南京郵電大學
Nanjing University of Posts and Telecommunications

无线城域网WiMAX-加密

汇报人：宁帅宇
汇报日期：4.29

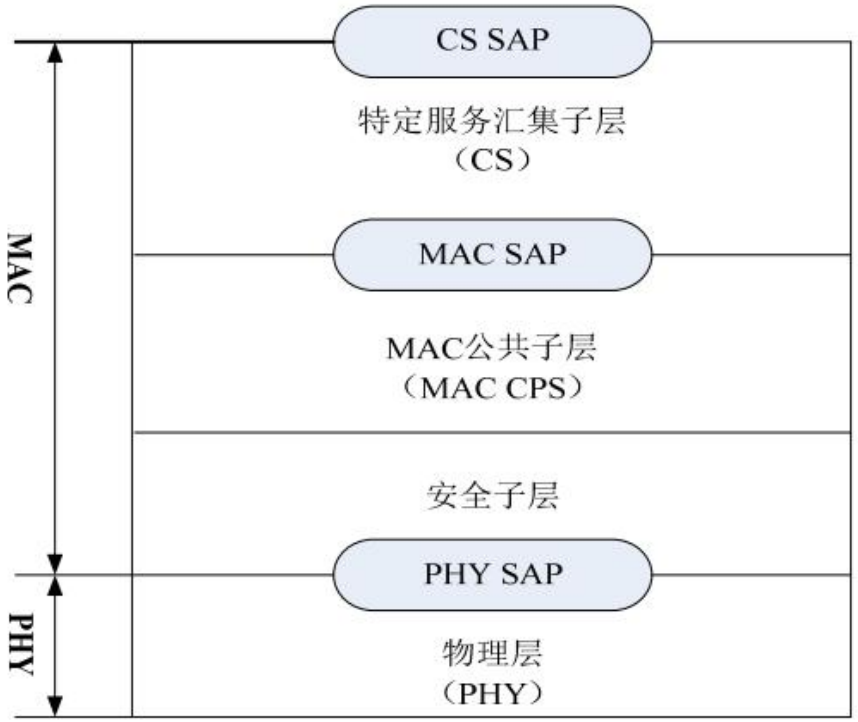
1.引言

WiMAX 是 IEEE 802.16 标准在市场推广方面采用的名称，同时因为它也是一项基于 IEEE 802.16 系列标准的宽带无线接入城域网(Broadband Wireless Access Metropolitan Area Network，BWAMAN)技术，所以亦常被称为 IEEE 无线城域网WMAN（Wireless Metropolitan Area Network）。IEEE 802.16 工作组是 802.16 宽带无线接入空中接口标准的制定者，主要针对 WMAN 的物理层和媒体访问控制（Medium Access Control，MAC）层制定规范和标准。如今WiMAX 已经成为一个能够适应市场需求提供增强的用户移动性的多功能技术。

WiMAX 安全有两个目标，一个是在整个无线网络中提供隐私，另一个是提供对网络的访问控制。隐私是通过加密用户站和基站之间的连接来实现的。基站通过对整个网络的服务流实施加密来防止未经授权的访问。因此对WiMAX 安全来说，加密是其中十分重要的一个环节。

2.安全子层

IEEE 802.16 标准中规定的协议框架如下图所示。该协议框架只定义了物理层（PHY）和媒质接入控制层（MAC）两个层面的技术。



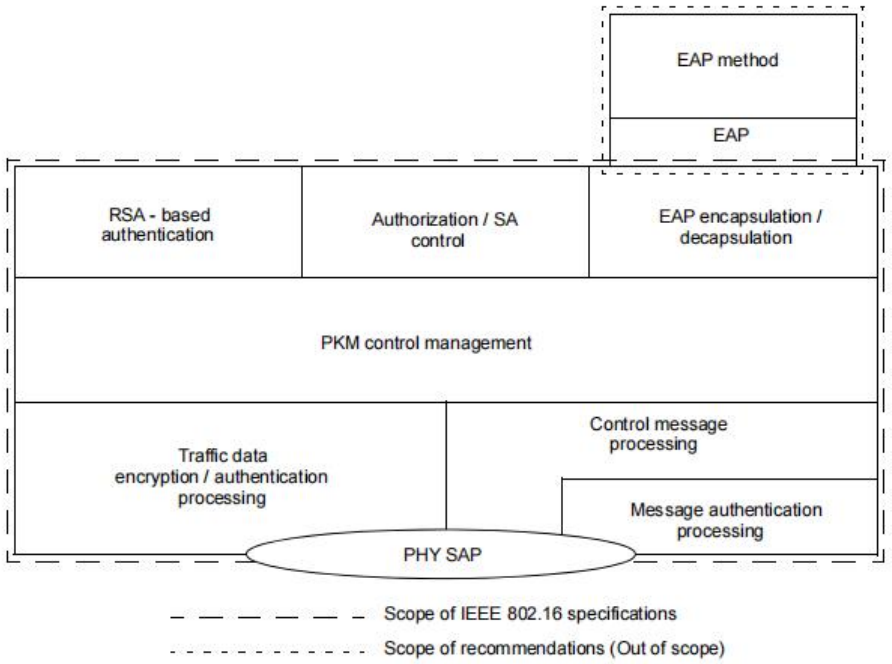
MAC 层包括三个子层：

特定服务汇聚子层、MAC 公共子层、安全子层。

安全子层是 IEEE 802.16 标准为了突出安全的重要性，专门在 MAC 层中增加的一层。安全子层为用户提供隐私、认证或保密性，确保宽带无线网络中的数据传输安全。它通过对在SS（ Subscriber Station，即用户站）和BS（Base Station，即基站，是无线网络中的核心组件）之间连接上传输的MAC PDU（协议数据单元）应用加密转换来实现这一目标。

2.安全子层

IEEE 802.16-2017 标准中规定的安全子层中的协议栈如下图所示。



PKM Control Management：PKM控制管理，此堆栈控制所有安全组件。各种密钥在此堆栈中派生和生成。

Traffic Data Encryption/Authentication Processing：流量数据加密/认证处理，此堆栈负责对流量数据进行加密或解密，并执行流量数据的认证功能。

Control Message Processing：控制消息处理，此堆栈处理与PKM相关的各种MAC消息。

Message Authentication Processing：消息认证处理，此堆栈执行消息认证功能。可以支持HMAC、CMAC或多个短HMAC。

RSA-based Authentication：基于RSA的认证，当选择基于RSA的授权作为SS和BS之间的授权策略时，此堆栈使用SS的X.509数字证书和BS的X.509数字证书执行基于RSA的认证功能。

EAP Encapsulation/Decapsulation：EAP封装/解封装，当选择基于EAP的授权或经过认证的基于EAP的授权作为SS和BS之间的授权策略时，此堆栈提供与EAP层的接口。

Authorization/SA Control：授权/SA控制，此堆栈控制授权状态机和流量加密密钥状态机。

2.安全子层

安全子层主要由用于保护固定宽带接入网络中数据包的封装协议和密钥管理协议 PKM 两部分组成：

密钥管理协议 PKM：提供 BS 与 SS/MS 密钥的协商与分发、同步及业务接入的授权等功能。PKM 协议利用一系列的规则来负责 SS/MS 的认证和授权的，从而方便 WiMAX 安全密钥的分配。

用于保护固定宽带接入网络中数据包的封装协议：负责加密数据包，包括加密与认证算法以及该认证算法的应用规则。即采用数据封装协议对在固定宽带无线接入网上传输的分组数据进行加密。该协议定义了一组支持的加密套件，即数据加密和认证算法的配对，以及将这些算法应用于MAC PDU有效负载的规则。

3.加密密钥分类

在802.16标准中，安全子层使用了多种加密密钥。下表中展示了802.16中定义的重要加密密钥的类别、符号和长度。

流量加密密钥（TEK） 是一种数据加密密钥，其生命周期介于30分钟到7天之间。

密钥加密密钥（KEK） 是一种3DES密钥，用于加密TEK。

认证密钥（AK） 由基站（BS）用于认证相关订户站（SS）的身份，其生命周期也介于30分钟到7天之间。

Mesh模式中的HMAC密钥 用于认证Mesh模式中的相关消息。

上行HMAC密钥 用于认证上行方向的相关消息。

下行HMAC密钥 用于认证下行方向的相关消息。

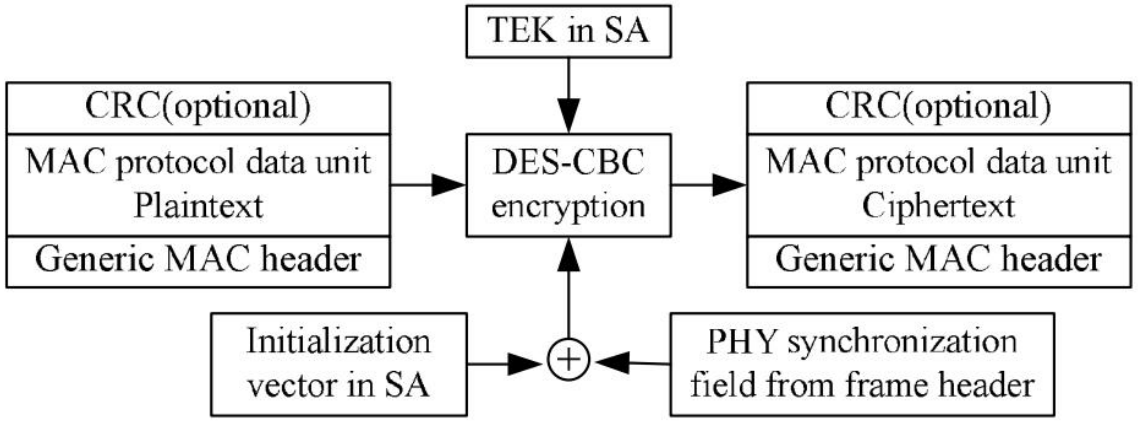
Name	Notation	Length (bit)
Traffic Encryption Key	TEK	128
Key Encryption Key	KEK	128
Authorization Key	AK	160
HMAC Key in Mesh mode	HMAC_KEY_S	
Uplink HMAC Key	HMAC_KEY_U	160
Downlink HMAC Key	HMAC_KEY_D	160

4.包数据加密方法

4.1、DES的CBC模式进行数据加密

如果SA的加密套件中的数据加密算法标识符等于0x01，则与该SA相关的连接上的数据将使用DES算法的CBC模式对MAC PDU有效负载进行加密。

在IEEE 802.16标准中，DES算法提供了56位密钥加密，并且是802.16设备中的强制要求。在完成认证和初始密钥交换过程后，使用TEK加密的数据开始在基站（BS）和用户站（SS）之间传输。使用DES的CBC模式时，MAC协议数据单元（MPDU）的有效负载字段被加密，但通用MAC头（GMH）和循环冗余检查（CRC）则不进行加密。



4.包数据加密方法

4.1、DES的CBC模式进行数据加密

当安全子层生成MPDU时，它会检查与当前连接相关的安全关联（SA）并获取初始化向量（IV）。CBC模式需要一个初始化向量，CBC的初始化向量将按照以下方式计算：

在下行链路（Downlink，DL）中，CBC将通过对以下两个值进行异或（XOR）操作来初始化： TEK密钥信息中的IV参数、当前帧号（右对齐）。

在上行链路（Uplink，UL）中，CBC将通过对以下两个值进行异或操作来初始化：TEK（Traffic Encryption Key，流量加密密钥）密钥信息中的IV参数、传输相关UL-MAP的帧号。

当最后一个块的长度小于64位时，将使用残差终止块处理来加密该块。如下图所示。

type, length, value for parameter 1	
type, length, value for parameter 2	
type, length, value for parameter *n*	
type, length, value for SS MIC	
end of data marker	pad (optional)

4.包数据加密方法

4.2、AES数据加密

AES可以根据应用场景分为四种模式：CBC模式、计数器加密模式（CTR）、带CBC消息认证码的计数器模式（CCM）和电子密码本模式（ECB）。就数据的并行处理能力和加密块的预处理而言，CTR模式比CBC模式更优，并且更容易实现。与CTR模式相比，CCM模式不仅能够加密数据，还能验证加密消息的真实性。ECB模式主要用于加密流量加密密钥（TEK）。

如果加密套件中的数据加密算法标识符为0x02，则与该SA相关的连接上的数据将使用AES算法的CCM模式对MAC PDU有效负载进行加密。如果标识符为 0x80，则与该 SA 关联的连接上的数据应使用 AES 算法的 CTR 模式来加密 MAC PDU 负载。在 MBS 中，AES 块大小和密码计数器块为 128 位。如果标识符为 0x03，则与该 SA 关联的连接上的数据应使用 AES 算法的 CBC 模式来加密 MAC PDU 负载。

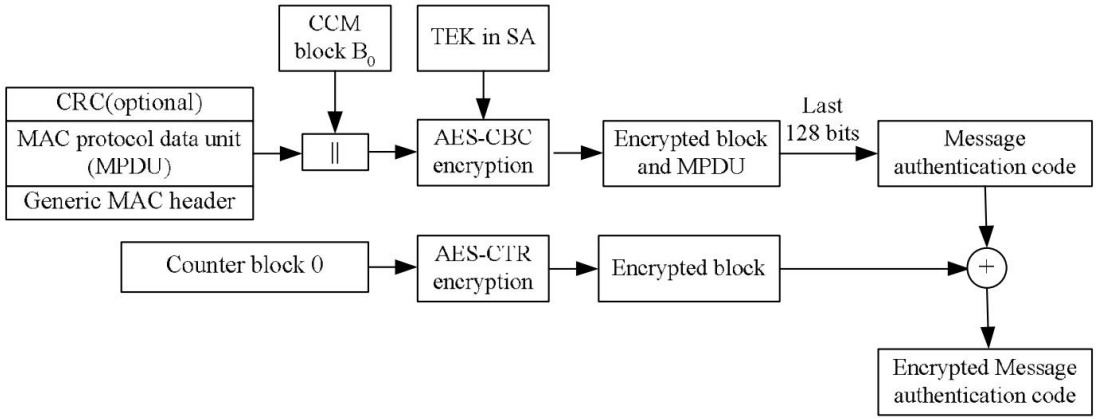
4.包数据加密方法

4.2.1 AES算法的CCM模式

AES-CCM 是一种密钥加密算法，其输出长度为 128 位。它比 DES 和 3DES 更安全。但是，AES-CCM 比 DES （3DES） 更复杂且速度稍慢。

右图说明了消息身份验证代码的创建和后续加密。可以通过加密初始 CCM块和明文负载来获取消息身份验证代码。

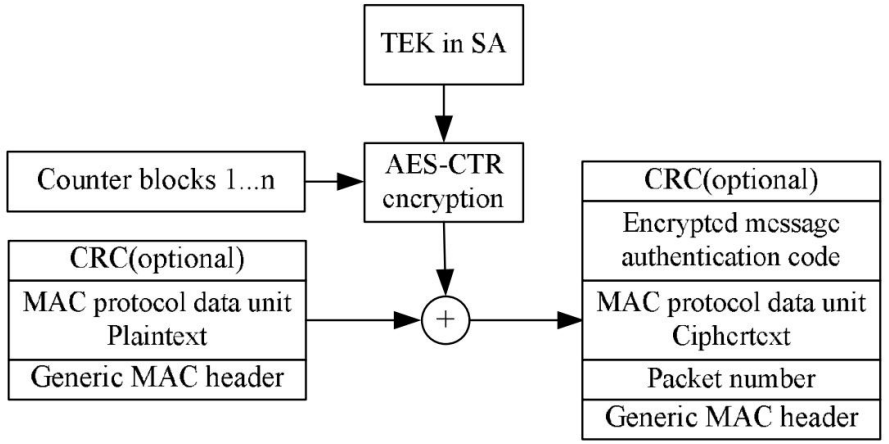
第一步是从 MPDU 派生明文有效负载，并将初始 CCM 块与其连接。然后，我们使用 AES-CBC 算法和 SA 中的 TEK 对后续结果进行加密。我们选择加密输出的最后 128 位（一个 AES 块的大小）作为消息身份验证代码。通过在 SA 中使用 AES-CTR 算法对计数器块 0 进行加密，我们可以对消息鉴权码进行加密，并将加密的块与消息鉴权码进行 XOR 运算，生成加密版本。



4.包数据加密方法

下图说明了 AES-CCM 有效载荷加密的过程。我们可以加密 MAC 协议数据单元，方法是首先使用用于加密消息身份验证代码的相同 TEK 通过 AES-CTR 加密计数器块 1 到 n。然后，将加密的计数器块与 MPDU 进行 XOR 运算，从而产生密文有效载荷。

最后，在密文负载之前添加数据包编号 （PN），并在密文负载之后附加加密消息身份验证代码。然后，后续的密文负载将替换原始的纯文本负载。GMH 中的 EC 位将设置为 1，表示 MPDU 中的负载已加密。EKS 位将被设置为指示使用哪个 TEK。如果涉及 CRC，它将根据 payload 和 MAC 标头的变化进行更新。



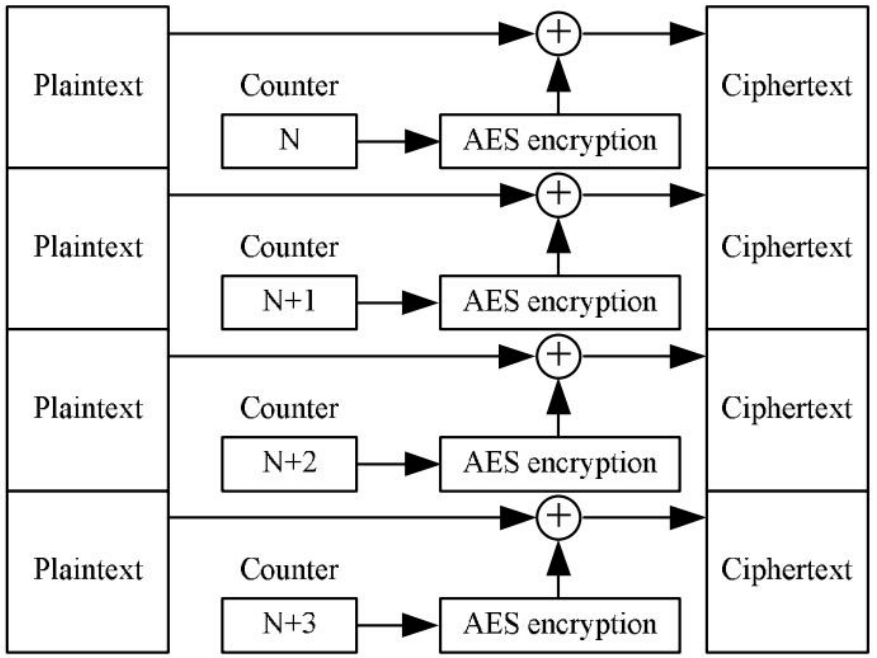
4.包数据加密方法

4.2.2 AES算法的CTR模式

AES-CTR 算法的示例如右图所示。

在 AES-CTR 模式下，在加密明文之前，我们使用 AES 算法对任意块（称为计数器）进行加密，然后将结果与明文进行 XOR 运算以创建密文。对于处理的每个连续块，counter 通常递增 1。对于每个块，即使输入相同，密文也不相同，从而防止攻击者观察到密文中的重复模式。

AES-CTR 的优点是使解密过程与加密完全相同，因为对相同的值进行两次 XOR 运算会产生原始值，从而简化了实现。此外，AES-CTR 还适用于多个块的并行加密。



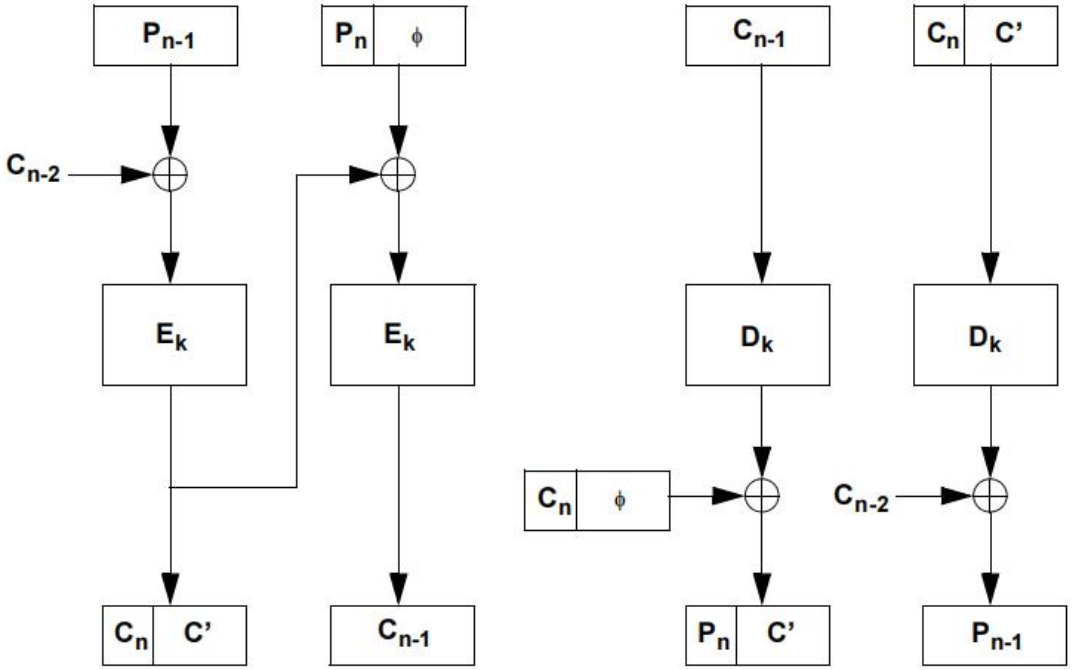
4.包数据加密方法

4.2.3 AES算法的CBC模式

AES 算法的 CBC 模式加密和解密过程如右图所示。

当最后一个明文块长度小于加密块大小时，应使用残差终止块处理对其进行加密。

在 CBC 模式中，每一个明文块在加密前会与前一个密文块进行 异或（XOR），首块则与初始化向量（IV）异或。此模式可以增强加密的随机性，但也要求所有块的长度一致。因此对于最后一个小于标准块长度的明文块，必须先进行填充（padding），使其满足 AES 的块长度（如128位），再进行加密。而为了确保解密方能正确还原明文，发送方必须对最后一个密文块做出特别处理，即残差终止块处理。



4.包数据加密方法

4.3 历届IEEE 802.16标准中加密协议的演进对比

版本	加密协议	密钥管理机制	主要特性	弱点或改进点
IEEE 802.16-2001	DES（Data Encryption Standard）	无明确规范（静态密钥）	初步引入数据加密	加密强度较弱，密钥管理缺失
IEEE 802.16a-2003	DES、Triple DES（3DES）	无认证机制，静态配置	增强加密强度，引入MAC层加密	无动态密钥协商，认证机制缺失
IEEE 802.16-2004	PKMv1（Privacy and Key Management v1）	RSA单向认证，静态配置	支持动态密钥分发，引入X.509证书	只支持单向认证，缺乏灵活性
IEEE 802.16e-2005	PKMv2、AES（Advanced Encryption Standard）	双向认证，支持EAP（可扩展认证协议）	强化认证机制、密钥更新，支持移动性	密钥交换复杂，部分实现不兼容
IEEE 802.16-2009	沿用PKMv2 + AES	多种认证方法可选（EAP-TLS/EAP-TTLS）	更高灵活性，细化密钥生命周期管理	实施复杂，需完善协议一致性
IEEE 802.16m（2011）	AES-CCM（Counter with CBC-MAC）	集成多层认证框架，支持多用户隔离	适配4G安全需求，引入QoS绑定加密策略	实施成本高，安全性依赖EAP实现

5.TEK加密方法

5.1、 使用3-DES加密TEK

对于加密套件中TEK加密算法标识符为0x01的SA，应使用此方法来加密TEK。基站（BS）会加密其发送给客户端SS的Key Reply消息中的TEK值字段。此字段使用两密钥3-DES算法，采用EDE模式，加密细节如下图所示。

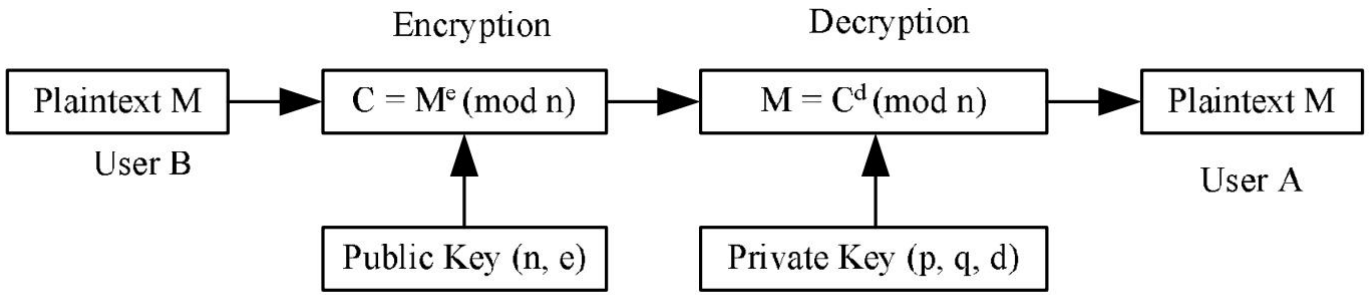
Encryption: C = Ek1[Dk2[Ek1[P]]]
Decryption: P = Dk1[Ek2[Dk1[C]]]
P = Plaintext 64-bit TEK
C = Ciphertext 64-bit TEK
k1 = most significant 64 bits of the 128-bit KEK
k2 = least significant 64 bits of the 128-bit KEK
E[ ] = 56-bit DES ECB mode encryption
D[ ] = 56-bit DES ECB decryption

5.TEK加密方法

5.2、 使用RSA加密TEK

对于加密套件中TEK加密算法标识符为0x02的SA，应使用RSA加密方法（PKCS #1 v2.0）来加密TEK。当使用RSA算法加密TEK时，TEK会使用SS的公钥进行RSA加密。非对称密钥加密使用两个密钥：一个公钥和一个私钥。当密文使用其中一个密钥加密时，只有另一个密钥可以解密。两个密钥是通过相同的算法同时生成的，公钥广泛公开，私钥则保持秘密。

下图为RSA算法的过程。



5.TEK加密方法

5.3、 使用AES加密TEK-128

对于加密套件中TEK加密算法标识符为0x03的SA，应使用此方法来加密TEK-128。基站（BS）会加密其发送给客户端SS的Key Reply消息中的TEK-128值字段。此字段使用128位AES算法，采用ECB模式进行加密。

Encryption: C = Ek1[P]
Decryption: P = Dk1[C]
P = Plaintext 128-bit TEK
C = Ciphertext 128-bit TEK
k1 = the 128-bit KEK
E[ ] = 128-bit AES ECB mode encryption
D[ ] = 128-bit AES ECB decryption

5.TEK加密方法

5.4、 使用AES密钥包装加密TEK-128

对于加密套件中TEK加密算法标识符为0x04的SA，应使用此方法来加密TEK-128。基站（BS）会加密其发送给客户端SS的Key Reply消息中的TEK-128值字段。此字段使用AES密钥包装算法进行加密。

AES密钥包装加密算法会返回密文和一个完整性检查值。解密算法返回明文密钥和完整性检查值。默认的完整性检查值应使用NIST AES密钥包装算法中的值。

Encryption: C,I = Ek[P]
Decryption: P,I = Dk[C]
P = Plaintext 128-bit TEK
C = Ciphertext 128-bit TEK
I = Integrity Check Value
k = the 128-bit KEK
Ek[ ] = AES Key Wrap encryption with key k
Dk[ ] = AES Key Wrap decryption with key k

5.TEK加密方法

5.5、 使用AES密钥包装加密AK（认证密钥）

对于加密套件中TEK加密算法标识符为0x04的SA，应使用此方法来加密AK。MR-BS（移动回传基站）会加密其发送到分布式安全模式下运行的接入RS（接入路由器）的AK Transfer消息中的AK值字段。此字段首先用32位nonce进行填充，然后使用AES密钥包装算法进行加密。

AES密钥包装加密算法接受密文和完整性检查值。解密算法返回明文密钥和完整性检查值。默认的完整性检查值应使用NIST AES密钥包装算法中的值。

Encryption: C, I = Ek [P||N]
Decryption: P||N, I = Dk [C]
P = 160-bit plaintext AK
N = 32-bit random value
C = 192-bit ciphertext
I = Integrity Check Value
k = the 128-bit KEK
Ek [ ] = AES Key Wrap encryption with key k
Dk [ ] = AES Key Wrap decryption with key k

6.消息摘要计算方法

HMAC Digest 属性和 HMAC 元组中键控哈希的计算应使用 HMAC和安全哈希算法 SHA-1。具体细节如下：

DL和UL认证密钥：

HMAC_KEY_D用于对下行（DL）方向的消息进行认证。

HMAC_KEY_U用于对上行（UL）方向的消息进行认证。

密钥派生：

上行（UL）和下行（DL）消息的认证密钥是从AK（认证密钥）中派生出来的。

HMAC序列号：

在HMAC元组或short-HMAC元组中，HMAC序列号应与从HMAC_KEY_x中派生出的AK的AK序列号相同。

PKMv2中的Short-HMAC摘要计算：

在PKMv2中，Short-HMAC摘要计算应包括HMAC_PN_*，该值应在MAC管理消息之后进行拼接。

7.加密算法与模式对比

协议/技术	加密算法与模式	密钥长度	主要特点
WiMAX (802.16e/m)	AES-CCM、AES-GCM	128/256-bit	集成加密与完整性保护（AEAD）
Wi-Fi (WPA2)	AES-CCMP（基于AES-CCM）	128-bit	针对WLAN优化的块加密
Wi-Fi (WPA3)	AES-GCMP、SAE（Simultaneous Authentication of Equals）	192/256-bit	强化密钥协商（抗字典攻击）
LTE/4G	SNOW 3G、AES-CTR	128-bit	流加密（SNOW 3G）与块加密（AES）
5G	AES-CTR、AES-GCM、ZUC（中国标准）	128/256-bit	支持多种算法，增强量子抵抗性
VPN (IPsec)	AES-CBC、AES-GCM、ChaCha20-Poly1305	128/256-bit	灵活模式选择，兼顾性能与安全
TLS/SSL	AES-GCM、ChaCha20-Poly1305	128/256-bit	互联网传输层主流加密，支持AEAD
Zigbee	AES-CCM	128-bit	轻量级物联网专用加密

7.参考文献

[1]付安民.WiMAX无线网络中的密钥管理协议研究[D].西安电子科技大学,2011.
[2]"IEEE Standard for Air Interface for Broadband Wireless Access Systems," in IEEE Std 802.16-2017 (Revision of IEEE Std 802.16-2012) , vol., no., pp.1-2726, 2 March 2018, doi: 10.1109/IEEESTD.2018.8303870.
[3]C. Luo, "A Simple Encryption Scheme Based on WiMAX," 2009 International Conference on E-Business and Information System Security, Wuhan, China, 2009, pp. 1-4, doi: 10.1109/EBISS.2009.5137899.

谢谢！

计算机学院 软件学院
网络空间安全学院
School of Computer Science