ICS 35.020
CCS L 80

团　体　标　准

T/WAPIA 007.11—2025

无线局域网产品工程化实现指南
第11部分：WAPI与IEEE 802.11be

Guides to Wireless Local Area Network Product Engineering Implementation
— Part 11: WAPI & IEEE 802.11be

2025-07-30 发布　　2025-07-30 实施

中关村无线网络安全产业联盟　发布

版权声明

本文件版权归中关村无线网络安全产业联盟所有。

本文件以电子文档形式面向公众公开。本声明在此授权所有组织或者个人对本文件进行使用和复制。任何组织或者个人对本文件的修改、翻译、摘编、汇编、销售行为，应事先获得中关村无线网络安全产业联盟书面授权，否则视为侵权。

联系中关村无线网络安全产业联盟标准化部（lmbz@wapia.org）可获取本文件授权相关信息。

目次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是T/WAPIA 007《无线局域网产品工程化实现指南》的第11部分。T/WAPIA 007已发布了以下部分：

——第 1 部分：WAPI 与 IEEE 802.11n；
——第 2 部分：WAPI 与 IEEE 802.11e；
——第 6 部分：WAPI 与 IEEE 802.11p；
——第 8 部分：WAPI 与 IEEE 802.11ac；
——第 9 部分：WAPI 与 IEEE 802.11ad；
——第 10 部分：WAPI 与 IEEE 802.11ax；
——第 11 部分：WAPI 与 IEEE 802.11be。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村无线网络安全产业联盟与工业和信息化部宽带无线IP标准工作组联合提出。

本文件由中关村无线网络安全产业联盟无线网络安全标准化工作委员会归口。

本文件起草单位：无线网络安全技术国家工程研究中心、西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟、西安芯语慧联信息科技有限公司、高通无线通信技术(中国)有限公司、国家无线电监测中心检测中心、北京数字认证股份有限公司、北京华信傲天网络技术有限公司、新华三技术有限公司、江苏省电子信息产品质量监督检验研究院、广州莲雾科技有限公司。

本文件主要起草人：张变玲、张国强、王江胜、黄振海、王立华、简练、童伟刚、颜湘、陈维刚、陈更、马丹丹、张璐璐、刘剑昕、刘洋、李琴、王月辉、潘琪、牛彬、段铭哲、于江艳、李培、李楠、尹玉昂、赵万峰、卢杰、祝张睿、侯鹏亮、刘婷、吴泽雄、管荑、苑超、蓝海昌。

引　言

本文件是对无线局域网产品工程化实现指南系列标准的完善，其适用于符合GB 15629.11所有部分及其他无线局域网规范和IEEE 802.11be标准的设备，以确保无线局域网产品能提供鉴别和保密通信，并且与其他厂商的无线局域网产品之间具有良好的WAPI安全协议互通性。旨在为符合GB 15629.11所有部分及其他无线局域网规范的无线局域网产品提供组合工程化实现技术。

T/WAPIA 007拟由以下部分构成。

——第1部分：WAPI与IEEE 802.11n。目的在于规范WAPI与IEEE 802.11n组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第2部分：WAPI与IEEE 802.11e。目的在于规范WAPI与IEEE 802.11e组合工程化实现技术，包括数据的处理流程、封装格式等。

——第3部分：WAPI与IEEE 802.11u。目的在于规范WAPI与IEEE 802.11u组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第4部分：WAPI与IEEE 802.11v。目的在于规范WAPI与IEEE 802.11v组合工程化实现技术，包括数据的处理流程、封装格式等。

——第5部分：WAPI与IEEE 802.11r。目的在于规范WAPI与IEEE 802.11r组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第6部分：WAPI与IEEE802.11p。目的在于规范WAPI与IEEE 802.11p组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第7部分：WAPI与IEEE 802.11aa。目的在于规范WAPI与IEEE 802.11aa组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第8部分：WAPI与IEEE 802.11ac。目的在于规范WAPI与IEEE 802.11ac组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第9部分：WAPI与IEEE 802.11ad。目的在于规范WAPI与IEEE 802.11ad组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第10部分：WAPI与IEEE 802.11ax。目的在于规范WAPI与IEEE 802.11ax组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

——第11部分：WAPI与IEEE 802.11be。目的在于规范WAPI与IEEE 802.11be组合工程化实现技术，包括数据的处理流程、封装格式及密码套件的工作模式等。

无线局域网产品工程化实现指南 第11部分:WAPI与IEEE 802.11be

1 范围

本文件规定了WAPI与IEEE 802.11be组合实现时的安全策略协商、密钥建立、 数据处理流程、封装格式及密码套件的工作模式等。给出了WAPI与IEEE 802.11be在产品中组合使用时的实现指南，物理层和媒体访问控制层采用IEEE 802.11be，安全机制采用WAPI，二者的结合方案应依照本指南实施。

本文件适用于WAPI与IEEE 802.11be组合的产品开发、测试和应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 15629.11—2003 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范

GB 15629.11—2003/XG1—2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单

GB/T 32907 信息安全技术 SM4分组密码算法

GB/T 36624 信息技术 安全技术 可鉴别的加密机制

T/WAPIA 045.1—2021 信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第1部分：服务和协议

T/WAPIA 045.3—2021 信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第3部分：采用证书的原子密钥建立与实体鉴别协议

T/WAPIA 045.4—2021 信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别 第4部分：采用预共享密钥的原子密钥建立与实体鉴别协议

T/WAPIA 046—2021 无线局域网安全技术规范

T/WAPIA 046—2021/XG1—2025 无线局域网安全技术规范 第1号修改单

IEEE 802.11be-2024 Information technology- Telecommunications and Information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Enhancements for extremely high throughput (EHT)

3 术语和定义

GB 15629.11—2003和GB 15629.11—2003/XG1—2006界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

AAD 附加鉴别数据（additional authenticated data）

AE	鉴别器实体（authenticator entity）
AKM	鉴别和密钥管理（authentication and key management）
AP	接入点（access point）
ASUE	鉴别请求者实体（authentication supplicant entity）
BK	基密钥（base key）
BKID	基密钥标识（base key identifier）
BKSA	基密钥安全关联（base key security association）
BSS	基本服务集（basic service set）
EEP	可扩展的封装协议(extensible encapsulation protocol)
EHT	极高吞吐率（extremely high throughput）
GCM	伽罗瓦计数器模式（galois/counter mode）
HE	高效率（high efficiency）
IBSS	独立基本服务集（independent basic service set）
ID	标识（identifier）
IE	信息元素（information element）
IMKSA	完整性组播密钥安全关联（integrality multicast key security association）
IV	初始化向量（initialization vector）
MAC	媒体访问控制（media access control）
MIC	消息完整性校验码（message integrity code）
MFPC	管理帧保护可用（management frame protection capable）
MFPR	管理帧保护必选(management frame protection required)
MLD	多链路设备（multi-link device）
MLO	多链路操作（multi-link operation）
MPDU	MAC协议数据单元（MAC protocol data unit）
MSDU	MAC服务数据单元（MAC service data unit）
MSKSA	组播会话密钥安全关联（multicast session key security association）
PDU	协议数据单元（payload data unit）
PN	分组序号（packet number）
QOS	服务质量（quality of service）
STA	站点（station）
USK	单播会话密钥（unicast session key）
USKSA	单播会话密钥安全关联（unicast session key security association）
WAI	无线局域网鉴别基础结构（WLAN authentication infrastructure）
WAPI	无线局域网鉴别与保密基础结构（WLAN authentication and privacy infrastructure）
WAPIE	WAPI信息元素（WAPI information element）
WPI	无线局域网保密基础结构（WLAN privacy infrastructure）

5 多链路模式 WAPI 策略协商

5.1 WAPI 策略通告

AP MLD 所有的附属 AP 通过在信标帧中包含 WAPIE 来通告支持的 WAPI 安全策略。除了鉴别和密钥管理套件列表字段和 WAPI 能力信息字段的 MFPR 子字段外，所有附属于 AP MLD 的 AP 都应通告相同的 WAPIE。附属于 AP MLD 的所有 AP 应在鉴别和密钥管理套件列表字段中通告至少一个相同的鉴别和密钥

管理套件。在 EHT 模式下，应启用管理帧保护。

5.2 WAPI 策略选择

在 MLO 模式下，non-AP MLD 应在(重新)关联请求帧中仅包括一个 WAPIE。WAPIE 应包括一个 AKM 套件、一个单播密码套件和一个组密码套件，这些套件在关联的目标 AP MLD 所有附属 AP 所通告的套件列表中是共同支持的。在 MLO 发现期间，non-AP MLD 通过被动或主动扫描附属于 AP MLD 的 AP 或通过与附属于 AP MLD 的一个或多个 AP 交换多链路探询请求和多链路探询响应帧来确定适当的 AKM 套件和单播密码套件。

注 1：附属于 AP MLD 的所有 AP 通告相同的单播密码套件列表。

注 2：在 MLO 模式下，(重)关联请求和响应帧在附属 STA 和附属 AP 之间传输，但是关联关系是建立在 non-AP MLD 和 AP MLD 之间。

如 AP MLD 鉴别器接收到包含 WAPIE 的(重)关联请求帧，并且如选择接受该关联作为安全关联，则执行以下操作：

——使用(重)关联请求帧中的 AKM 套件和单播密码套件与 non-AP MLD 建立 WAPI 安全关联；

——将(重)关联请求帧中的 MFPC 和 MFPR 位的值与由每个附属 AP 为每个请求的链路通告的 MFPC 和 MFPR 位进行比较，根据管理帧保护策略来确定是否可接受链路请求。

AP MLD 管理 USKSA，附属 AP 管理 MSKSA 和 IMKSA。

6 多链路模式 WAPI 鉴别和密钥建立

6.1 WAPI 安全关联定义

6.1.1 BKSA 是双向的，当身份鉴别过程完成后，BKSA 在 ASUE 或 AE 中创建。BKSA 用于创建 USKSA，BKSA 在它的生存期内被缓存。对于与 AP MLD 关联的 non-AP MLD，BKSA 关联位于 APMLD 和 non-AP MLD 之间。一个 BKSA 包含以下内容：

——BKID，标识 BKSA；

——AE 的 MAC 地址（对于 MLO，AE 的 MAC 地址是 AP MLD 的 MLD MAC 地址）；

——ASUE 的 MAC 地址；

——BK；

——生存期；

——AKM；

——其他安全参数（可选）。

6.1.2 USKSA 是密钥协商的结果，它是双向的。USKSA 是基于 BK 的，在生存期中被缓存。对于每一对 ASUE 和 AE，最多只有两个 USKSA。在 BSS 中，一般只有一个 USKSA 处于有效状态，但在密钥更新时，会有两个 USKSA 处于有效状态，在接收到使用新 USKSA 加密的单播数据 MPDU 时，旧 USKSA 被置为无效状态。在 IBSS 中，MAC_{AE}（AE 的 MAC 地址）大于 MAC_{ASUE}（ASUE 的 MAC 地址）协商出的 USKSA 用于单播数据 MPDU 的保护，其更新密钥的状态和 BSS 相同；MAC_{AE} 小于 MAC_{ASUE} 协商出的 USKSA 不用于单播数据 MPDU 加密，仅用于组播密钥通告，当新的 USKSA 处于有效状态时，旧的 USKSA 立刻处于无效状态。一个 USKSA 包含以下内容：

——USKID；

——USK；

——选择的单播密码套件；

——生存期；

——ASUE 的 MAC 地址；

——AE 的 MAC 地址（在 MLO 模式下，AE 的 MAC 地址是 AP MLD 的 MLD MAC 地址， 而 ASUE 的 MAC 地址是 non-AP MLD 的 MLD MAC 地址）；

——其他安全参数，比如包括用于预鉴别和 STAKey 的重放计数器。

6.1.3 MSKSA 是组播密钥通告的结果。在 BSS 中，只有一个 MSKSA 处于有效状态，AP 用它加密发送的广播/组播 MPDU，STA 用它解密收到的广播/组播 MPDU。在 IBSS 中，每个 STA 有多个有效的 MSKSA，一个用于加密发送的广播/组播 MPDU，其他分别用于解密各个对端 STA 发送的广播/组播 MPDU。在进行 MSKSA 更新时，对于 AP 或每个对端 STA，STA 中用于解密广播/组播 MPDU 的 MSKSA 可有两个处于有效状态，在使用新的 MSKSA 解密收到广播/组播 MPDU 后，旧的 MSKSA 才被置为无效状态；而用于发送加密广播/组播 MPDU 的 MSKSA 只有一个处于有效状态。在已经成功完成多链路(重)建立的 AP MLD 和 non-AP MLD 之间，对于每个建立的链路，存在一个 MSKSA，该 MSKSA 专门用于加密由附属于 AP MLD 的 AP 发送的组寻址 MPDU，以及用于解密附属于 non-AP MLD 的 non-AP STA 接收的组播帧。一个 MSKSA 包含以下内容：

——方向（接收或发送）；
——MSKID；
——选择的组播密码套件；
——生存期；
——MSK；
——AE 的 MAC 地址(在 MLO 模式下，AE 的 MAC 地址是 AP MLD 的 MLD MAC 地址)；
——如 dot11multiLinkActivated 为 true，MSKSA 对应链路的附属 AP 的 MAC 地址；
——其他安全参数（可选）。

6.1.4 IMKSA 是完整性组播密钥通告的结果。在 BSS 中，只有一个 IMKSA 处于有效状态，AP 用它计算广播/组播 MMPDU 的完整性校验码，STA 用它校验收到的广播/组播 MMPDU。在 IBSS 中，每个 STA 有多个有效的 IMKSA，一个用于计算发送的广播/组播 MMPDU 的完整性校验码，其他分别用于校验各个对端 STA 发送的广播/组播 MMPDU。在进行 IMKSA 更新时，对于 AP 或每个对端 STA，STA 中用于校验广播/组播 MMPDU 的 MSKSA 可有两个处于有效状态，在使用新的 IMKSA 校验收到广播/组播 MMPDU 后，旧的 IMKSA 才被置为无效状态；而用于计算完整性校验码并发送广播/组播 MMPDU 的 IMKSA 只有一个处于有效状态。当启用管理帧保护时，当 non-AP MLD 的 SME 接收到完整性组播密钥通告或具有指示成功的状态码的快速 BSS 切换协议的重新关联响应帧时，non-AP MLD 的 SME 为每个建立链路创建 IMKSA。当鉴别器的 SME 建立或改变与其具有有效 USKSA 的所有 STA 的 IMK 时，鉴别器的 SME 创建 IMKSA。当 AP MLD 的 SME 使用在链路上运行并且附属于其具有有效 USKSA 的 non-AP MLD 的所有 non-ap STA 建立或改变 IMK 时，它为其所有链路创建 IMKSA。IMKSA 具有与 BSS 相同的生命周期。一个 IMKSA 包含以下内容：

——方向（接收或发送）；
——IMKID；
——选择的组管理密码套件；
——生存期；
——IMK；
——AE 的 MAC 地址(在 MLO 模式下，AE 的 MAC 地址是 AP MLD 的 MLD MAC 地址)；
——在 MLO 模式下，IMKSA 对应链路的附属 AP 的 MAC 地址；
——其他安全参数（可选）。

6.2 WAPI 密钥管理

在 MLO 模式下，AP MLD 鉴别器和 non-AP MLD 鉴别请求者管理 BK 和单播密钥导出。鉴别和密钥协商都运行在 AP MLD 验证方和 non-AP MLD 请求方之间。附属 AP 管理其各自链路的组播密钥。当组播密钥更新被触发时，所属 AP 将组播密钥分发给 STA。通过 AP MLD 和 non-AP MLD 之间的组播密钥握手而附属于非 AP MLD。

密钥更新。删除 USKSA 后，non-AP MLD 可与相同的 AP MLD 重新关联，并且重新建立 WAPI 安全关联。

在 MLO 模式下，由 AP MLD 的 AE 管理 USKSA 的分组序号分配，对于某一个链路，由附属 AP 管理 MSKSA 和 IMKSA 的分组序号分配，如要启动 MSKSA 和 IMKSA 的更新，由附属 AP 通过 AP MLD 和 non-AP MLD 之间的组密钥握手来更新密钥。

6.3 WAPI 密钥建立

6.3.1 WAPI 密钥数据 IE 字段

6.3.1.1 WAPI 密钥数据 IE 封装

在AP MLD和non-AP MLD之间运行WAPI协议来建立WAPI安全关联，在协议字段中，AE的MAC地址设置为AP MLD的MLD MAC地址，并将ASUE的MAC地址设置为non-AP MLD的MLD MAC地址。

WAPI密钥数据IE采用厂商自定义IE封装，包含了密钥建立时所需要的信息，WAPI密钥数据IE格式见T/WAPIA 046附录B 4.3。

6.3.2 WAPI 密钥建立

6.3.2.1 一般要求

为建立MLD之间的身份鉴别及密钥协商，在单播密钥协商每条消息中增加MAC 地址信息，即发送方MLD的MAC地址，也是AE或ASUE的MAC地址。

在AP发送的密钥信息中消息中增加MLO WAPI-MSK，MLO WAPI-IMK，MLO WAPI-Link Info信息，其中MLO WAPI-Link Info信息包括附属于AP MLD的每个链路的信息。并且该信息的相关字段应与信标帧和探询响应帧中的相应字段内容一致。non-AP STA在收到这些信息时应进行有效性验证。

在non-AP STA发送的密钥信息中消息中增加MLO WAPI-Link Info信息，其中MLO WAPI-Link Info信息包括附属于AP MLD的每个链路的信息。并且该信息的相关字段应与关联请求消息中的相应字段内容保持一致。AP在收到这些信息时应比较验证是否一致。

当安全关联策略协商采用WAI鉴别与密钥建立协议时，在多链路模式下密钥建立协议见6.3.2.2和6.3.2.3，当安全关联策略协商采用WAI2鉴别与密钥建立协议时，在多链路模式下密钥建立协议见6.3.2.4和6.3.2.5。

6.3.2.2 WAI 协议单播密钥建立

6.3.2.2.1 WAI 协议分组格式

WAI 协议分组中各字段如无特殊说明均按大数结尾顺序编码发送。

ASUE、AE 和 ASE 之间的 WAI 协议分组数据的格式定义见图 1。

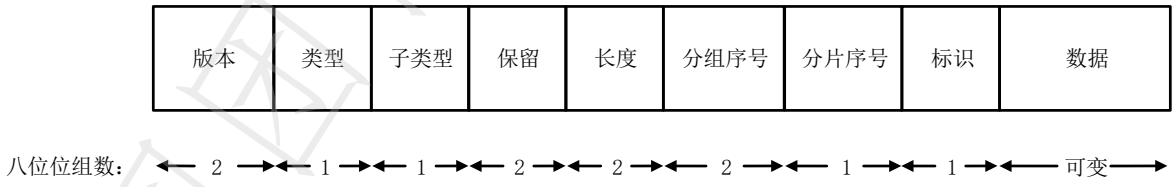

图1 WAI 鉴别系统的 WAI 协议分组数据基本格式

其中：

——版本字段长度为 2 个八位位组，表示鉴别基础结构的版本号。当前版本为 1；

——类型字段长度为 1 个八位位组，表示协议类型，其中：

1 表示 WAI 协议分组；

其他值保留。

——子类型字段的长度为 1 个八位位组，当类型字段的值为 1 时，子类型字段值定义如下：当类型字段为其他值时，子类型字段值保留；

1 表示预鉴别开始分组；

2 表示站间密钥请求分组；

3 表示鉴别激活分组；

4 表示接入鉴别请求分组；
5 表示接入鉴别响应分组；
6 表示证书鉴别请求分组；
7 表示证书鉴别响应分组；
8 表示单播密钥协商请求分组；
9 表示单播密钥协商响应分组；
10 表示单播密钥协商确认分组；
11 表示组播密钥/站间密钥通告分组；
12 表示组播密钥/站间密钥响应分组；
13~20 保留；
21 表示多链路单播密钥协商请求分组；
22 表示多链路单播密钥协商响应分组；
23 表示多链路单播密钥协商确认分组；
24 表示多链路组播密钥/站间密钥通告分组；
25 表示多链路组播密钥/站间密钥响应分组。

注：在 WAI 协议和 IEEE 802.11be 组合实现时，在非 MLO 模式下，单播密钥和组播密钥建立使用子类型 8 至 12 分组类型，在 MLO 模式下，单播密钥和组播密钥建立使用子类型 21 至 25 分组类型。

——保留字段长度为 2 个八位位组，默认值为 0；
——长度字段长度为 2 个八位位组，其值表示 WAI 协议分组所有字段的八位位组数；
——分组序号字段长度为 2 个八位位组，其值表示协议分组序号。第一个分组序号为 1，后序分组依次按 1 递增；
——分片序号字段长度为 1 个八位位组，其值表示分片的顺序编号，每一个分组的第一个分片序号为 0，后序分片依次按 1 递增；
——标识字段长度为 1 个八位位组，位 0 表示后续是否有分片，值为 0 表示没有，值为 1 表示有。位 1 至位 7 保留；
——数据字段的内容根据类型和子类型的值而定，它除了包含固定的内容，还可包含可选的属性。

其中分组序号字段、分片序号字段和标识字段仅在 ASUE 和 AE 之间的 WAI 协议分组中有效。定义 WAI 协议分组的最大长度为 65535 个八位位组。

6.3.2.2.2 多链路单播密钥协商请求分组

多链路单播密钥协商请求分组数据字段格式见图 2。

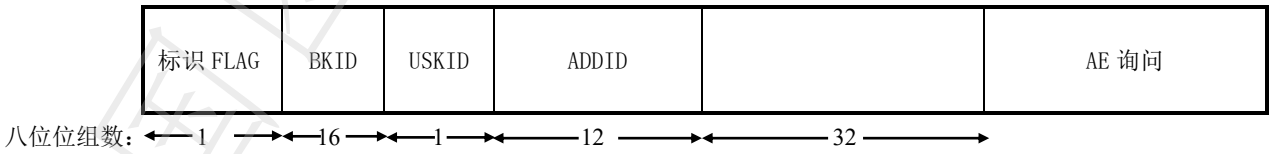

图2 多链路单播密钥协商请求分组数据字段格式

其中：
——标识 FLAG 字段长度为 1 个八位位组，位 4（USK 更新标识）有意义。当 AE 进行会话密钥更新时，位 4（USK 更新标识）的值为 1；否则为 0。其他位保留；
——BKID 字段长度为 16 个八位位组，表示当前作为共享密钥的基密钥，其值为鉴别过程中生成或由预共享密钥导出的 BKID；
——USKID 字段长度为 1 个八位位组，其中位 0 标识当前协商的单播会话密钥，其他位保留。本字段的位 0 在 BKSA 建立后第一次单播密钥协商时初值为 0，以后再重新进行单播密钥协商时该

位在 0 和 1 之间翻转；

——ADDID 字段长度为 12 个八位位组，该字段的值为 $MAC_{AE}||MAC_{ASUE}$；

——AE 询问字段长度为 32 个八位位组，记作 N1。若标识字段的位 4（USK 更新标识）的值为 0，则 AE 的询问为 AE 产生的随机数；若标识字段的位 4（USK 更新标识）的值为 1，则 AE 询问为上一次单播密钥协商过程所协商的值。

在 AE 完成证书鉴别过程并建立有效的 BKSA 后，或采用预共享密钥鉴别方式时，或缓存的 BKSA 被使用，或进行单播密钥更新时，AE 向 ASUE 发送单播密钥协商请求分组开始与 ASUE 进行单播密钥协商。

ASUE 接收到与其相关联的 AE 发送的单播密钥协商请求分组后，进行如下处理：

a) 首先检查 BKID 所指 BKSA 是否有效，若无效，则丢弃该分组；否则检查标识字段的位 4（USK 更新标识）是否为 0，若是 0，执行 c）操作；若是 1，则检查 USKID 所指的 USKSA 是否有效，若有效，则丢弃该分组；否则，执行 b）操作；

b) 检查 AE 询问与本地保存的值是否相同，若不同，则丢弃该分组；否则，执行 c）操作；

c) ASUE 利用随机数产生器产生 ASUE 询问 N_2，然后计算 KD-HMAC-SHA256（BK ，ADDID||N_1||N_2||“pairwise key expansion for unicast and additional keys and nonce”），其中 N_1 为 AE 询问，N_2 为 ASUE 询问。生成 96 个八位位组，前 64 个八位位组为单播会话密钥（第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK，第四个 16 个八位位组为密钥加密密钥 KEK）。最后 32 个八位位组为下一次单播会话密钥协商过程的 AE 询问的种子，然后对该种子使用 SHA-256 函数计算得到长度为 32 个八位位组的下一次单播密钥协商过程的 AE 询问并保存；

d) 用消息鉴别密钥 MAK 通过 HMAC-SHA256 算法计算消息鉴别码，构造单播密钥协商响应分组发往 AE；

e) 若为 BSS 模式，则 ASUE 利用原语 MLME-SETWPIKEYS.request 安装新协商的单播会话密钥；若为 IBSS 模式，只有当 AE 的 MAC 地址大于 ASUE 的 MAC 地址时，ASUE 才利用原语 MLME-SETWPIKEYS.request 安装新协商的单播会话密钥。对于新安装的密钥，ASUE 调用原语 MLME-SETPROTECTION.request 仅启用其接收功能，即允许用其解密 AE 发来的单播数据。

6.3.2.2.3 多链路单播密钥协商响应分组

单播密钥协商响应分组数据字段格式件见图 3。

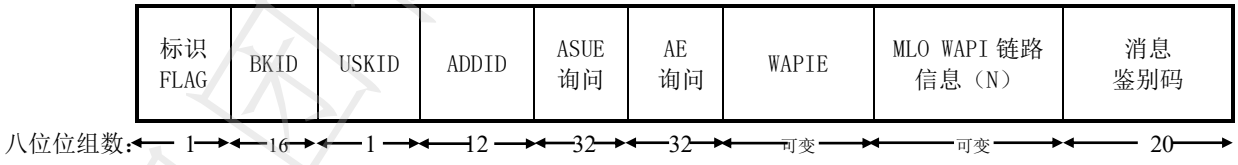

图3 多链路单播密钥协商响应分组数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位位组，位 4（USK 更新标识）有意义。当 AE 进行会话密钥更新时，位 4 （USK 更新标识）的值为 1；否则为 0。其他位保留；

——BKID 字段长度为 16 个八位位组，表示当前共享的基密钥，其值为鉴别过程中生成或由预共享密钥导出的 BKID；

——USKID 字段长度为 1 个八位位组，其中位 0 标识当前协商的单播会话密钥，其他位保留；

——本字段的位 0 初始值为 0，每次重新进行单播密钥协商时该位在 0 和 1 之间翻转；

——ADDID 字段长度为 12 个八位位组，该字段的值为 $MAC_{AE}||MAC_{ASUE}$；

——AE 询问字段长度为 32 个八位位组。若 ASUE 发起密钥更新，ASUE 设置标识字段的位 4 （USK 更新标识）的值为 1，AE 询问字段为上一次单播密钥协商过程所协商的值；否则该字段和单播

密钥协商请求分组中的 AE 询问字段相同；

——ASUE 询问字段长度为 32 个八位位组，由 ASUE 利用随机数产生器生成；

——WAPIE 字段为 ASUE 选择的 WAPIE。在 BSS 模式下，该字段和 ASUE 在关联请求帧中发送的 WAPIE 相同；在 IBSS 模式下，该字段包含 ASUE 选择的单播密码算法、AE 通告的组播密码算法和当前使用的鉴别和密钥管理套件列表；

——收到多链路单播密钥协商响应后，AE 应验证 WAPIE 所有字段的值与(重新)关联请求帧中接收的 WAPIE 相应字段值相同；

——MLO WAPI 链路信息（N），在 MLO 模式下，当 non-AP MLD 在(重新)关联请求帧中请求多于一条链路且单播密钥协商响应分组用于初始密钥协商时，其应包括 MLO WAPI 链路信息（N）密钥数据信息字段，MLO WAPI 链路信息（N）密钥数据信息字段包含对个对应于每个链路的 MLO WAPI 链路信息，其中包含关联请求帧中 Basic Multi-Link element 字段包含的每条链路对应的 LinkID 和与附属 STA 的 MAC 地址。在 MLO 模式下，如多链路单播密钥协商响用于密钥更新，则它应包含 MLO WAPI 链路信息（N）密钥数据信息字段，该密钥数据信息包含对应于每条已建立链路的 LinkID 和附属 STA MAC 地址；

——消息鉴别码字段长度为 20 个八位位组。其值为 ASUE 利用最新协商的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对本字段之前的所有协议数据字段内容计算得到，不包含分组头。

ASUE 进行密钥更新时，或收到 AE 的多链路单播密钥协商请求分组并构造单播密钥协商响应后，发送单播密钥协商响应分组给 AE。

AE 收到单播密钥协商响应分组后，进行如下处理：

a) 若标识字段的位 4（USK 更新标识）为 1，执行 b）操作；否则执行 c）操作；

b) 若当前有有效的 USKSA 并且 USKID 所指 USKSA 无效，则执行 c）操作；否则，丢弃该分组；

c) 检查 AE 询问值是否正确，若不正确，则丢弃该分组；否则，执行 d）操作；

d) 计算 KD-HMAC-SHA256,ADDID||N_1||N_2||“pairwise key expansion for unicast and additional keys and nonce”），其中 N_1 是 AE 询问，N_2 是 ASUE 询问。生成 96 个八位位组，前 64 个八位位组为单播会话密钥（第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK，第四个 16 个八位位组为密钥加密密钥 KEK）。后 32 个八位位组为下一次单播会话密钥协商过程的 AE 询问的种子，然后对种子使用 SHA-256 函数计算得到长度为 32 个八位位组的下一次单播会话密钥协商过程的 AE 询问。利用消息鉴别密钥 MAK 通过 HMAC-SHA256 算法计算消息鉴别码，与分组中的消息鉴别码字段值比较，若相同，则执行操作 e)；否则，丢弃该分组；

e) 若标识字段的位 4（USK 更新标识）为 0，在基础模式下，则检查 WAPIE 字段和自己收到的关联请求帧的 WAPIE 是否相同，若不同，解除与 STA_{ASUE} 的链路验证；若相同，则执行操作 f)；在 IBSS 模式下，检查 WAPIE 字段中选择的单播密钥算法是被支持的，然后执行操作 f)；否则解除与 ASUE 的链路验证；若标识字段的位 4（USK 更新标识）为 1，则执行操作 f)。在 MLO 模式下，如 non-AP MLD 在(重)关联请求帧中的 Basic Multi-Link element 中包括所请求的链路(多条)，并且单播密钥协商响应分组用于初始密钥协商，则验证(重)关联请求帧中的多链路元素中包括的每个链路的附属 STA MAC 地址与单播密钥协商响应分组中的每个链路的附属 STA MAC 地址相同。在 MLO 模式下，如单播密钥协商响应分组用于密钥更新，则验证每个建立链路的附属 STA MAC 地址是否有效。如不同或无效，解除与 STA_{ASUE} 的链路验证；若相同，则执行操作 f)；

f) 用消息鉴别密钥 MAK 通过 HMAC-SHA256 算法本地计算消息鉴别码,构造单播密钥协商确认分组，发送给 ASUE；

g) 若为 BSS 模式，则 AE 利用原语 MLME-SETWPIKEYS.request 安装新协商的单播会话密钥；若为 IBSS 模式，只有当 AE 的 MAC 地址大于 ASUE 的 MAC 地址时，AE 才利用原语 MLME-SETWPIKEYS.request 安装新协商的单播会话密钥。对于新安装的密钥，AE 调用原语

MLME-SETPROTECTION.request 启用其收发功能，即可利用其对单播数据进行加解密。若此次单播密钥协商过程为更新过程，则一旦使用新密钥正确解密数据时，删除旧的单播会话密钥；或者启用新密钥收发数据 60 秒之后，自动删除旧的单播密钥。

6.3.2.2.4 多链路单播密钥协商确认分组

多链路单播密钥协商确认分组数据字段格式见图 4。

标识 FLAG	BKID	USKID	ADDID	ASUE 询问	密钥通告标识	密钥数据长度	WAPI 密钥数据信息密文	消息鉴别码
八位位组数：1	16	1	12	32	16	2	可变	20

图4 多链路单播密钥协商确认分组数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位位组，本字段和多链路单播密钥协商响应分组的标识字段相同；

——BKID 字段长度为 16 个八位位组，本字段和单播密钥协商响应分组的 BKID 字段相同；

——USKID 字段长度为 1 个八位位组，其中位 0 标识当前协商的单播密钥，其他位保留。本字段和单播密钥协商响应分组的 USKID 字段相同；

——ADDID 字段长度为 12 个八位位组，本字段和单播密钥协商响应分组的 ADDID 字段相同；

——ASUE 询问字段长度为 32 个八位位组。本字段和单播密钥协商响应分组中的 ASUE 询问字段相同；

——密钥通告标识字段长度为 16 个八位位组，表示一个整数，初始值为 0x5C365C365C365C365C365C365C365C36，在每次密钥更新通告时该字段值加 1。若通告的密钥不变，则本字段值保持不变。AE 端判断密钥通告标识字段值单调递增溢出后，与所有已关联的 STA 解除链路验证。该字段还用作密钥数据的 IV；

——密钥数据长度为 2 个八位位组，标识 WAPI 密钥数据信息字段的长度；

——WAPI 密钥数据信息密文字段包含用密钥加密密钥 KEK 采用协商选择的单播密码算法对若干个 WAPI 密钥数据 IE 加密后的密文，加密所使用的 IV 为密钥通告标识字段，见图 5。

MLO WAPI-MSK (N)	MLO WAPI-IMK (N)	MLO WAPI 链路信息 (N)

图5 多链路单播密钥协商确认分组 WAPI 密钥数据信息字段格式

其中：

- MLO WAPI-MSK(N)密钥数据 IE 字段，在 MLO 模式下，包含每个已建立链路的 MLO WAPI-MSK 密钥数据信息；
- MLO WAPI-IMK（N）密钥数据 IE 字段，在 MLO 模式下，如协商了管理帧保护，包含每个已建立链路的 MLO WAPI-IMK 密钥数据信息；
- MLO WAPI 链路信息（N）密钥数据 IE 字段，在 MLO 模式下，MLO WAPI 链路信息（N）包含由每个附属 AP 在信标帧和探询响应帧中发送的 LinkID 字段、附属 AP MAC 地址以及 WAPIE。

注 1：在初始安全关联时，在多链路单播密钥协商确认分组中包含所需通告的 MLO WAPI-MSK、MLO WAPI-IMK 等密钥信息，在密钥更新时，采用多链路组播密钥通告协议更新通告密钥。

——消息鉴别码字段长度为 20 个八位位组。其值为 AE 利用最新协商的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对本字段之前的所有协议数据字段内容计算得到，不包含分组头。

注 2：当 non-AP MLD 接收到来自 AP 的信标或探询响应帧时，或者当它接收到附属于同一 AP MLD 的另一个附

属 AP 发送的多链路探询响应时，non-AP MLD 获得附属于该 AP 的 Link ID、AP MAC 地址、WAPIE，该多链路探询响应携带包含该 AP 完整的基本多链路元素。

AE 收到单播密钥响应分组后，发送单播密钥协商确认分组给 ASUE。

ASUE 接收到 AE 的单播密钥协商确认分组后，进行如下处理：

a）在 MLO 模式下，验证每个已建立链路的 WAPIE：

请求方验证每个请求链路的附属 AP MAC 地址和 WAPIE 中的所有字段与 AP MLD 的相应附属 AP 接收的相关字段内容相同。如单播密钥协商确认分组用于密钥更新，则 ASUE 验证每个建立链路的附属 AP MAC 地址和 WAPIE 中的所有字段与 AP MLD 的相应附属 AP 接收的相关字段内容相同。ASUE 验证关联的 AP MAC 地址和 WAPIE 中的所有字段，以及其他发现的链路(如信息可用)中的所有字段，与 AP MLD 的关联 AP 接收的字段内容相同。

注 3：当 non-AP MLD 接收到来自 AP 的信标或探询响应帧时，或者当接收到由附属于同一 AP MLD 的另一个 AP 发送的多链路探询响应时，non-AP MLD 获得与该 AP MLD 关联的 AP 的 Link ID、AP MAC 地址、WAPIE，该多链路探询响应携带包含该 AP 的完整的基本多链路元素。

如以上验证步骤中的任何一个指示不匹配，ASUE 应解除关联或解除链路验证；

b） 检查 ASUE 询问与自己在单播密钥协商响应分组中发送的值是否相同，若不同，则丢弃该分组；否则，执行 c）操作；

c） 利用消息鉴别密钥 MAK 通过 HMAC-SHA256 算法本地计算消息鉴别码，与分组中的消息鉴别码字段值比较，若相同，则执行操作 d)；否则，丢弃该分组；

d） 若标识字段的位 4（USK 更新标识）为 0，则检查 WAPIE 字段和自己收到的信标帧和探询响应帧的 WAPIE 是否相同，若相同，则执行操作 e)；否则，解除与 STA_{AE} 的链路验证。若标识字段的位 4（USK 更新标识）为 1，则执行操作 e)；

e） 调用原语 MLME-SETPROTECTION.request 启用新安装的单播会话密钥的发送功能，即允许利用该新密钥加密发送单播数据。若此次单播密钥协商过程为更新过程，则还需删除旧的单播会话密钥。

6.3.2.3 WAI 组播建立

6.3.2.3.1 WAI 多链路组播密钥建立协议

WAI 多链路组播密钥通告过程使用多链路单播密钥协商过程协商出来的密钥进行组播密钥通告，并建立 MSKSA 和 IMKSA，协议见图 6。

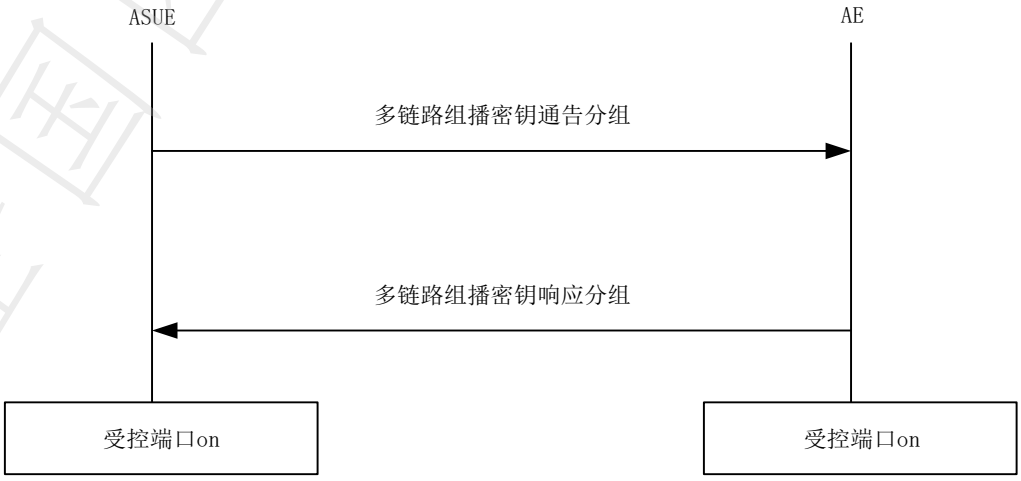

图6 多链路组播密钥通告过程

6.3.2.3.2 WAI 多链路组播密钥通告分组

单播密钥协商成功后，或 AE 要更新组播密钥时， AE 向 ASUE 发送组播密钥/站间密钥通告分组通告组播密钥。

多链路组播密钥通告分组数据字段格式见图 7。

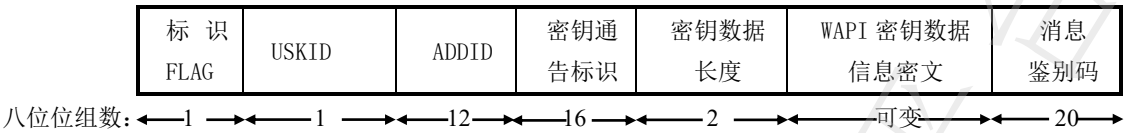

图7 多链路组播密钥通告分组数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位位组，该字段作为保留字段；

——USKID 字段长度为 1 个八位位组，其中位 0 标识计算消息鉴别码字段值所用的消息鉴别密钥 MAK；

——ADDID 字段长度为 12 个八位位组。该字段的值为 $MAC_{AE}||MAC_{ASUE}$；

——密钥通告标识字段长度为 16 个八位位组，表示一个整数，初始值为 0x5C365C365C365C365C365C365C365C36，在每次密钥更新通告时该字段值加 1。若通告的密钥不变，则本字段值保持不变。AE 端判断密钥通告标识字段值单调递增溢出后，与所有已关联的 STA 解除链路验证。该字段还用作密钥数据的 IV；

——密钥数据长度为 2 个八位位组，标识 WAPI 密钥数据信息字段的长度；

——WAPI 密钥数据信息密文字段包含用密钥加密密钥 KEK 采用协商选择的单播密码算法对若干个 WAPI 密钥数据 IE 加密后的密文，加密所使用的 IV 为密钥通告标识字段，见图 8。

MLO WAPI-MSK (N)	MLO WAPI-IMK (N)	MLO WAPI 链路信息 (N)

图8 多链路组播密钥通告分组 WAPI 密钥数据信息字段格式

其中：

- MLO WAPI-MSK(N)密钥数据 IE 字段,在 MLO 模式下,包含每个已建立链路的 MLO WAPI-MSK 密钥数据；
- MLO WAPI-IMK（N）密钥数据 IE 字段，在 MLO 模式下，如协商了管理帧保护，包含每个已建立链路的 MLO WAPI-IMK 密钥数据；
- MLO WAPI 链路信息（N）密钥 IE 字段，在 MLO 模式下，MLO WAPI 链路信息（N）包含由每个附属 AP 在 Beacon 和探询响应帧中发送的包含 LinkID 字段、附属 AP MAC 地址以及 WAPIE。

——消息鉴别码字段长度为 20 个八位位组。其值为 AE 利用 USKID 字段标识的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对本字段之前的所有协议数据字段内容计算得到，不包含分组头。

ASUE 接收到 AE 发送的组播密钥/站间密钥通告分组后，进行如下处理：

a） ASUE 利用 USKID 字段标识的消息鉴别密钥 MAK 计算校验值，与消息鉴别码字段值进行比较，若不同，则丢弃该分组；否则执行 b）操作；

b） 检查密钥通告标识字段值是否单调递增，若为单调递增，则执行 c）操作；否则丢弃该分组；

c） 对密钥数据解密得到组播会话密钥和/或完整性组播密钥；

d） 保存密钥通告标识字段值，生成组播密钥响应分组，发送给 AE；

e） 安装或删除密钥。若此次为组播密钥通告过程，则利用原语 MLME-SETWPIKEYS.request 为指定的链路安装新的组播会话密钥和/或完整性组播密钥，并调用原语

MLME-SETPROTECTION.request 启用其接收功能；若此次组播密钥通告过程为 BKSA 建立后的首次通告过程，则将受控端口的状态设置为 On；若此次组播密钥通告过程为更新过程，则一旦使用此新密钥正确解密过数据时，删除旧的组播密钥和/或完整性组播密钥。

若 AE 通告了新的组播密钥和/或完整性组播密钥，ASUE 保存组播密钥和/或完整性组播密钥，在接收组播数据帧时根据 KeyID 字段选择组播会话密钥，当 ASUE 接收到 AE 用最新通告的组播密钥加密/完整性保护的组播数据帧，并且校验和解密均正确时，丢弃旧的组播会话密钥和/或完整性组播密钥。

6.3.2.3.3 WAI 多链路组播密钥响应分组

多链路组播密钥响应分组数据字段格式见图 9。

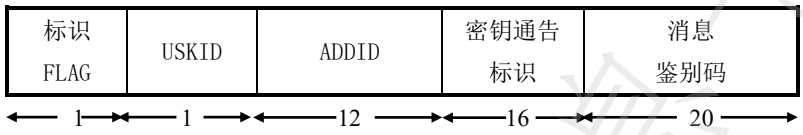

图9　多链路组播密钥响应分组数据字段格式

其中：

——标识字段长度为 1 个八位位组，此字段值应与 AE 发送的组播密钥/站间密钥通告分组中的标识字段值相同；

——USKID 字段长度为 1 个八位位组，其中位 0 标识计算消息鉴别码字段值所用的消息鉴别密钥 MAK。此字段值应与 AE 发送的组播密钥/站间密钥通告分组中的 USKID 字段值相同；

——ADDID 字段长度为 12 个八位位组，该字段的值和组播密钥/站间密钥通告分组中 ADDID 字段值相同；

——密钥通告标识字段长度为 16 个八位位组，表示一个整数，取值为 AE 发送的组播密钥/站间密钥通告分组中的密钥通告标识字段值；

——消息鉴别码字段长度为 20 个八位位组。其值为 ASUE 利用 USKID 字段标识的消息鉴别密钥 MAK 通过 HMAC-SHA256 算法对本字段之前的所有协议数据字段内容计算得到，不包含分组头。

ASUE 向 AE 发送组播密钥/站间密钥响应分组，AE 接收到 ASUE 发送的组播密钥响应分组后，进行如下处理：

a） 利用 USKID 字段标识的消息鉴别密钥 MAK 计算校验值，与消息鉴别码字段值进行比较，若不同，则丢弃该分组；否则，执行 b）操作；

b） 比较标识、USKID 字段、ADDID 字段和密钥通告标识字段与发送的组播密钥/站间密钥通告分组中的相应字段值，若均相同，则本次组播密钥/站间密钥通告成功；否则，丢弃该分组；

c） 通告成功后，若此次通告的密钥尚未安装，则利用原语 MLME-SETWPIKEYS.request 安装新密钥。AE 调用原语 MLME-SETPROTECTION.request 启动新密钥的发送功能，即利用此密钥加密组播数据；若此次组播密钥通告过程为 BKSA 建立后的首次通告过程，则将受控端口的状态设置为 On；若此次组播密钥通告过程为更新过程且已通告给所有已关联的 ASUE，则删除旧密钥。

AE 在更新组播密钥过程中，使用旧的组播密钥对组播数据帧进行加密发送，当对所有已关联到该 AP 的 STA 均组播密钥通告后，才启用最新通告的组播密钥用于组播数据帧的加密发送。

6.3.2.4 WAI2 单播密钥建立

WAI2协议鉴别采用AKEA协议，AKEA提供多种鉴别与密钥建立方法，实现实体鉴别的同时，完成基密钥和单播密钥的建立。其中鉴别和密钥管理必应支持双向鉴别，WAI2协议支持AKEA-C和AKEA-P协议，AKEA-C鉴别协议定义见T/WAPIA 045.3—2021，AKEA-P鉴别协议定义见T/WAPIA 045.4—2021。WAPI中的ASUE实体对应AKEA中的REQ，WAPI的AE实体对应AKEA中AAC,WAPI实体中的ASE实体对应AKEA中的AS。

在AKEA协议中，通过附带文本Text字段封装密钥建立过程中的密钥数据信息。

在AKEA-C-AACInit和AKEA-P-AACInit消息负载中， $Text_{AAC}$（$Text_{AAC}$字段定义见T/WAPIA 045.1—2021）字段封装AE的WAPI密钥数据信息，其中Text数据元素中的数据元素值字段格式见图10。

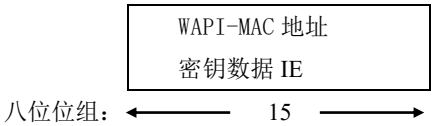

图10　AKEA-C-AACInit 和 AKEA-P-AACInit 中 TextAAC 数据元素值格式

其中：

——WAPI-MAC 密钥数据地址 IE，其中包含的 Mac 地址为 AP MLD 的 MAC 地址。

在AKEA-C-REQInit和AKEA-P-REQInit消息负载中， $Text_{REQ}$字段封装ASUE的WAPI密钥数据信息，其中Text数据元素中的数据元素值字段格式见图11。

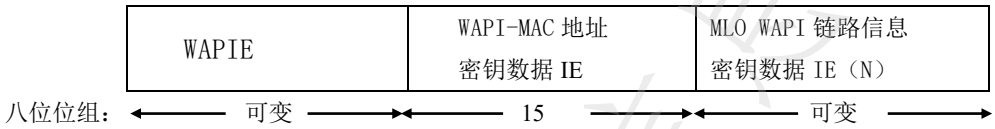

图11　AKEA-C-REQInit 和 AKEA-P-REQInit 中 TextREQ 数据元素值字段格式

其中：

——WAPIE 字段为 ASUE 发送的 WAPIE。在 BSS 模式下，该字段和 ASUE 在关联请求帧中发送的 WAPIE 相同；在 IBSS 模式下，该字段包含 ASUE 选择的单播密码算法、AE 通告的组播密码算法和当前使用的鉴别和密钥管理套件列表。收到 AKEA-C-REQInit 或 AKEA-P-REQInit 消息后，AE 应验证 WAPIE 所有字段的值与(重新)关联请求帧中接收的 WAPIE 相应字段值相同；

——WAPI-MAC 地址密钥数据 IE，其中包含的 Mac 地址为 non-AP MLD 的 MAC 地址；

——MLO WAPI 链路信息密钥数据 IE（N），在 MLO 模式下，当 non-AP MLD 在(重新)关联请求帧中请求多于一条链路时，其应包括 MLO WAPI 链路信息密钥数据 IE 字段（N），包含对应于每个链路的 MLO WAPI 链路信息密钥数据 IE，MLO WAPI 链路信息密钥数据 IE 包含关联请求中 Basic Multi-Link element 字段包含的每条链路对应的 LinkID 和与附属 STA 的 MAC 地址。

在AKEA-C-AACauth和AKEA-P-AACAuth消息负载中，$Text_{AAC}$字段封装AE的WAPI密钥数据信息，WAPI密钥数据信息字段包含若干个WAPI密钥数据IE，其中$Text_{AAC}$数据元素中的数据元素值字段格式见图12。

WAPI-MAC 地址	WAPIE	WAPI-MSK	WAPI-IMK	MLO WAPI-MSK（N）	MLO WAPI-IMK（N）	MLO WAPI 链路信息（N）

图12　AKEA-C-AACauth 和 AKEA-P-AACAuth 中 TextAAC 数据元素值字段格式

其中：

——WAPI-MAC 地址密钥数据 IE，其中包含的 Mac 地址为 AP MLD 的 MAC 地址；

——WAPIE 字段为 AE 在信标帧和探询响应帧中发送的 WAPIE，在非 MLO 模式下，该字段存在；

——WAPI-MSK 密钥数据 IE 字段，包含 AE 通告的组播会话密钥，在非 MLO 模式下，该字段存在；

——WAPI-IMK 密钥数据 IE 字段，包含 AE 通告的完整性组播密钥，在非 MLO 模式下，该字段存在；

——MLO WAPI-MSK 密钥数据 IE（N），在 MLO 模式下每个链路的组播回话密钥；

——MLO WAPI-IMK（N）密钥数据 IE 字段，在 MLO 模式下，如协商了管理帧保护，包含每个已建立链路的 MLO WAPI-IMK 密钥数据 IE；

——MLO WAPI 链路信息密钥数据 IE（N）字段，在 MLO 模式下，MLO WAPI 链路信息（N）包含每个

链路的 MLO WAPI 链路信息密钥数据 IE，由每个附属 AP 在 Beacon 和探询响应帧中发送的包含 LinkID 字段、附属 AP MAC 地址以及 WAPIE 组成。

注：在初始安全关联时，应在 AKEA-C-AACauth 和 AKEA-P-AACAuth 消息中包含所需通告的 MLO WAPI-MSK、MLO WAPI-IMK 等密钥信息，在密钥更新时，采用组播密钥建立协议更新通告密钥。

在AKEA-C-REQauth和AKEA-P-REQAuth消息负载中， $Text_{AAC}$字段封装AE的WAPI密钥数据信息，其中Text数据元素中的数据元素值字段格式见图13。

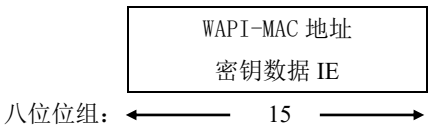

图13　AKEA-C-REQauth 和 AKEA-P-REQAuthText 中 $Text_{AAC}$ 数据元素值字段格式

其中：WAPI-MAC地址IE，其中包含的Mac地址为non-AP MLD的MAC地址。

在AKEA-P-AACResp消息负载中，$Text_{AAC}$字段封装AE的WAPI密钥数据信息，其中$Text_{AAC}$中的数据元素值字段格式见图14。

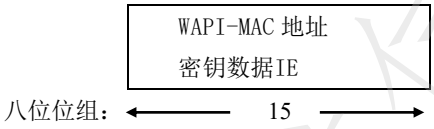

图14　AKEA-P-AACResp 中 $Text_{AAC}$ 数据元素值字段格式

其中WAPI-MAC地址IE，其中包含的Mac地址为AP MLD的MAC地址。

EncData类型和Text类型的数据元素定义见T/WAPIA 045.1—2021第5章中的规定。

6.3.2.5　WAI2 组播密钥建立

6.3.2.5.1　WAI2 组播密钥建立协议

WAI2组播密钥分组和组播密钥响应分组封装在加密的可扩展的封装协议EEP安全数据通信（组播密钥分发）格式的数据部分。EEP见T/WAPIA 045.1—2021第8章中的规定。组播密钥密钥通告过程分组中固定字段定义见T/WAPIA 046—2021中6.2.2.1.1。

WAI2组播密钥建立协议见图15。

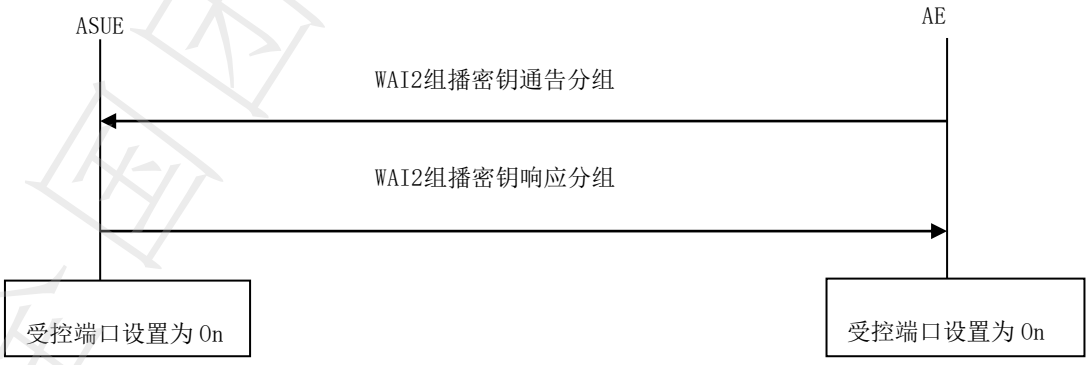

图15　WAI2 组播密钥通告过程

EEP中封装的组播密钥分发数据格式见16。

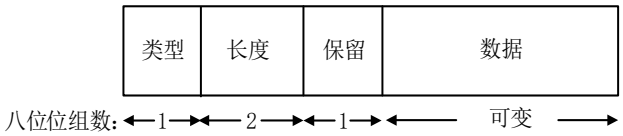

图16　组播密钥分发数据格式

其中：

——类型字段长度为 1 个八位位组，标识消息类型，类型字段的值定义如下：

1 表示组播密钥钥通告分组；

2 表示组播密钥响应分组；

其他值保留；

——长度字段长度为 2 个八位位组，标识组播密钥分发数据所有字段的长度；

——保留字段长度为 1 个八位位组，默认值为 0；

——数据字段的内容根据类型字段的值而定。

6.3.2.5.2　WAI2 组播密钥通告分组

单播密钥协商成功后，或 AE 要更新组播密钥时， AE 向 ASUE 发送组播密钥通告分组通告组播密钥。WAI2 组播密钥通告分组数据字段格式见图 17。

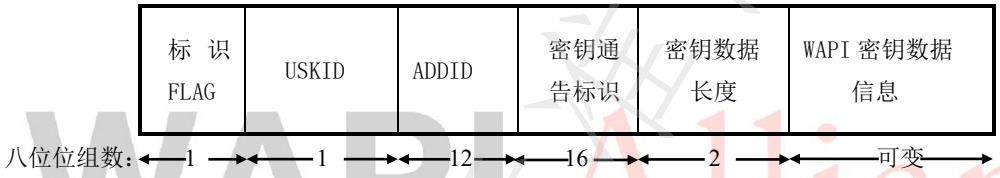

图17　WAI2 组播密钥通告分组数据字段格式

其中：

——标识 FLAG 字段长度为 1 个八位位组，该字段作为保留字段；

——USKID 字段长度为 1 个八位位组；

——ADDID 字段长度为 12 个八位位组。该字段的值为 $MAC_{AE}||MAC_{ASUE}$；

——密钥通告标识字段长度为 16 个八位位组，表示一个整数，初始值为 0x5C365C365C365C365C365C365C365C36，在每次密钥更新通告时该字段值加 1。若通告的密钥不变，则本字段值保持不变。AE 端判断密钥通告标识字段值单调递增溢出后，与所有已关联的 STA 解除链路验证；

——密钥数据长度为 2 个八位位组，标识 WAPI 密钥数据信息字段的长度；

——WAPI 密钥数据信息字段包含若干个 WAPI 密钥数据 IE，见图 18。

WAPI-MAC 地址	WAPI-MSK	WAPI-IMK	MLO WAPI-MSK（N）	MLO WAPI-IMK（N）	MLO WAPI 链路信息（N）

图18　WAI2 组播密钥通告分组 WAPI 密钥数据信息字段格式

其中：

- WAPI-MAC 地址密钥数据 IE，其中包含的 Mac 地址为 AP MLD 的 MAC 地址；
- WAPI-MSK 密钥数据 IE 字段，包含 AE 通告的组播会话密钥。在非 MLO 模式下，该字段存在；
- WAPI-IMK 密钥数据 IE 字段，包含 AE 通告的完整性组播密钥。在非 MLO 模式下，该字段

存在；

- MLO WAPI-MSK（N）密钥数据 IE 字段，在 MLO 模式下，包含每个已建立链路的 MLO WAPI-MSK 密钥数据；
- MLO WAPI-IMK（N）密钥数据 IE 字段，在 MLO 模式下，如协商了管理帧保护，包含每个已建立链路的 MLO WAPI-IMK 密钥数据信息；
- MLO WAPI 链路信息 IE（N）密钥数据字段，在 MLO 模式下，MLO WAPI 链路信息（N）包含由每个附属 AP 在 Beacon 和探询响应帧中发送的包含 LinkID 字段、附属 AP MAC 地址以及 WAPIE。

ASUE 接收到 AE 发送的组播密钥/站间密钥通告分组后，进行如下处理：

a） 检查密钥通告标识字段值是否单调递增，若为单调递增，则执行 b）操作；否则丢弃该分组；

b） 对密钥数据解密得到组播会话密钥和/或完整性组播密钥；

c） 保存密钥通告标识字段值，生成组播密钥响应分组，发送给 AE；

d） 安装或删除密钥。若此次为组播密钥通告过程，则利用原语 MLME-SETWPIKEYS.request 为指定的链路安装新的组播会话密钥或完整性组播密钥，并调用原语 MLME-SETPROTECTION.request 启用其接收功能；若此次组播密钥通告过程为 BKSA 建立后的首次通告过程，则将受控端口的状态设置为 On；若此次组播密钥通告过程为更新过程，则一旦使用此新密钥正确解密过数据时，删除旧的组播密钥或完整性组播密钥。

若 AE 通告了新的组播密钥或完整性组播密钥，ASUE 保存组播密钥或完整性组播密钥，在接收组播数据帧时根据 KeyID 字段选择组播会话密钥，当 ASUE 接收到 AE 用最新通告的组播密钥加密或完整性保护的组播数据帧，并且校验和解密均正确时，丢弃旧的组播会话密钥或完整性组播密钥。

6.3.2.5.3 WAI2 组播密钥响应分组

WAI2 组播密钥响应分组数据字段格式见图 19。

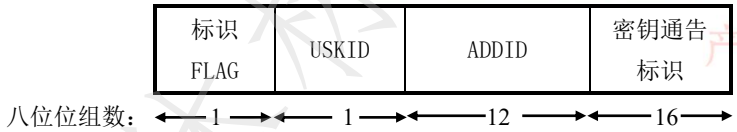

图19 WAI2 组播密钥响应分组数据字段格式

其中：

——标识字段长度为 1 个八位位组，此字段值应与 AE 发送的组播密钥/站间密钥通告分组中的标识字段值相同；

——USKID 字段长度为 1 个八位位组，此字段值应与 AE 发送的组播密钥/站间密钥通告分组中的 USKID 字段值相同；

——ADDID 字段长度为 12 个八位位组，该字段的值和组播密钥/站间密钥通告分组中 ADDID 字段值相同；

——密钥通告标识字段长度为 16 个八位位组，表示一个整数，取值为 AE 发送的组播密钥/站间密钥通告分组中的密钥通告标识字段值。

ASUE 向 AE 发送 WAI2 组播密钥响应分组，AE 接收到 ASUE 发送的 WAI2 组播密钥响应分组后，进行如下处理：

a） 利用 USKID 字段标识的消息鉴别密钥 MAK 计算校验值，与消息鉴别码字段值进行比较，若不同，则丢弃该分组；否则，执行 b）操作；

b） 比较标识、USKID 字段、ADDID 字段和密钥通告标识字段与发送的 WAI2 组播密钥通告分组中的相应字段值，若均相同，则本次组播密钥通告成功；否则，丢弃该分组；

c） 通告成功后，若此次通告的密钥尚未安装，则利用原语 MLME-SETWPIKEYS.request 安装新密钥。

AE 调用原语 MLME-SETPROTECTION.request 启动新密钥的发送功能，即利用此密钥加密组播数据；若此次组播密钥通告过程为更新过程且已通告给所有已关联的 ASUE，则删除旧密钥。

AE 在更新组播密钥过程中，使用旧的组播密钥对组播数据帧进行加密发送，当对所有已关联到该 AP 的 STA 均组播密钥通告后，才启用最新通告的组播密钥用于组播数据帧的加密发送。

6.3.2.6 多链路重配置密钥建立

6.3.2.6.1 多链路重配置

Non-AP MLD 和 AP MLD 可通过一组流程将一条或多条链路添加到多链路操作中（过程见 IEEE 802.11be：35.3.6）。

如 AP MLD 接受添加一条或多条链路，且在启用 WAPI 时，AP MLD 应在链路重配置响应帧中包含密钥数据信息字段。对于每个添加的链路，AP MLD 将在密钥数据信息字段中包含 MLO WAPI-MSK 和 MLO WAPI-IMK，作为由 LinkID 子字段标识链路的组播会话密钥和完整性组播密钥。AP MLD 和 Non-AP MLD 为新建立的链路建立安全关联。

当 AP MLD 和 Non-AP MLD 通过多链路重配置删除链路时，应删除该链路对应的安全关联，包括 MSKSA 和 IMKSA。

6.3.2.6.2 链路重配置响应帧格式

当 AP MLD 接收到 non-AP MLD 发送的链路重配置请求帧时，发送链路重配置响应帧，以接受或拒绝 non-AP MLD 的多链路建立添加或删除请求。

链路重配置响应帧是受保护的 EHT 的 Action 帧。链路重配置响应帧的 Action 字段包含的信息见表 2。

表 2 链路重配置响应 Action 帧字段格式

次序	字段内容
1	类型值
2	受保护的 EHT Action 字段
3	对话令牌
4	计数
5	重配置状态列表
6	组播密钥数据（可选）
7	OCI 元素（可选）
8	Basic Multi-Link 元素

链路重配置响应 Action 帧字段格式定义见 IEEE 802.11be：9.6.38.14。

组播密钥数据子字段为可选，可包含成功添加的多链路(状态值为成功时)链路组密钥，格式见图 20。

如在链路重配置响应帧中没有将相应链路重配置请求帧中请求的链路添加指示为成功，则不包含该子字段。

图20 组播密钥数据字段格式

其中：

——密钥数据长度是 WAPI 密钥数据信息字段的八位位组数；

——WAPI 密钥数据信息字段包含对应于添加链路的一个或多个多链路组播密钥数据 IE。每个 MLO 密钥数据都使用 6.3.1.1 中图 1 所示的 WAPI 密钥数据 IE 格式进行封装。

注：每个多链路 WAPI 密钥数据对应于特定的链路，包含 linkID。

7 多链路模式下数据处理

7.1 WPI 完整性校验的数据组成

参与WPI完整性校验计算的数据来自于MAC头，由于部分字段值在传输等操作中会产生变化，并不是所有MAC头中的数据都被用于完整性校验计算（例如，持续时间字段），或者一些字段值在用于完整性校验计算的时候被屏蔽置为0。参与WPI完整性校验计算的数据组成见图21。

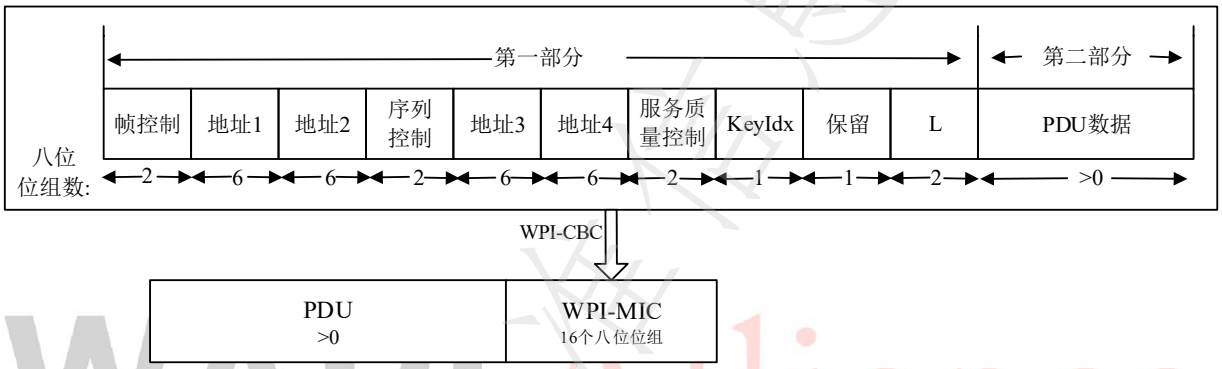

图21 完整性校验数据

其中，完整性校验数据包含二部分内容：

第一部分：

——帧控制字段长度为 2 个八位位组；

1) 位 4、5、6 在数据帧中置为 0；
2) 位 11、12、13 置为 0；
3) 位 14 置为 1；
4) 位 15：当该分组时包含 QoS Control 字段的数据帧时置为 0，；

——地址 1 字段长度为 6 个八位位组。按如下设置：

- 如 MPDU 是 AP MLD 和与之相关联的 non-AP MLD 之间的单播数据帧，则地址 1 设置为 MPDU 的预期接收者 MLD 的 MLD MAC 地址；
- 否则，地址 1 设置为 MPDU 地址 1 字段。

——地址 2 字段长度为 6 个八位位组。按如下设置：

- 如 MPDU 是 AP MLD 和与之相关联的 non-AP MLD 之间的单播数据帧，则设置地址 2 设置为 MPDU 的发送方的 MLD MAC 地址；
- 否则，地址 2 设置为 MPDU 地址 2 字段。

——序列控制（位 4—15 置为 0）字段长度为 2 个八位位组；

——地址 3 字段长度为 6 个八位位组。设置如下：

- MPDU 地址 3 是 BSSID,并且 MPDU 是 AP MLD 和与之相关联的 non-AP MLD 之间的单播数据帧，则将地址 3 设置为 AP MLD 的 MLD MAC 地址；
- 否则将地址 3 设置为 MPDU 地址 3 字段。

——地址 4 字段长度为 6 个八位位组，若 MAC 帧头中不存在地址 4，则该字段的 6 个八位位组的值均置为 0，如存在设置如下；

- MPDU 地址 4 是 BSSID,并且 MPDU 是 AP MLD 和与之相关联的 non-AP MLD 之间的单播数据帧，则地址 4 为 AP MLD 的 MLD MAC 地址；

- 否则，则将其设置为 MPDU 地址 4 字段。

——服务质量控制 QC 字段长度为 2 个八位位组；若 MAC 帧头包含服务质量控制字段，则该字段存在。服务质量控制表示 MSDU 的优先级。QC TID 字段用于构建 AAD，保留原始值。如在 non-DMG BSS 中里 STA 和对端的 SPP A-MSDU Capable 字段都为 1，那么 AAD 构建里使用位 7（the A-MSDU Present 字段）。当 STA 或对端的 SPP A-MSDU Capable 字段为 0，QC 字段的其余位设置为 0（位 4～6,8～15，位 7）。数据发送时，在 DMG BSS 中，位 7 和位 8（A-MSDU Type 字段）用于构建 AAD，其余位的值在构建 AAD 时设为 0（位 4～6，位 9～15）。

——KeyIdx 字段长度为 1 个八位位组；

——保留：1 个八位位组；

——L 字段长度为 2 个八位位组，该字段表示 PDU 数据的长度，按大数结尾编码计算。

7.2 WPI-SM4-GCM 工作模式

WPI-SM4-GCM工作模式采用SM4加密算法，SM4算法见GB/T 32907，加密和完整性校验模式采用GCM。GCM保护MPDU数据字段和MPDU报头的选定部分的完整性，提供数据机密性、身份鉴别、完整性和重播保护。GCM应符合GB/T 36624—2018第11章的规定。WAPI和IEEE802.11be组合实现时，应启用WPI-SM4-GCM工作模式。

数据发送时，WPI-SM4-GCM的MPDU发送处理见图22。

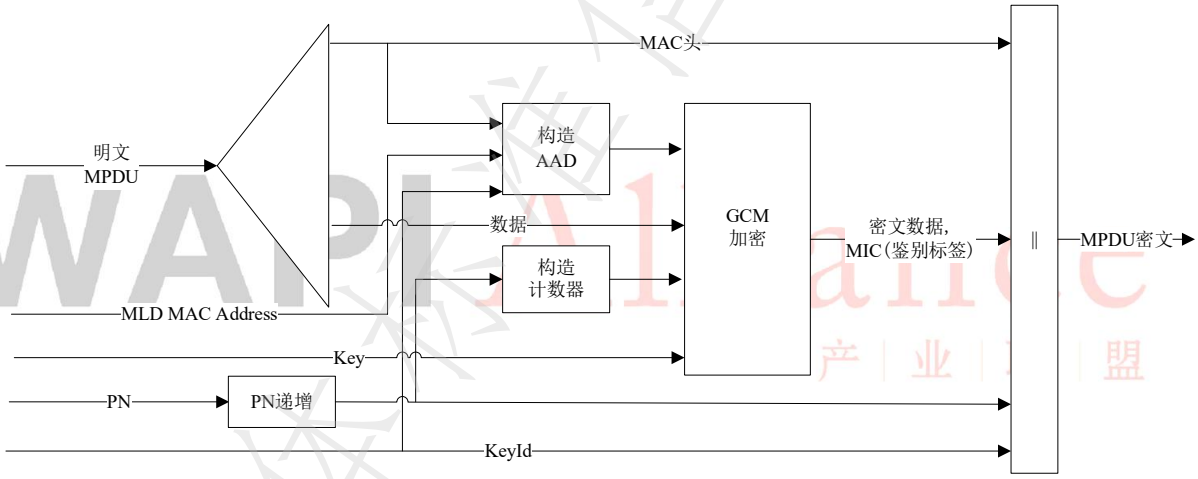

图22 WPI-SM4-GCM 的 MPDU 发送处理

数据发送时，WPI-SM4-GCM封装与输入参数的映射关系见图23。

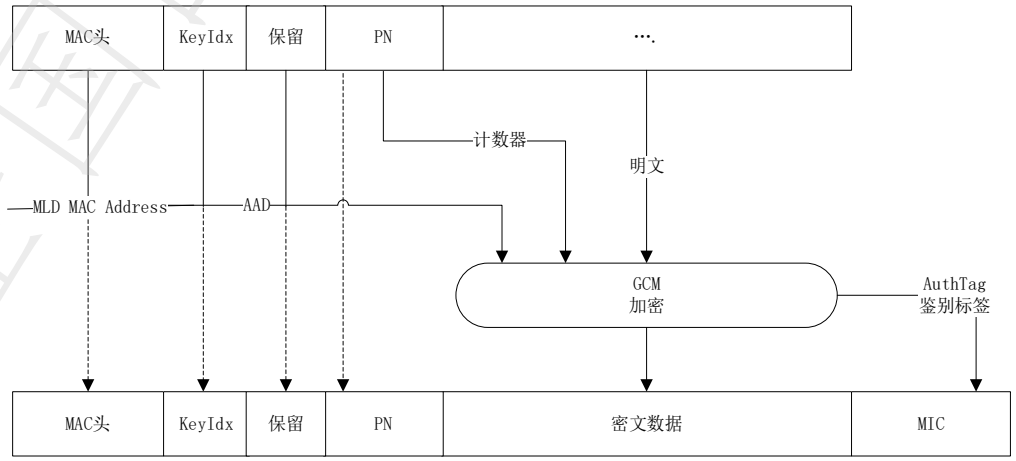

图23 WPI-SM4-GCM 封装与输入参数的映射关系

数据发送时，WPI-SM4-GCM使用以下规则对MPDU进行封装：

a） 增加 PN，每个 MPDU 都使用不相同的 PN；

注：重传时，重传 MPDU 的帧体内容不改变，在 MLO 模式下帧重传时 PN 值不变。

b） 使用 MPDU 头里的字段构造 GCM 使用的 AAD（Additional authenticated data）。GCM 算法提供了 AAD 里字段的完整性保护。如重传时 MPDU 头里某些字段发生改变，在构造 AAD 时将其屏蔽设置为 0，见 7.1；

c） 根据 PN 的低 96 位作为 IV 构造计数器；

d） 将新的 PN 和 Keyid 放在 WPI 头里；

e） GCM 加密处理过程使用 Key，AAD，计数器和 MPDU 数据生成密文和 MIC；

f） 原始的 MPDU 头，WPI 头和加密后的 MPDU 数据及 MIC 形成了加密 MPDU。

数据接收时，WPI-SM4-GCM的MPDU接收处理见图24。

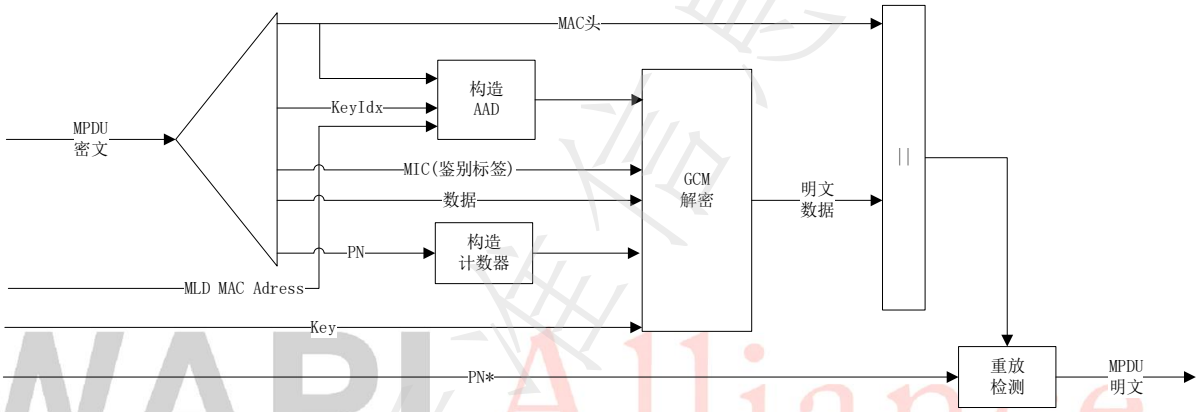

图24 WAPI-GCM-SM4 的 MPDU 接收处理

数据接收时，WPI-SM4-GCM解封装与输入参数的映射关系见图25。

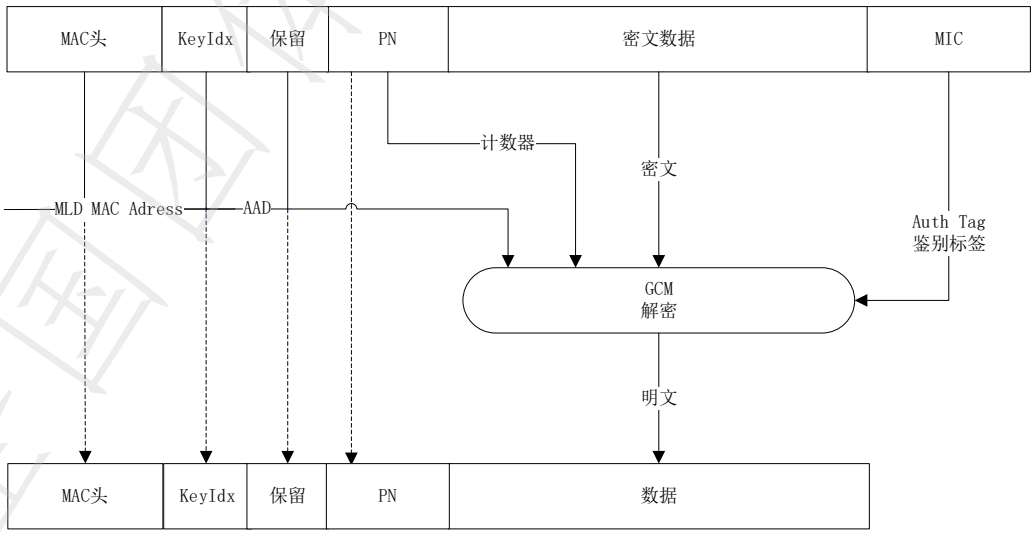

图25 WPI-SM4-GCM 解封装与输入参数的映射关系

数据接收时，WPI-SM4-GCM使用下面的规则解密MPDU密文数据，并对MPDU明文进行解封装：

1） 分解 MPDU 密文，构建 AAD 和计数器；

2） 通过 MPDU 密文的 MPDU 头形成 AAD，当 MPDU 是在 AP MLD 和与之相关联的 non-AP MLD 之间并通过附属的 AP 和 STA 传输的单播数据帧时，用发送方和接收方的 MLD MAC 地址构造 AAD（见 7.1）；

3） PN 字段低 96 位作为 IV 构建计数器；

4） MIC 被提取出来用于 GCM 完整性校验；

5） GCM 接收过程使用 Key，AAD，计数器，MIC 和 MPDU 密文数据这些参数进行处理，得出 MPDU 明文数据，同时也校验了 AAD 和 MPDU 明文数据的完整性；

6） MPDU 头和 MPDU 明文数据需要连接在一起形成一个明文 MPDU。

解密过程通过比较MPDU里的PN是不是要大于重放计数器来防止MPDU重放攻击。

7.3 WPI-SM4-OFB+CMAC 工作模式

OFB加密和CBC-MAC模式处理见图26。

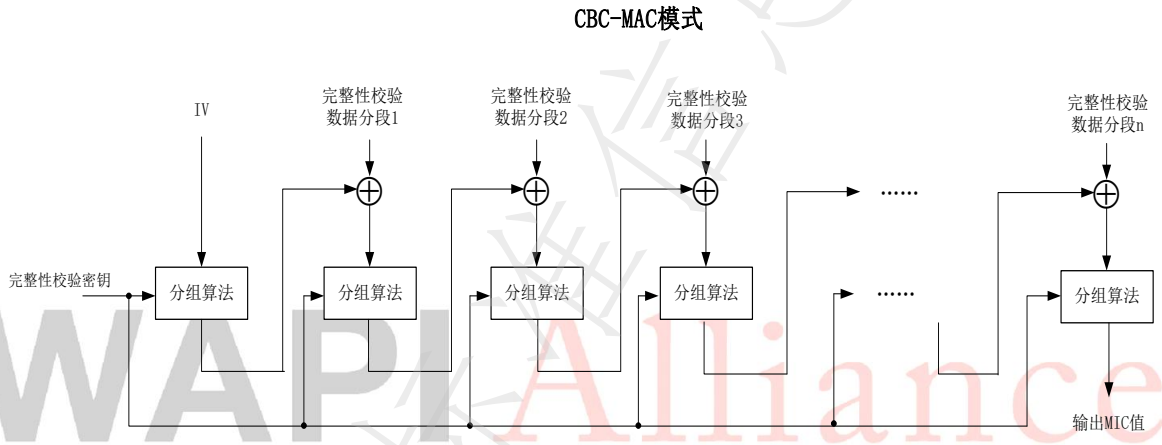

图26a CBC-MAC工作模式

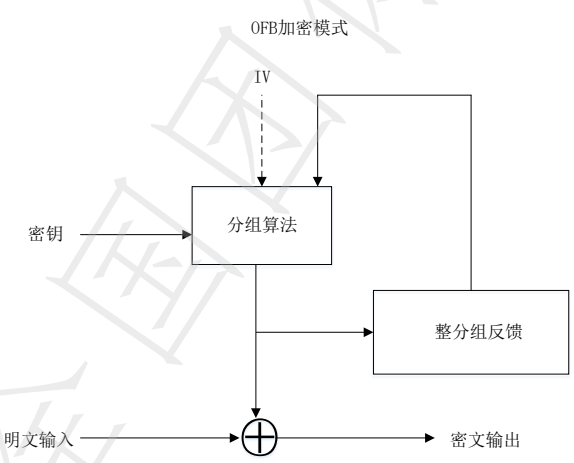

图 26b OFB 加密模式

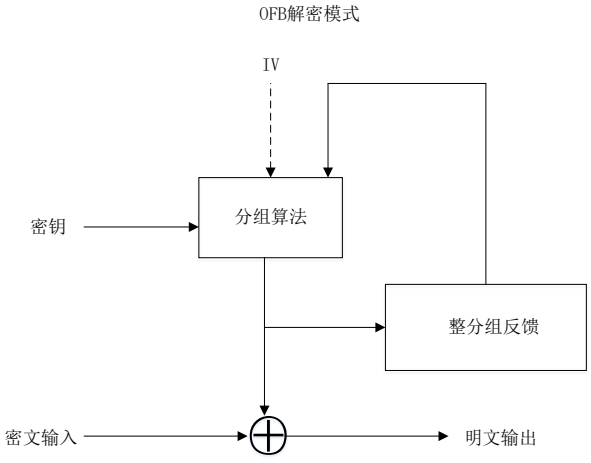

图 26c OFB 解密模式

图26 工作模式

注：本章图中涉及的工作模式、封装处理和发送接收处理可适用于不同密钥长度的密码算法。