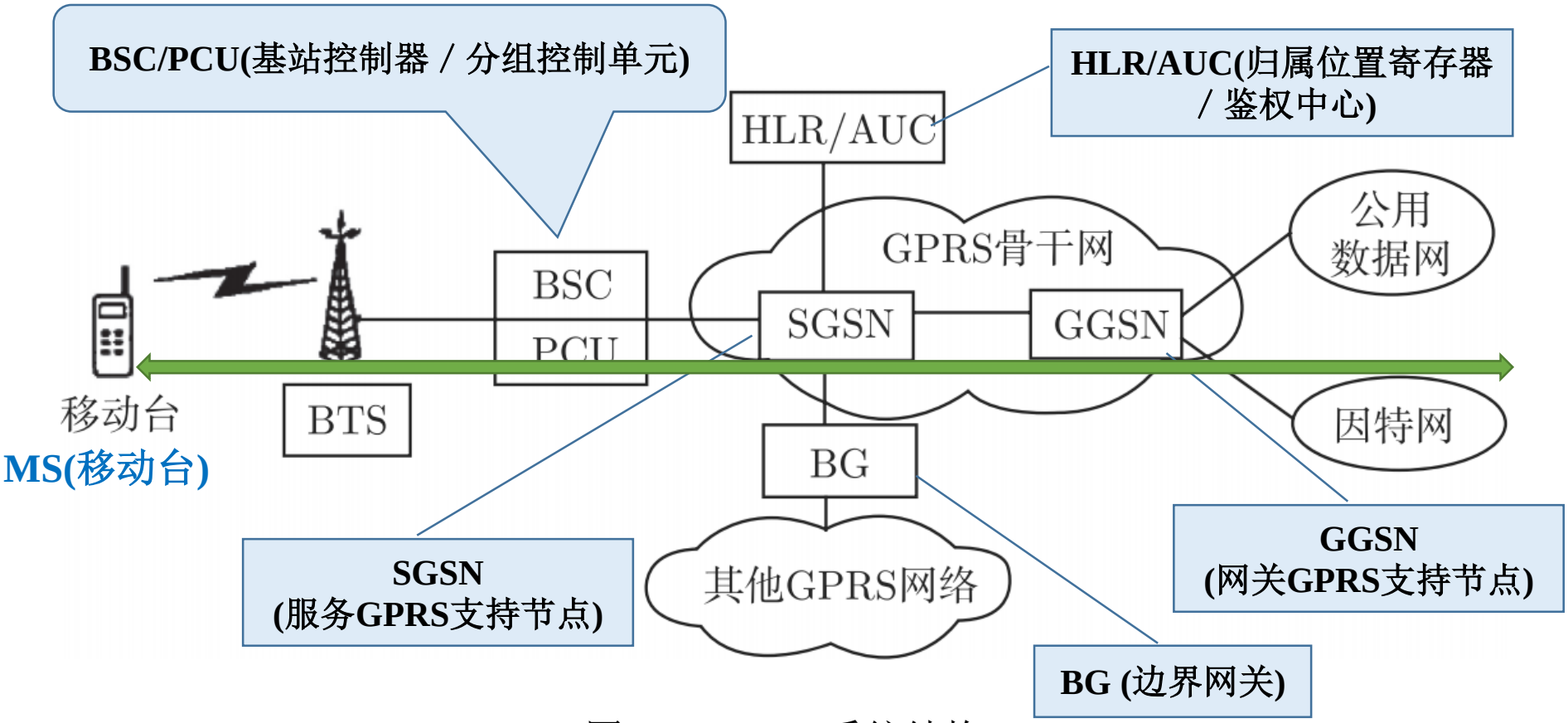


图11-21 GPRS系统结构

GPRS网络是在现有GSM网络中增加分组控制单元(PCU)、服务GPRS支持节点(SGSN)和网关GPRS支持节点(GGSN)而实现的，使得用户能够在端到端分组方式下发送和接收数据。

GPRS业务的基本流程

① 电脑或其他数据设备通过串行或无线方式连接到GPRS移动台上；

② GPRS移动台与基站通信，但与电路交换式数据呼叫不同，GPRS分组是从基站经分组控制单元处理后发送到SGSN，而不是通过移动交换中心连接到语音网络上；

③ SGSN与 GGSN进行通信，GGSN对分组数据进行相应的处理，再发送到目的网络，如因特网或X.25网络；

④ 来自因特网且标识有移动台地址的IP包，由GGSN接收，再转发到SGSN，继而传送到移动台上。

2.GPRS网络的安全机制

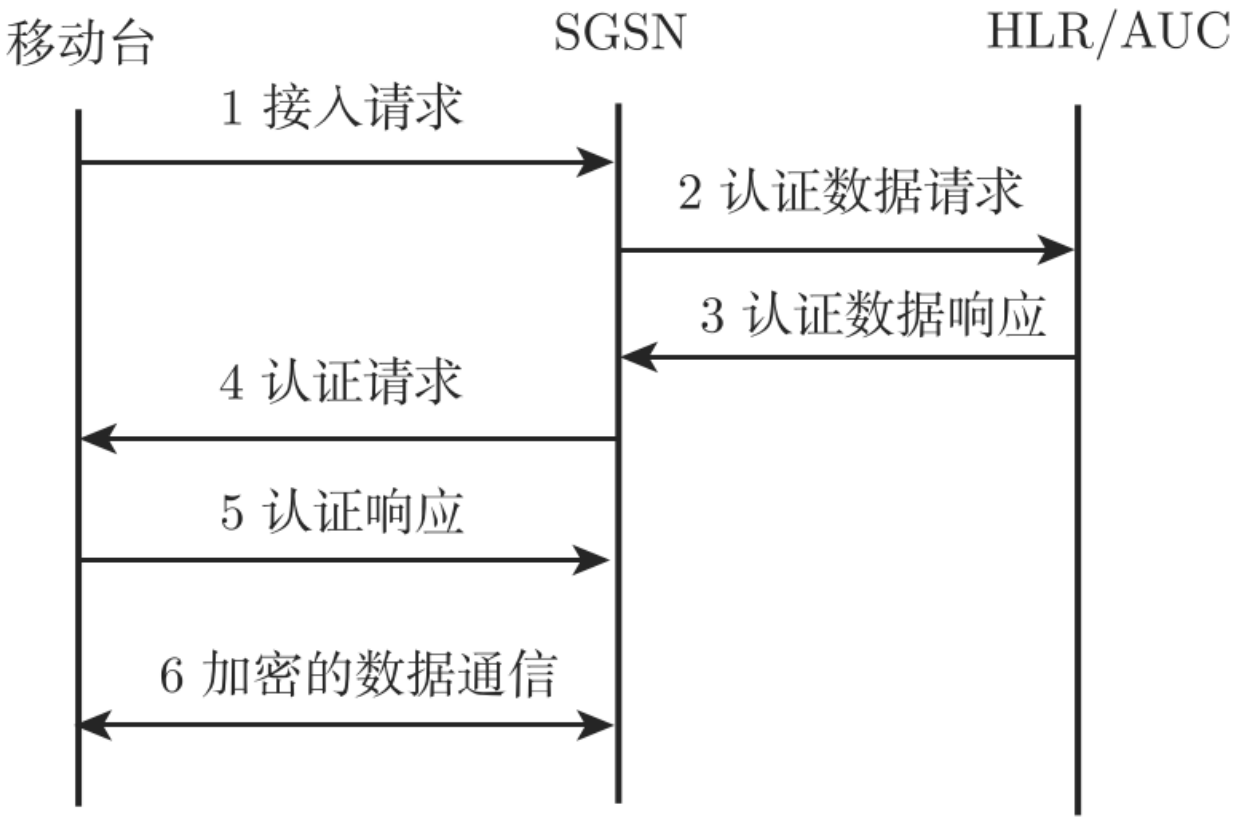


图11-22 GPRS系统的认证过程

1) GPRS网络的安全机制

- GPRS系统的身份认证由移动台、SGSN和HLR/AUC共同完成
- 认证是基于移动台和 HLR/AUC之间的共享密钥K_i。

2)信令数据和用户数据加密

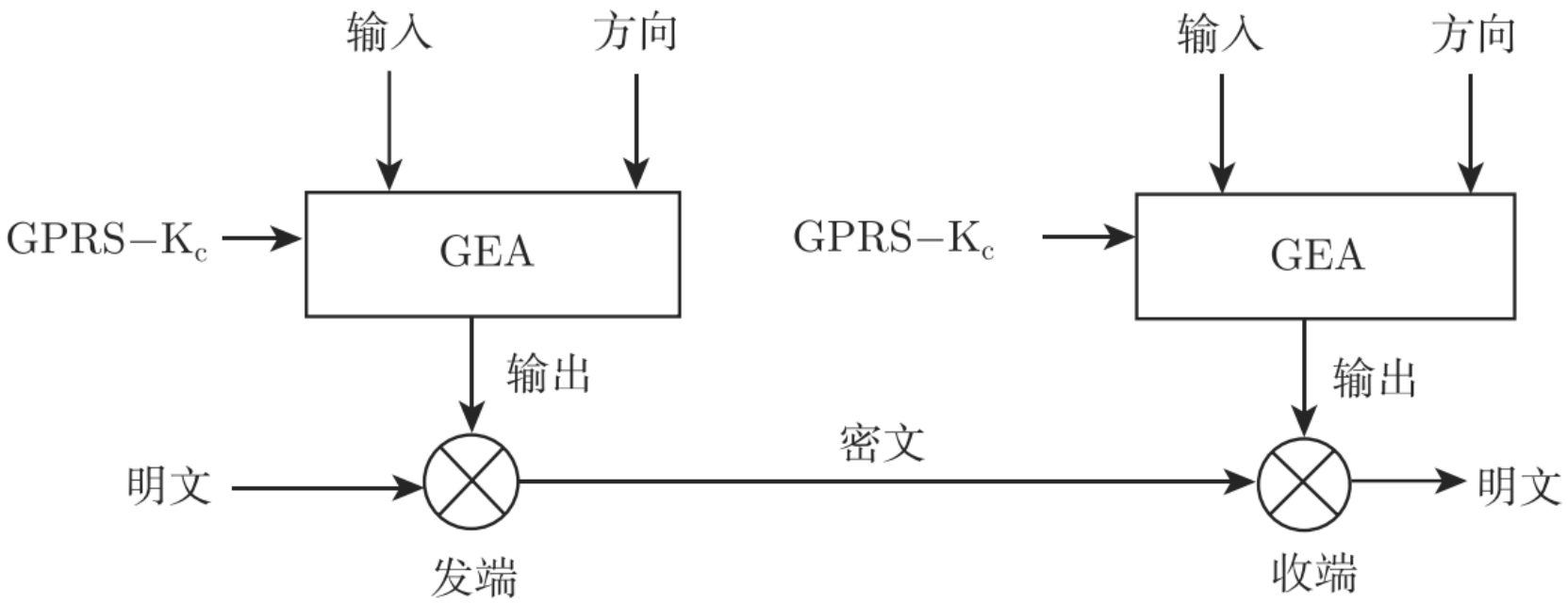


图11-23 加密和解密流程

3)身份保密

- 身份保密的目的是保护用户的隐私，使攻击者不能根据手机到基站的无线链路上的数据或从基站到SGSN的数据链路上的数据识别出用户。

- 作为用户标识的国际移动用户标识码(IMSI)应尽量少用，而以临时逻辑链路标识(TLLI)代替。TLLI与路由区域标识(RAI)一起使用，可以唯一确定用户。

- TLLI与IMSI的关系由SGSN中的数据库保存。

4) SIM卡的使用

- GPRS系统的用户终端利用SIM卡保存用户信息，包括用户的密钥K_i及国际移动用户标识IMSI。
- **SIM卡实质上是一个智能卡，卡中实现了A3、A8和GEA算法，**与**安全相关的运算都在SIM卡中进行，以防止密钥的泄露**。
- 认证中心在用户注册时，将用户的密钥K_i和IMSI分配给用户并装入到SIM卡中，并同时存入AUC的数据库中。
- K_i只在SIM卡和 AUC中使用，永远不会在网络中传输，可以有效避免密钥的泄露。

3.安全缺陷分析

1)身份认证问题

- 通过SGSN对移动用户的认证，可以保证GPRS网络资源不被非授权用户使用，保护了运营商的利益。
- 但是**认证过程是单向的**，即只是网络对移动用户认证，用户对SGSN不做认证。因而可能存在攻击者利用**假的SGSN对用户进行欺骗**，让用户以为连接到了真正的GPRS网络上，这样可能使用户的敏感信息被窃取或无法正常地访问网络资源。

2)信令及数据加密问题

- GPRS系统中的加密范围是从移动台到SGSN，不提供端到端的加密。对于需要端到端安全的应用来说，必须考虑到这个因素，不能仅依赖GPRS系统的安全性，而应该在系统设计时增加端到端的安全功能。
- GPRS的安全算法也存在问题。加密算法GEA密钥长度太短，只有64比特，无法抵抗穷举攻击。
- 在电信安全领域，开放性对于加密算法的完善来说是至关重要的。然而GPRS设计委员会却将所有安全规范保密，使别的专家无法对算法进行分析评估，以及时发现其缺陷并进行修正。

3) SIM卡问题

- GSM及GPRS系统的安全性都是基于私钥密码，用户存储在SIM卡中的私钥K_i是系统安全的根本。
- 最近，IBM的研究人员发现了SIM卡的一个漏洞，运用一种称为分割攻击的方法，可以获取SIM卡中的密钥。这种方法通过监视边信道（即加密硬件进行加密运算时，可以被监测到的与加密运算相关的信息），如电能消耗及电磁辐射，**攻击者可以在几分钟内获得SIM卡中的密钥信息**，这比攻击SIM卡中的算法或从芯片中提取密钥更简单。在此之前最有效的攻击SIM卡的方法是对卡内的算法进行密码分析，大约需要8小时。
- **从终端用户的角度来说，要防止别人获得自己的终端。**

4)其他安全问题

由于GPRS系统的骨干网是基于IP的网络，所以IP网络的所有安全问题在GPRS网络中仍然存在，包括来自内部的安全攻击和来自于GPRS网络相连的外部数据网络及其他 GPRS网络的威胁。

5)结论

- GPRS网络继承了GSM网络有效的安全特征，如采用身份认证、用户数据和信令数据的加密以及利用硬件存储用户的密钥等。同时GPRS网络在安全方面比GSM网络有所提高，表现在其用户数据和信令数据的加密范围比GSM网络大，降低了明文传输的范围。

- 但是GPRS网络毕竟是在GSM网络基础上通过增加特定的网络设备构建起来的，所以必然存在GSM网络在安全方面的一些缺陷，如认证是单向的，加密密钥太短。所以**在利用GPRS进行安全通信时，不能只依靠GPRS系统本身的安全机制，还应在应用层上加强安全保护**。

- 在未来移动通信系统的研究和设计中，应该继承GSM、GPRS网络中有效的安全特征，并克服和改进其不足。

11.2.3 第三代移动通信系统(3G)的安全

- 3G系统的安全体系主要有两个系列：**3GPP(WCDMA) 和 3GPP2(cdma2000)**。
- 本节基于3GPP体制探讨3G的安全体制，重点分析3G认证与密钥分配协议和加密与完整性保护。
- 3GPP2的认证协议也采用了“请求—响应”的形式，整个认证方式与3GPP类似，但其认证是以基站为核心的，只有其增强认证和加密模式才可提供用户和网络的相互认证。

1. 3GPP安全体制的总体结构

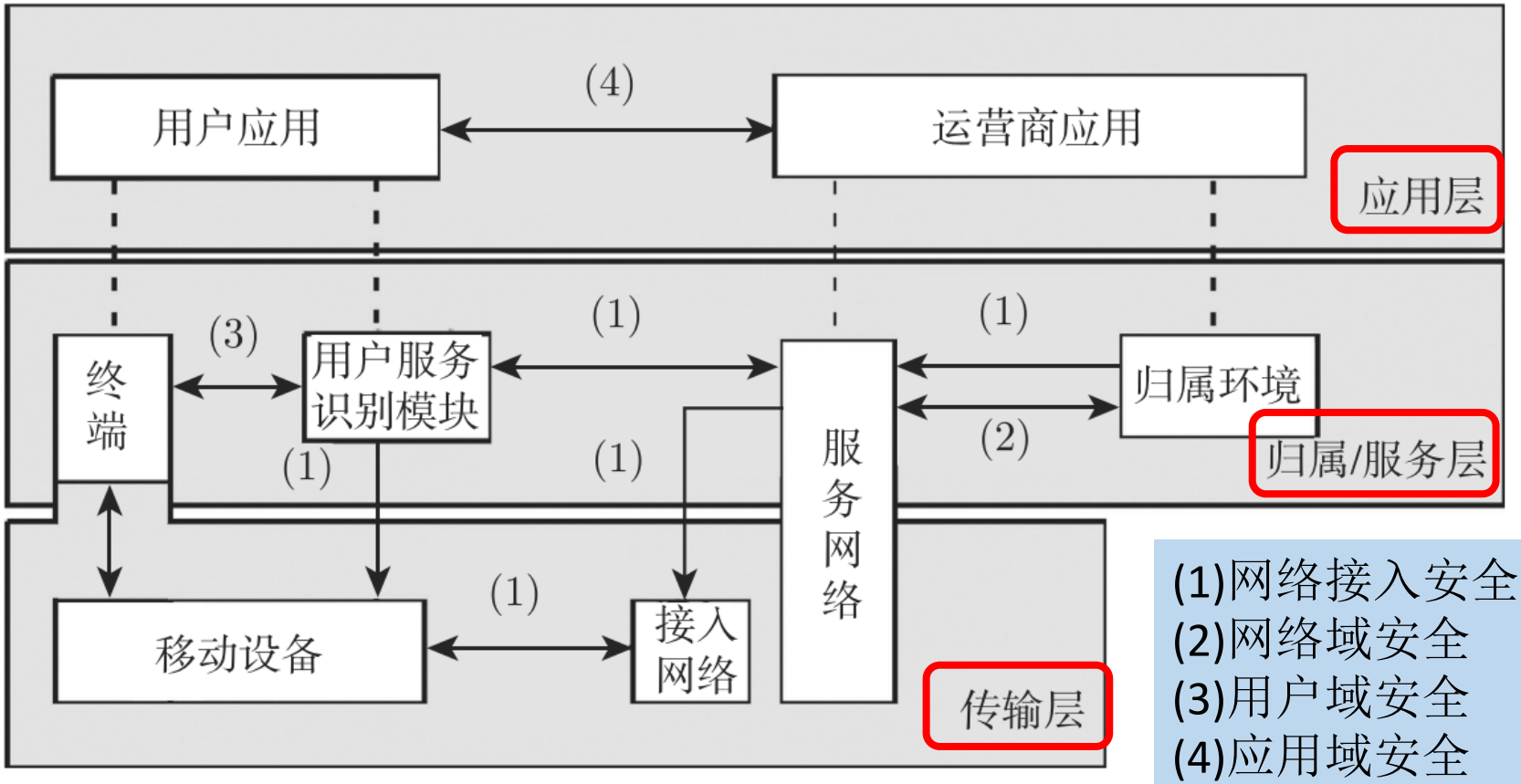
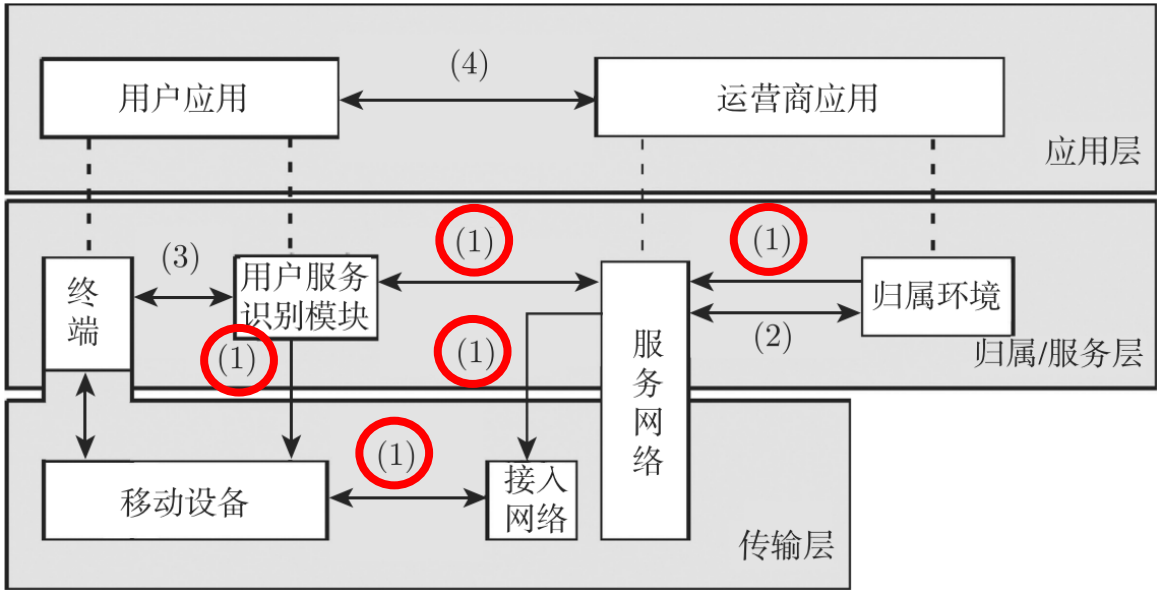


图11-24 3GPP安全体制总体结构

(1)网络接入安全
(2)网络域安全
(3)用户域安全
(4)应用域安全
(5)安全特性的可视性及可配置能力

网络接入安全



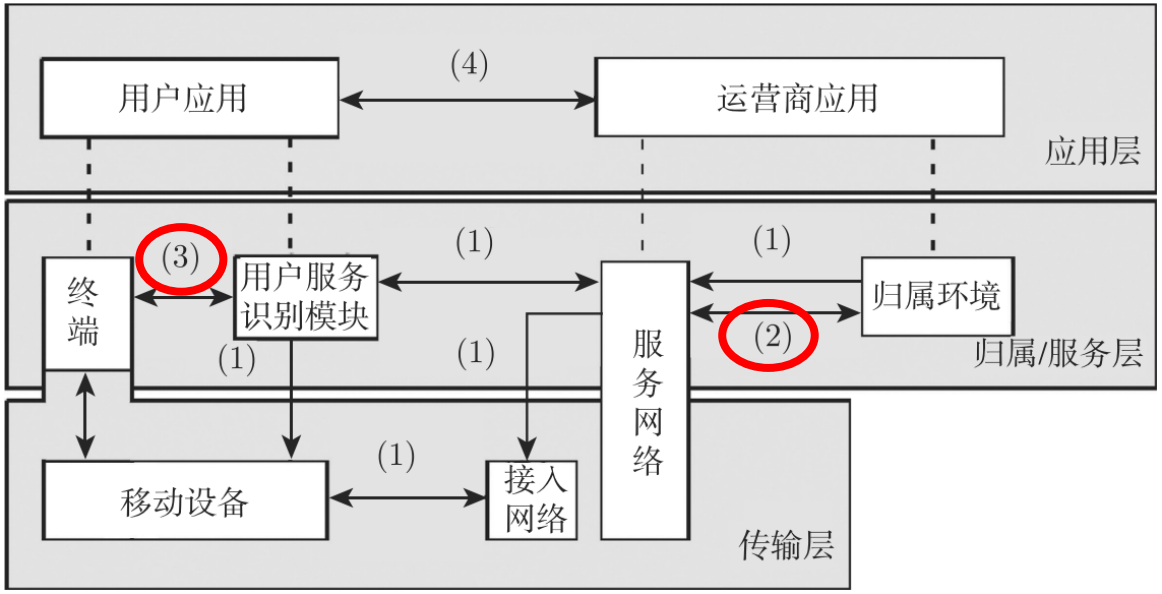
(1)网络接入安全

提供安全接入3G服务网的机制并抵御对无线链路的攻击。

空中接口的安全性最为重要，因为无线链路最易遭受各种攻击。

- 这一部分的功能包括：用户身份保密、认证和密钥分配、数据加密和完整性等。
- 其中，认证和密钥分配是基于USIM和HE/AuC共享秘密信息K的相互认证。认证过程中也融合了加密、完整性保护等措施。

网络域安全和用户域安全



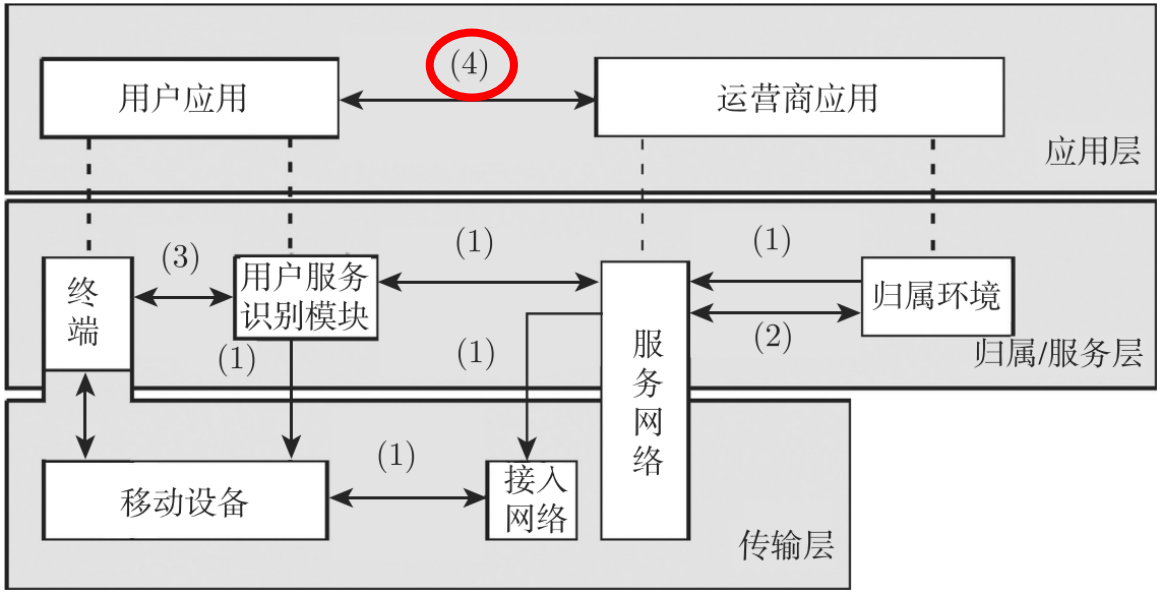
(2) 网络域安全

- 保证网内信令的安全传送并抵御对有线网络（核心网部分）的攻击。

(3) 用户域安全

- 主要保证对移动台的安全接入。包括用户与智能卡间的认证，智能卡与终端间的认证及其链路的保护。

应用域安全



(4) **应用域安全**

- 使用户域与服务提供商的应用程序间能够安全地交换信息。

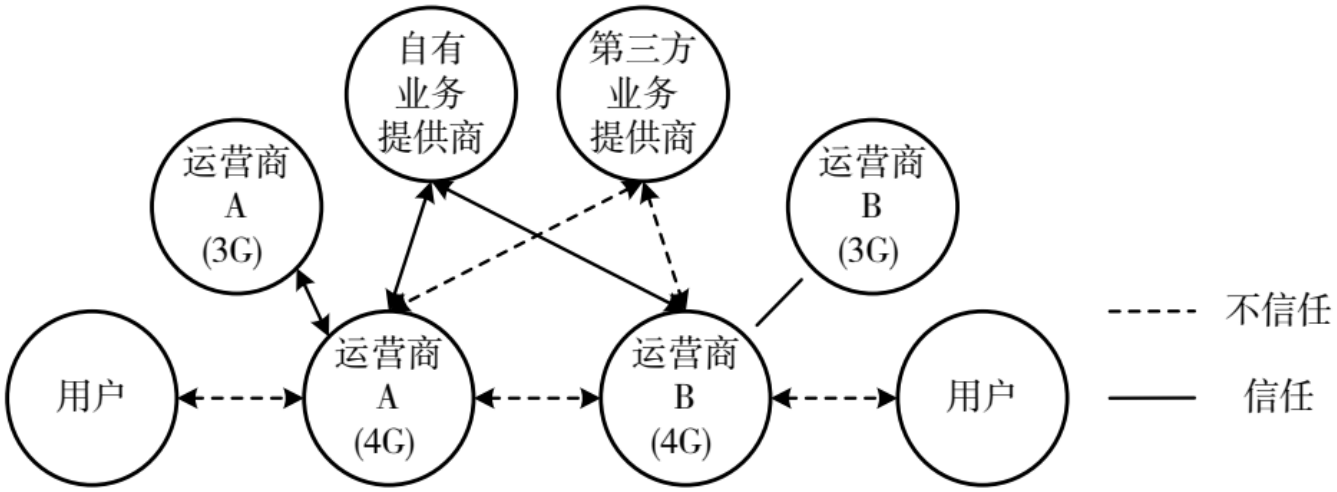
(5) **安全特性的可视性及可配置能力**

- 主要指用户能获知安全特性是否在使用以及服务提供商提供的服务是否需要以安全服务为基础。

11.3 第四代移动通信系统(4G)的安全（补充）

- 4G 无线技术集合称为长期演进计划（Long Term Evolution，LTE）
- 基于正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）和多输入多输出（Multiple Input Multiple Output，MIMO）两大关键技术，将数据下行速率从2 Mb/s 提高到100 Mb/s，将上行速率提高到 50 Mb/s，终端的移动速率从步行速率提高到车辆形式速率，并提供完备的服务质量（Quality of Service，QoS）机制。
- 因此，4G 网络从真正意义上提供了移动宽带互联网服务。

4G 的信任模型



- 4G 系统的信任模型考虑了 3G 时代出现的安全问题，同时考虑了运营商之间的互信问题，做了以下几个设计假定：

① 运营商之间可以出现假冒问题，可利用较低代价模式运营商，需要有互信机制；

② 需要考虑与 3G 系统的前向兼容性，实际上取缔了 2G的 SIM 卡，只能够使用 3G、4G 的 USIM 卡才能够接入系统。

4G的安全架构

- 到了LTE时代，3GPP国际标准化组织为4G网络打造了比3G网络更可靠、鲁棒性更高的安全机制。
- 3GPP在安全总体架构中在安全性上强化了归属域概念，如图所示。图中定义了4G安全特征组，每个特完成特定的安全目标。

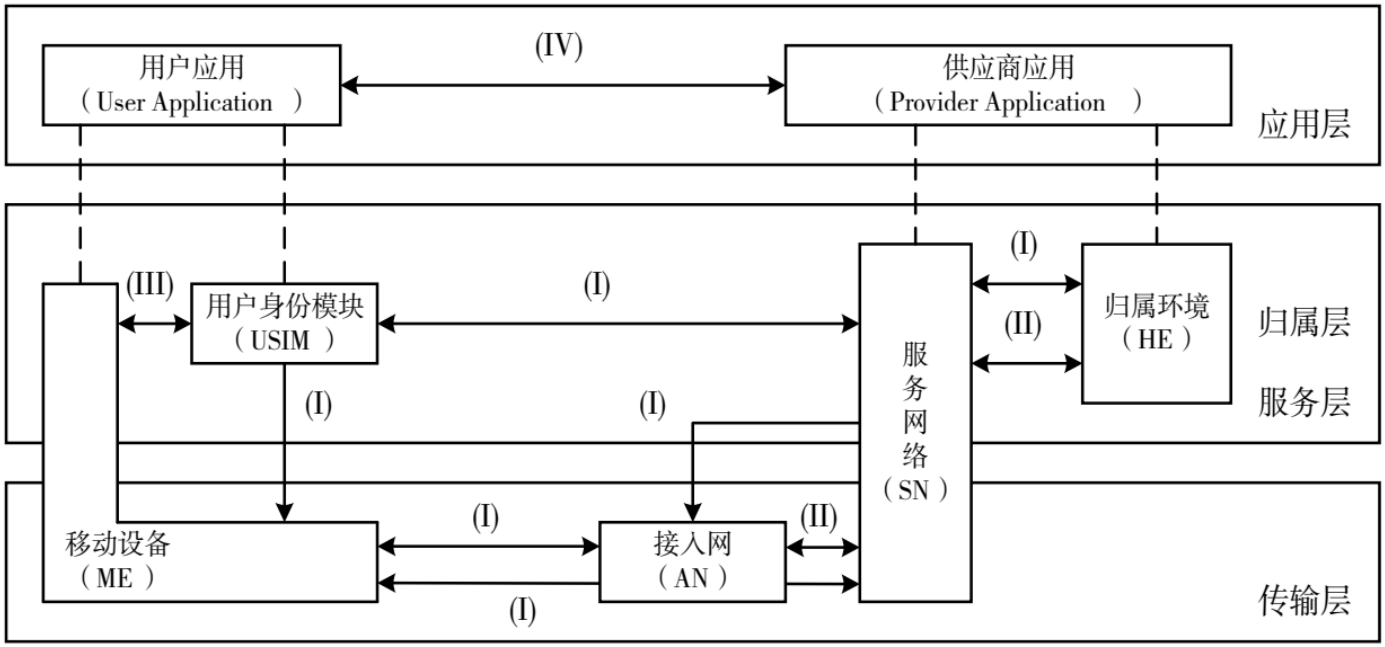
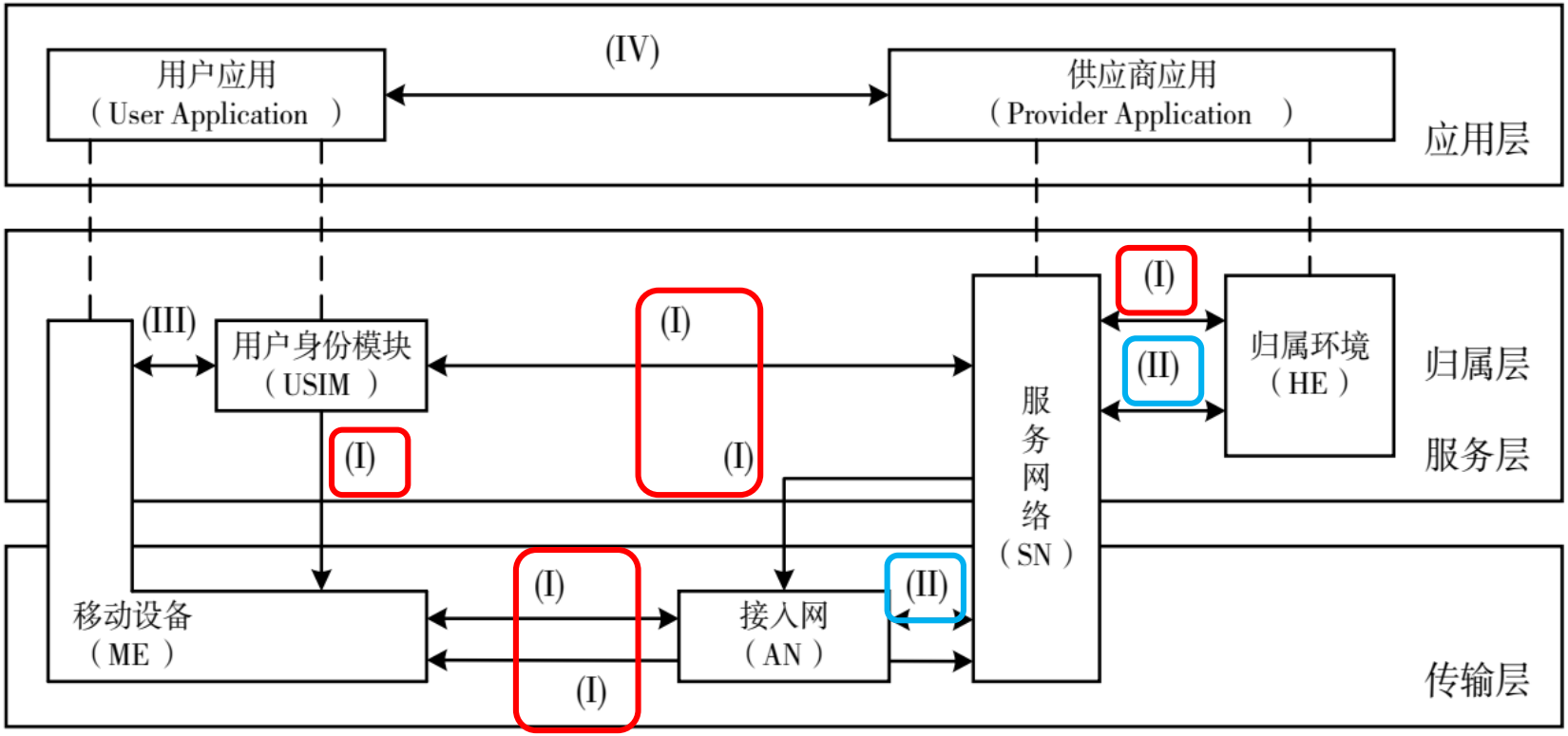


图8 4G系统安全总体架构

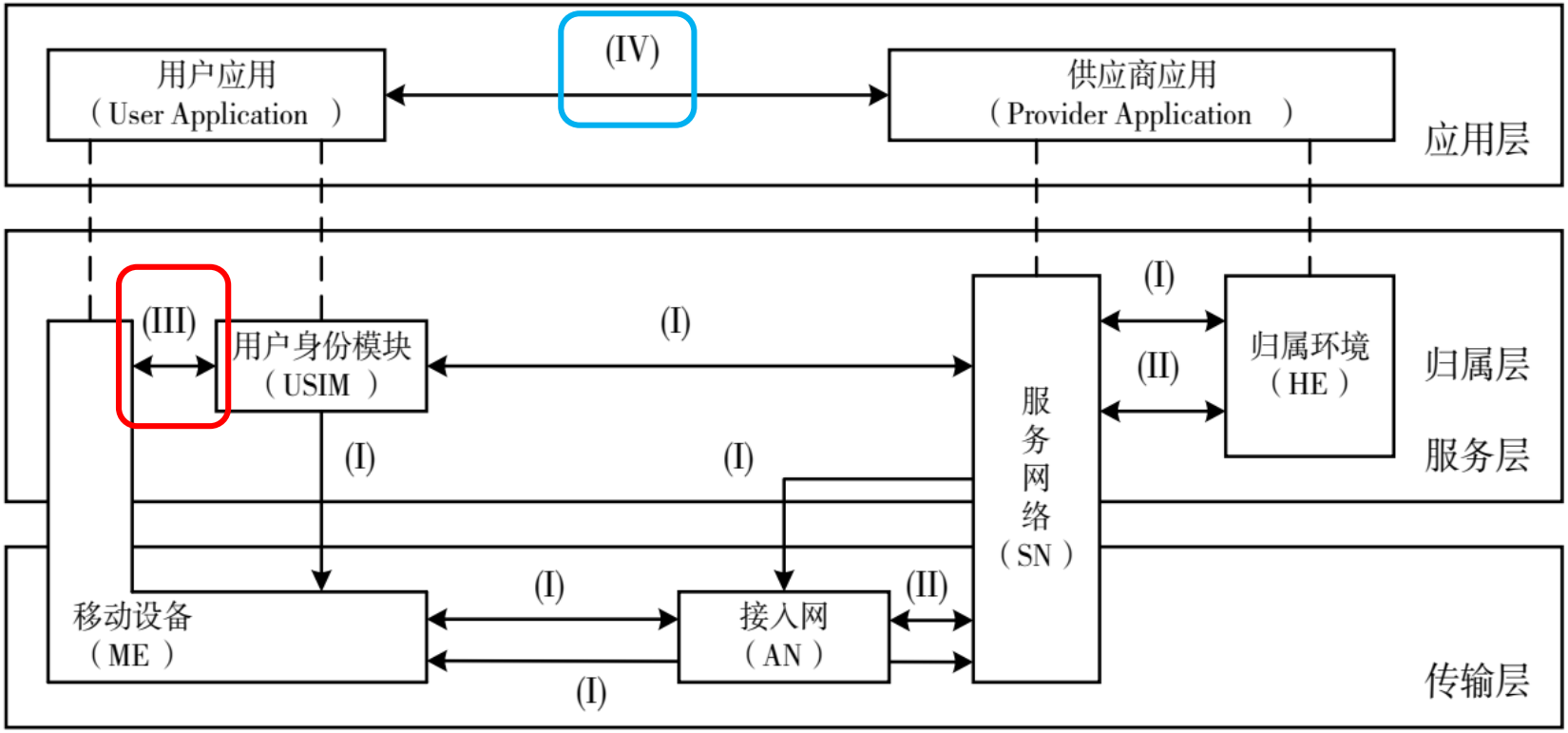


（1）安全特征组（I）：

- 网络接入安全。提供给用户到 4G 业务的安全接入安全特征组，用于实现用户的双向身份认证和安全接入。

（2）安全特征组（II）：

- 网络域安全。提供域内节点能够安全交互信令消息的安全特征组，用于实现接入网、拜访域和归属域之间的安全交互。



（3）**安全特征组（III）**：用户域安全。提供安全接入移动终端的安全特征组，用于实现用户终端对 USIM 卡的识别和安全交互。

（4）**安全特征组（IV）：应用域安全**。提供用户和应用供应商域内的应用能够安全地交互消息的安全特征组，用于实现 4G 分组业务的安全交互。

（5）安全特征组（V）：可视可配置安全。提供用户能够感知他自己的一个安全特征是否在使用中，业务的使用和提供是否依赖安全特征。

4G 安全架构与 3G 安全架构的不同之处

4G 安全架构与 3G 安全架构的不同之处：

- ✓一是加强了网络接入安全，通过强制要求双向认证彻底杜绝伪基站；
- ✓二是加强了网络域安全，通过取消电路域彻底杜绝了运营商假冒的问题。

4G安全机制

- （1）身份认证。只允许 USIM 卡接入，使用2G SIM 卡无法接入 4G 系统，彻底杜绝了伪基站。
- （2）用户隐私保护。沿用 2G、3G 的机制，用临时可变的 TMSI/GUTI 替代永久不变的 IMSI，以便减少 IMSI 在空口暴露的频次。
- （3）空口业务防护。仍然只提供了可选的机密性保护，没有提供正式的完整性保护。加密算法用 AES 取代了 KASUMI，新引入了中国的 ZUC 算法，共支持 AES、SNOW 3G、ZUC 这 3 种算法。
- （4）网络域安全。由于取缔了电路域，因此不再有电路域情况下七号信令假冒问题，从而实现了运营商之间的互信及安全交互，杜绝了假冒运营商的问题。

4G的优缺点

- 4G由于不再前向兼容 2G 系统，因此彻底堵上了伪基站的漏洞，同时因为取缔了电路域，实现了运营商之间的安全交互问题。
- 但是，仍然存在缺点：

① 由于 EPS AKA 的认证协议存在设计漏洞，拜访域 MME 作为认证结果的判决实体，存在拜访域欺骗归属域的风险，因此拜访域运营商仍然能够出于计费、监控等目的对归属域运营商进行欺骗。

② 空口业务防护仍然只提供可选的机密性保护，业务数据仍然容易被篡改。虽然TMSI/GUTI 能够减少 IMSI 在空口暴露的频次，但仍然会延续 2G、3G 空口明文暴露 IMSI 的问题。

11.4 第五代移动通信系统(5G)的安全（补充）

- 4G 网络只考虑了移动互联网一种应用场景，5G 将来不仅用于人与人之间的通信，还会用于人与物以及物与物之间的通信。
- 面向增强移动宽带（Enhanced Mobile Broadband，**eMBB**）、低功耗大连接（Massive Machine Type Communication，**mMTC**）和高可靠低时延（Ultra-reliable and Low Latency Communications，**uRLLC**）3 大应用场景，已经成为 5G 移动通信系统架构设计的核心需求。

5G概述

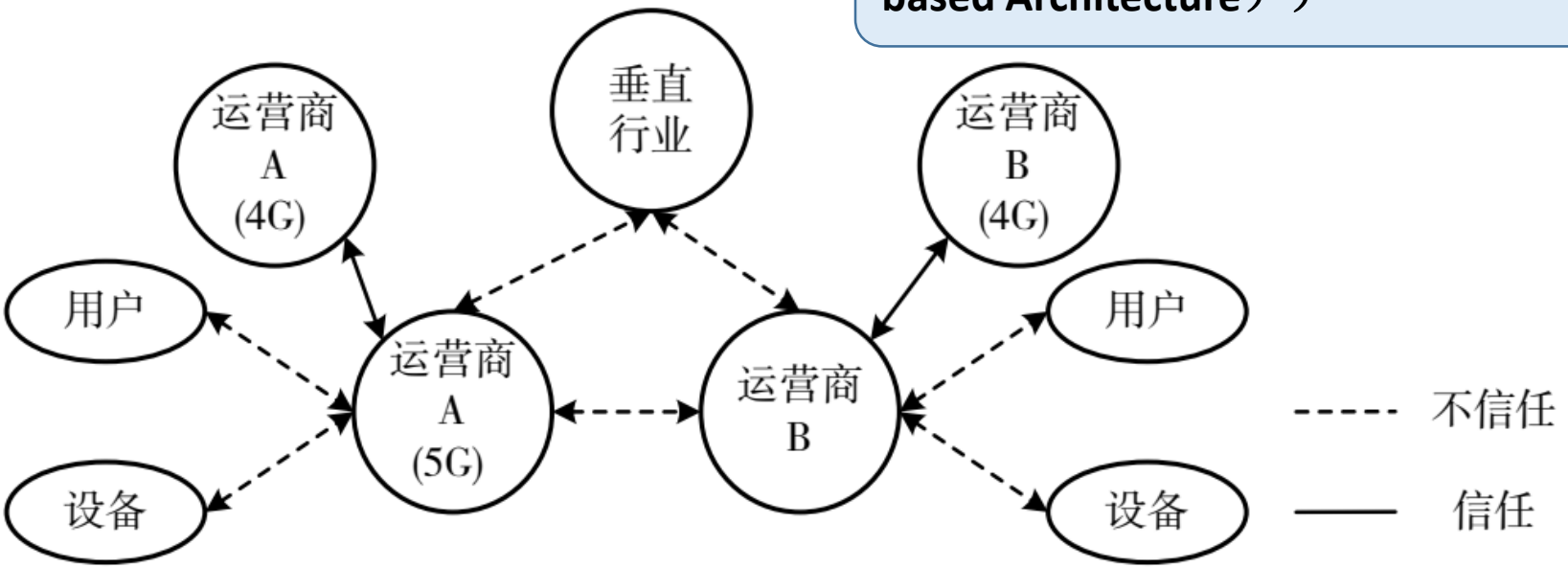
- eMBB 聚焦对带宽有极高需求的业务，网络峰值速率和用户体验速率较 4G 增长 10 倍以上，如高清视频、虚拟现实（Virtual Reality，VR）和增强现实（Advanced Reality，AR）等，满足了人们对数字化生活的需求。

- uRLLC 聚焦对时延极其敏感的业务，端到端时延从 10 ms 降到了 1 ms，如自动驾驶 / 辅助驾驶、远程控制等，满足了人们对数字化工业的需求。

5G信任模型

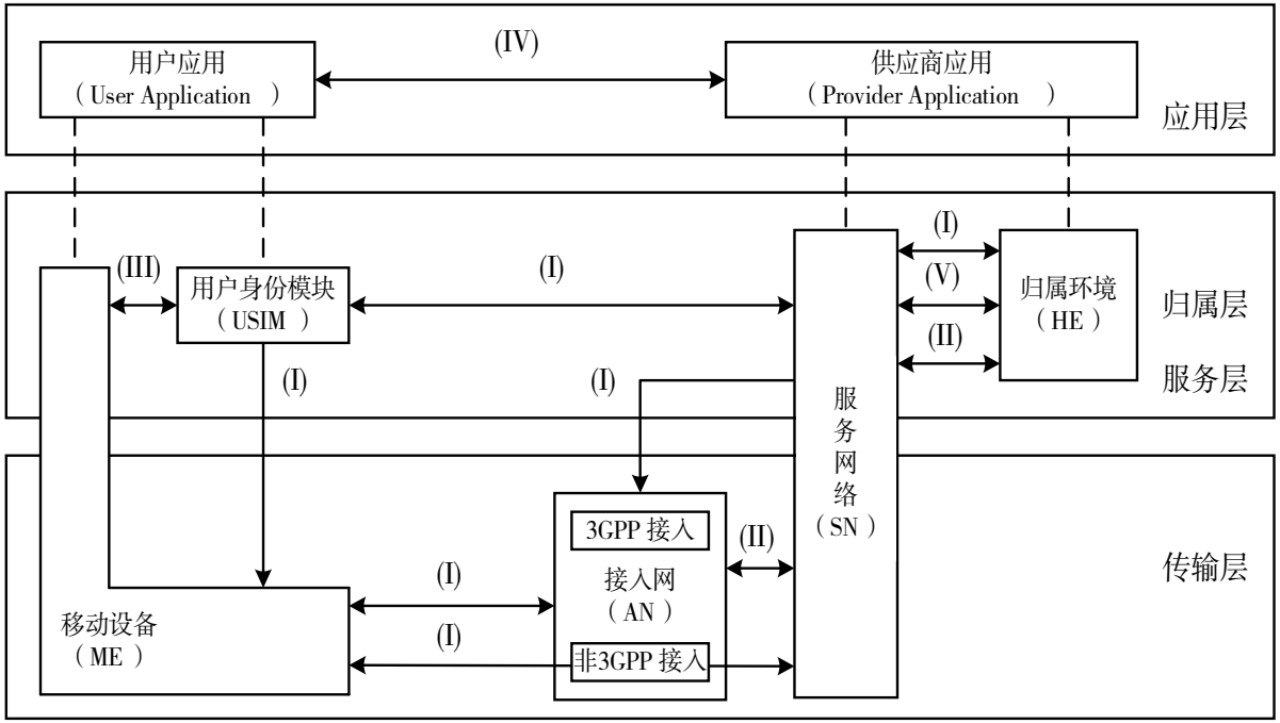
- 为了应对差异化应用需求，5G网络不仅是全IP的，还是开放的和服务化的。因此，对网络内外部安全机制的考虑更加充分，信任模型如图所示。

SBA 架构（服务化架构（SBA：Service-based Architecture））



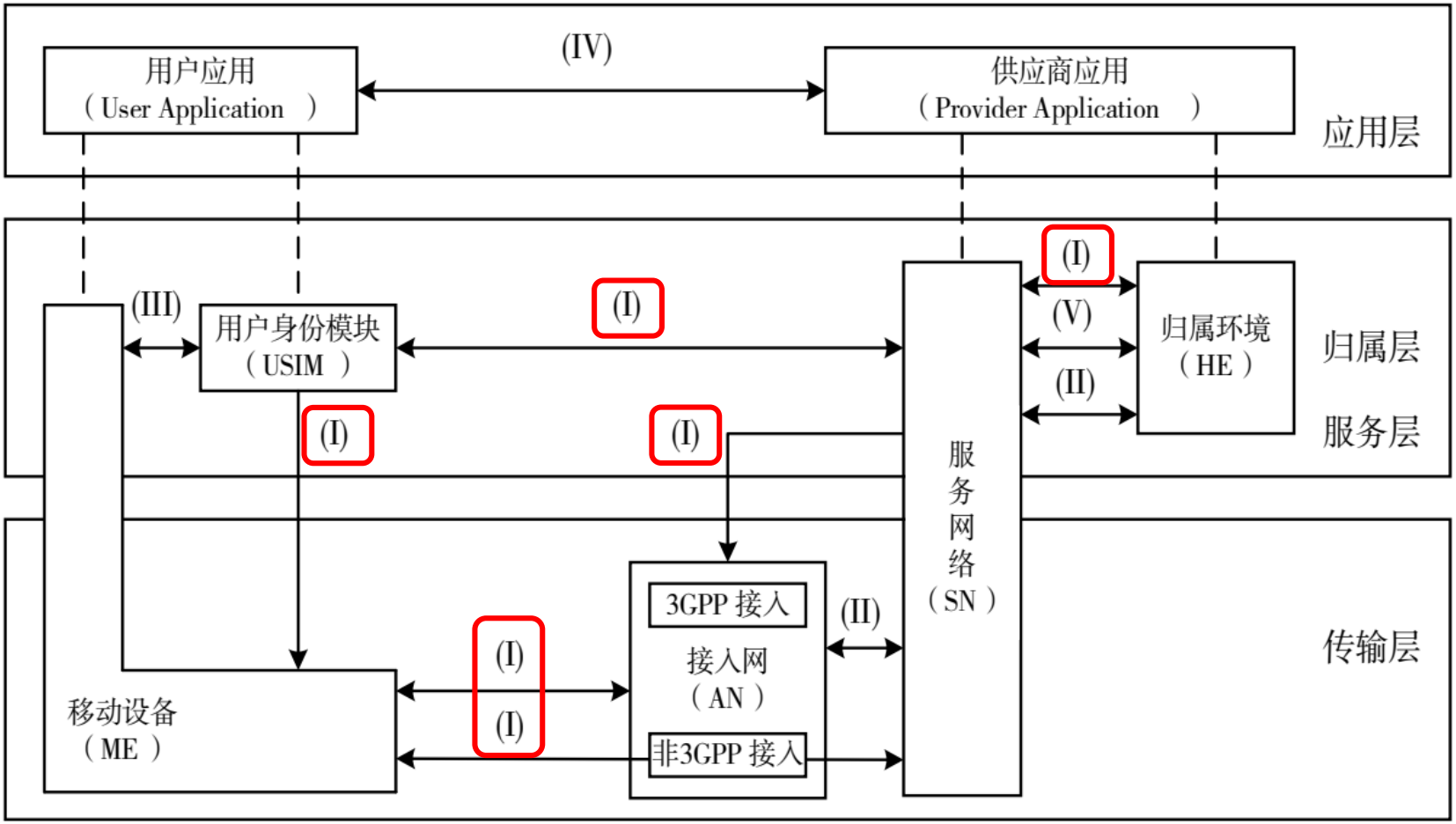
5G 系统信任模型

5G安全架构

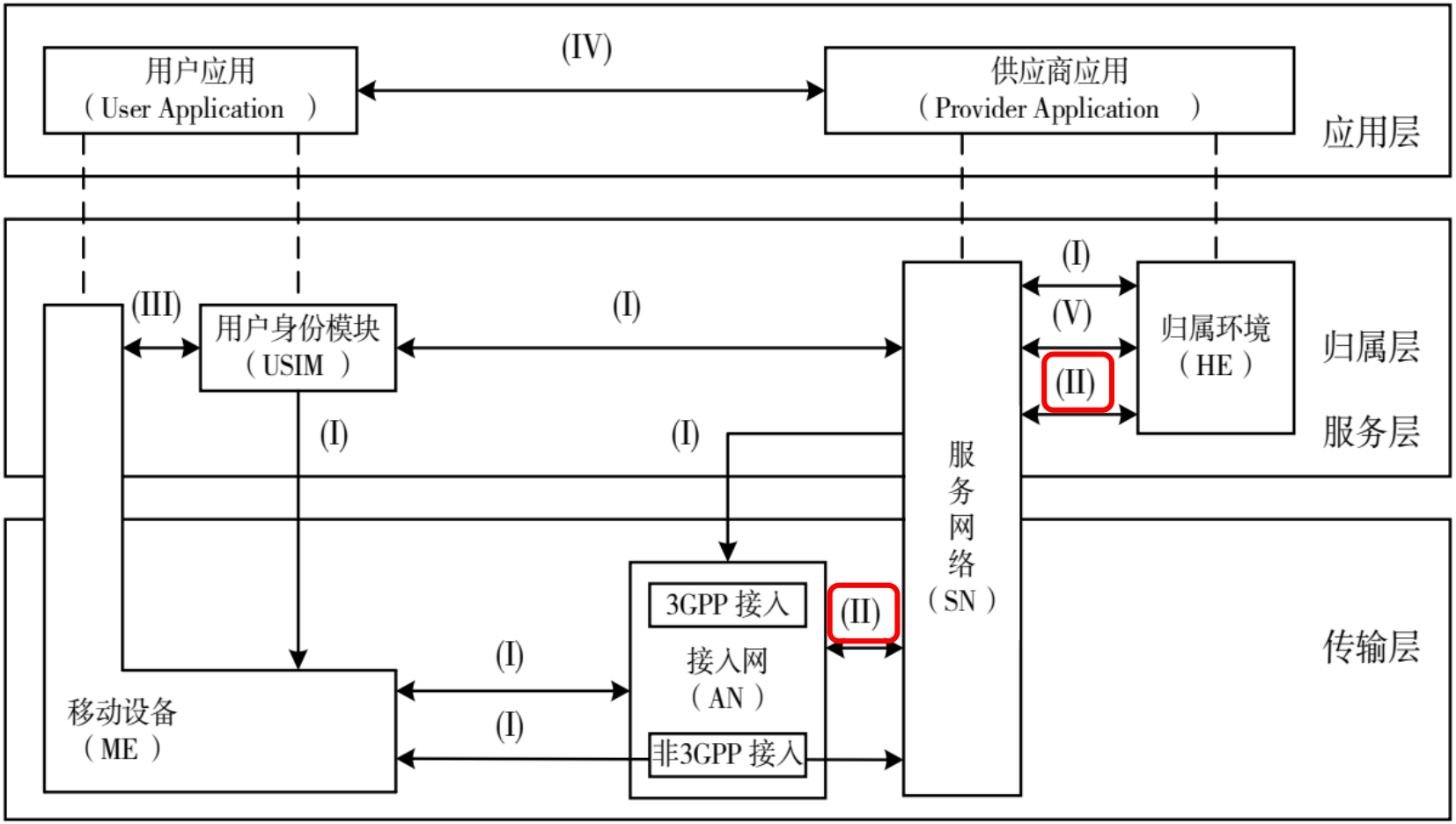


5G 系统安全总体架构

- 从 5G 信任模型可以看出，5G 系统引入了新的利益相关方——垂直行业，因此 3GPP 在安全总体架构（参见 TS 33.501）中引入了非 3GPP 接入方式和 SBA 域的安全特征组，如图所示。

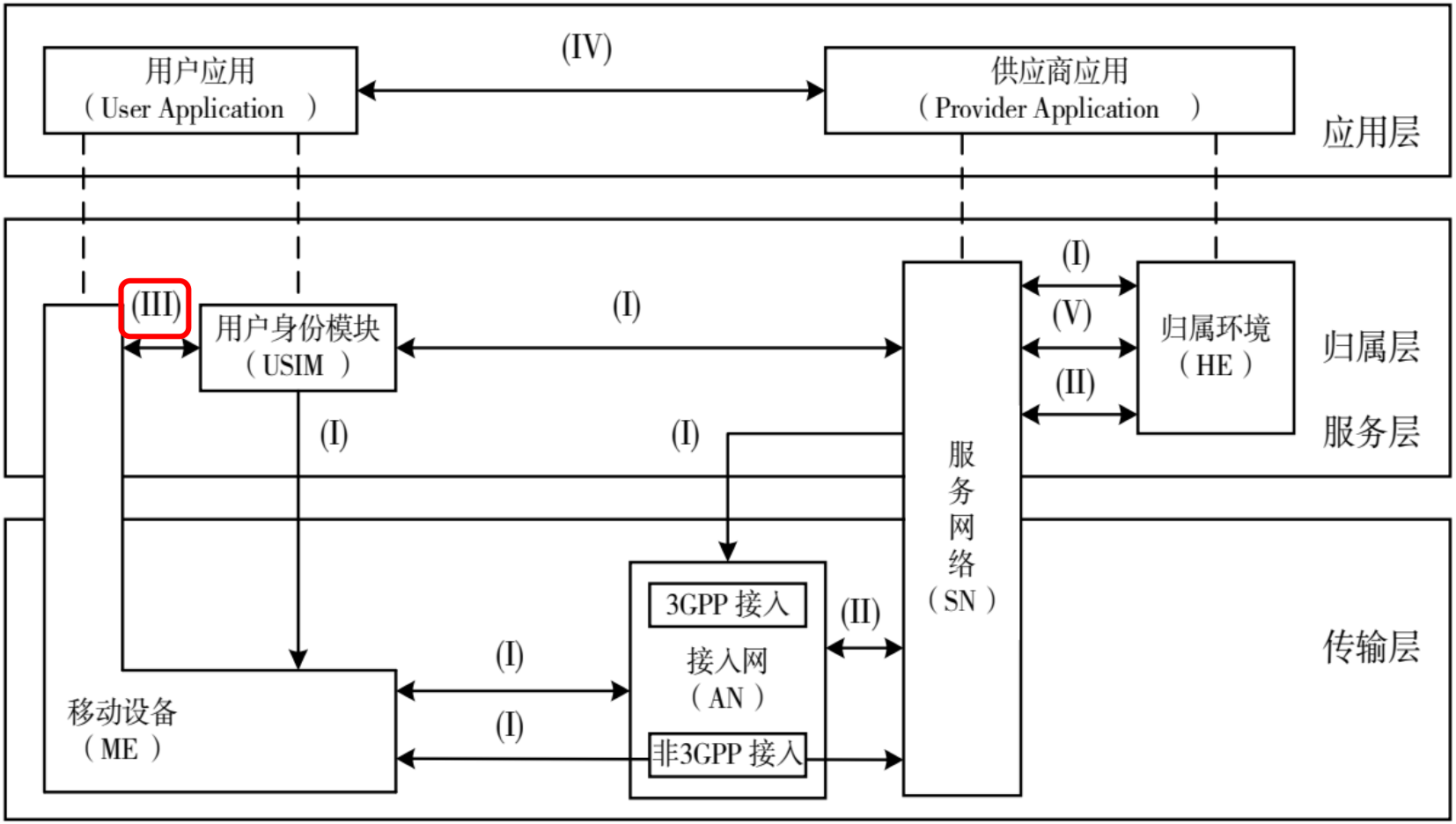


（1）网络接入域安全（I）：
提供给用户到 4G业务的安全接入安全特征组，用于实现 3GPP 接入场景和非 3GPP 接入场景用户的双向身份认证以及安全接入。

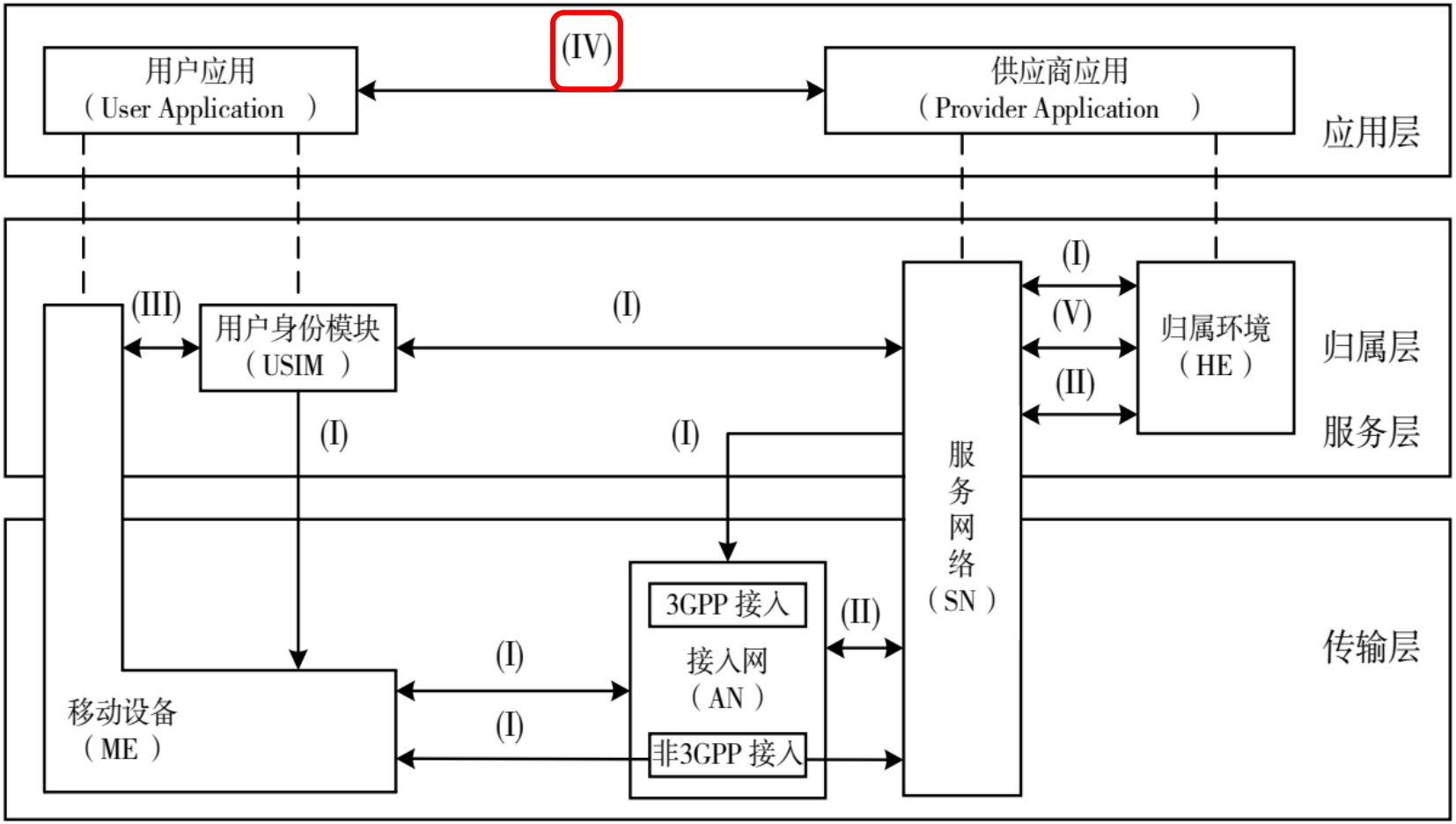


（2）网络域安全（II）：

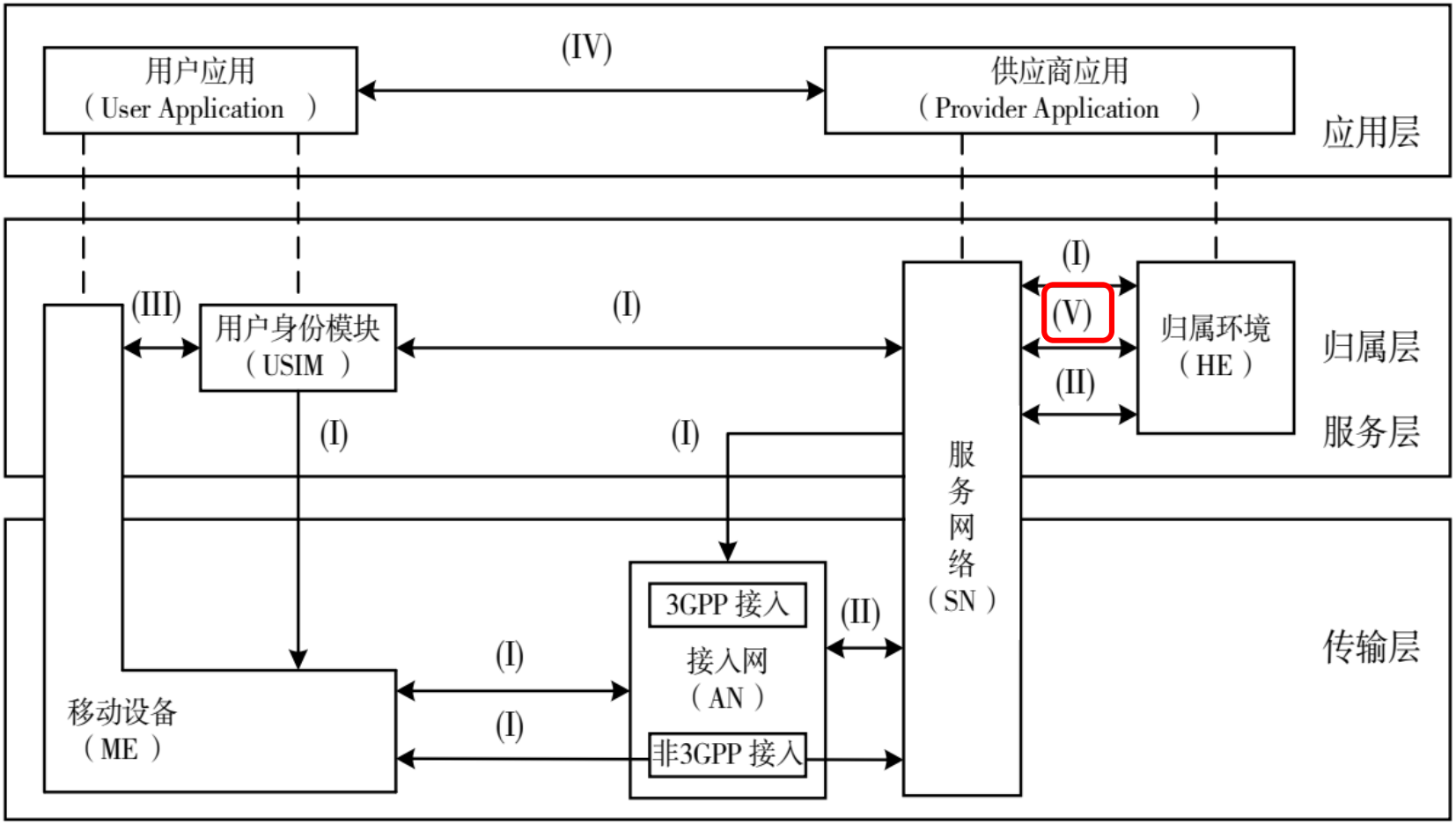
提供域内节点能够安全交互信令消息和用户面数据的安全特征组，用于实现接入网、拜访域和归属域之间的安全交互。



（3）用户域安全（III）：
提供安全接入移动终端的安全特征组，用于实现用户终端对 USIM 卡的识别和安全交互。



（4）应用流程域安全（IV）：
提供用户和应用供应商域内的应用能够安全地交互消息的安全特征组，用于实现 5G 分组业务的安全交互。



（5）基于SBA域 的 安 全（V）：

提 供 使 得SBA 架构的网络功能能够在服务网络内以及与其他网络进行安全通信的安全特征组。用于实现对包括网络功能注册、发现和授权安全方面以及对基于服务的接口的保护。

5G 安全架构与 4G 安全架构的不同之处

- 一是加强了网络接入安全，增加了非 3GPP 接入，同时增强了AKA协议，堵上了拜访域欺骗归属域的漏洞；
- 二是面向垂直行业需求，新增了二次认证，在满足垂直行业差异化需求的同时增强了安全性；
- 三是新增了SBA域的安全，考虑了服务化网元的安全交互；
- 四是应用域安全，新增了空口可选的完整性保护手段。

5G安全机制

- （1）**身份认证**。AKA 协议加强了归属域控制，堵上了拜访域欺骗归属域的漏洞；新引入了非3GPP 接入和二次认证，满足了垂直行业需要。
- （2）**用户隐私保护**。新引入非对称密码，通过用户隐藏标识符（Subscription Concealed Identifier，SUCI）对 SUPI/IMSI 进行加密，堵上了2G、3G、4G 在空口明文暴露 IMSI 的漏洞。
- （3）**空口业务防护**。新增加了可选的完整性保护。
- （4）**网络域安全**。新增 SBA 域安全的概念，同时为跨网信令防护新增了安全边界协议代理（Security Edge Protection Proxy，SEPP）网元。
- 目前**业界公认5G是安全性最强的一代**，面向普通公众应用已经非常完备。

5G 面向垂直行业应用的安全不足

(1) 接入认证

- 3GPP 原生安全的接入认证的 Milenage 算法框架推荐使用国际标准算法 AES，存在后门风险。关键行业需要使用国产或专用的认证算法进行安全增强。

(2) 隐私保护

- 3GPP 原生安全的隐私保护的 SUCI 只解决了空口的隐私保护，合法监听 LI 接口让拜访域 AMF 网元仍然能够获得 SUPI/IMSI，因此攻击者仍然可利用技术途径从核心网拜访域对 IMSI 进行捕获，进而对特定用户进行持续性跟踪和定位。关键行业需要解决针对核心网拜访域的隐私保护问题，实现关键用户的防追踪、防定位。

5G 面向垂直行业应用的安全不足

(3) 签约信息

- 运营商提供的专网未能实现用户签约信息包括IMSI、根密钥 Ki 等信息的专网专用，存在从管理上泄露用户身份隐私信息的风险。关键行业需要解决用户签约信息的自主管理问题。

(4) 业务防护

- 3GPP 原生安全的业务安全防护仅对无线空口传输提供可选的机密性保护、可选的完整性保护，存在业务数据在承载网上被窃取和篡改的风险。关键行业需要提供端到端的业务数据全程加密防护的安全增强能力。

5G安全展望

① 未来5G安全在标准制定过程中需要更加全面，充分考虑垂直行业的安全需求，让 3GPP 自带的原生安全能够更近一步。

② 未来5G安全需要更加开放，在向外提供能力的同时能够接纳外部第三方，便于嵌入第三方的安全增强能力，以便在更加多样化的应用场景、多种接入方式、差异化的网络服务方式以及新型网络架构的基础上提供全方位的安全保障。

- 最终实现构建更加**安全可信的5G内生安全网络**的目标。

6G 安全技术发展探讨

- 历代移动通信系统都是在上一代的基础上持续演进，6G 可以推测应该也会在 5G 的基础上不断发展。
- 相比较 5G 以 3 大场景为代表的业务，6G 会支持和创造更多的应用场景与业务需求，进一步提升网络性能，并由地面覆盖网络发展为空天地立体覆盖网络，促进人类真正迈入数字信息化时代。
- 设想与 5G 的区别，6G 时代海量业务处理，对 6G 安全提出了更高的要求，**安全架构需要具备融合性、内生性和自适应性的特点**。

6G的安全需求

(1) 面向接入认证高效性需求

- 相对于 5G 的海量物联连接，在 6G 时代将会更加突出，超海量的物联设备具有长周期、短数据的业务特征，传统“先做认证、后建连接”在这种业务模型下效率就会下降，迫切需要更加高效的接入认证体制。

(2) 面向业务加密高效性需求

- 5G 频段最高到毫米波频段，而在 6G 时代将可能上太赫兹。同时，天空地一体化组网将可能造成6G 的基站规模远大于 5G 基站规模，将会给传统的密钥派生机制带来极大挑战，迫切需要更加高效的业务加密体制。

(3) 面向行业应用开放性需求

- 移动通信系统作为当前和未来各垂直行业构建虚拟专网所依赖的首选公共基础设施，基于通用安全架构满足垂直行业差异化安全需求将会越来越困难，因此迫切需要更加开放的安全架构，用于嵌入不同垂直行业具有差异化的安全需求。

谢谢！