



中 华 人 民 共 和 国 电 影 行 业 标 准

DY/T 2.3—2020

数字电影打包 第 3 部分：MXF 轨迹文件基本数据加密

Digital cinema (D-cinema) packaging — Part 3: MXF track file essence encryption

(ISO 26429-6:2008, Digital cinema (D-cinema) packaging – Part 6: MXF track
file essence encryption, MOD)

2020 – 09 – 22 发布

2020 – 09 – 30 实施

国家电影局 发布

目 次

| | |
|----------------------|----|
| 前言..... | V |
| 引言..... | VI |
| 1 范围..... | 1 |
| 2 规范性引用文件..... | 1 |
| 3 缩略语..... | 1 |
| 4 概述..... | 2 |
| 5 加密的基本数据容器..... | 3 |
| 6 加密框架..... | 3 |
| 6.1 概述..... | 3 |
| 6.2 加密框架键..... | 5 |
| 6.3 长度..... | 5 |
| 6.4 上下文 SR..... | 5 |
| 7 加密上下文..... | 5 |
| 7.1 概述..... | 5 |
| 7.2 加密上下文键..... | 7 |
| 7.3 长度..... | 7 |
| 7.4 上下文 ID..... | 7 |
| 7.5 源基本数据容器标签..... | 7 |
| 7.6 加密算法..... | 7 |
| 7.7 MIC 算法..... | 7 |
| 7.8 加密密钥 ID..... | 8 |
| 8 加密三元组..... | 8 |
| 8.1 概述..... | 8 |
| 8.2 加密三元组键..... | 9 |
| 8.3 长度..... | 9 |
| 8.4 加密上下文链接..... | 9 |
| 8.5 明文偏移量..... | 9 |
| 8.6 源键..... | 9 |
| 8.7 源长度..... | 9 |
| 8.8 加密源值..... | 10 |
| 8.9 轨迹文件 ID（可选）..... | 10 |
| 8.10 序列号（可选）..... | 10 |
| 8.11 MIC（可选）..... | 11 |
| 9 加密轨迹文件约束..... | 11 |

| | | |
|--------------|---|----|
| 9.1 | 概述..... | 11 |
| 9.2 | 加密基本数据轨迹..... | 11 |
| 9.3 | 加密框架 DM 轨迹..... | 11 |
| 9.4 | 索引表..... | 11 |
| 10 | 解密处理参考模型 | 12 |
| 10.1 | 概述..... | 12 |
| 10.2 | 总体流程..... | 12 |
| 10.3 | 模块..... | 13 |
| 10.3.1 | 概述..... | 13 |
| 10.3.2 | 加密过滤器模块..... | 13 |
| 10.3.3 | MIC 键推导模块 | 14 |
| 10.3.4 | 加密三元组完整性模块..... | 14 |
| 10.3.5 | 加密三元组解密模块..... | 15 |
| 10.3.6 | 索引表生成模块..... | 16 |
| 11 | 标签和键的结构 | 16 |
| 11.1 | 加密基本数据容器标签..... | 16 |
| 11.2 | 加密框架标签..... | 17 |
| 11.3 | 加密框架键..... | 17 |
| 11.4 | 加密上下文键..... | 18 |
| 11.5 | 加密三元组键..... | 18 |
| 11.6 | 128 位 AES-CBC 的 UL..... | 19 |
| 11.7 | 128 位 HMAC-SHA1 的 UL..... | 19 |
| 附录 A (资料性附录) | 本部分与 ISO 26429-6:2008 相比章条编号变化对照一览表 | 21 |
| 附录 B (资料性附录) | 安全属性..... | 23 |

前 言

《数字电影打包》标准已经或计划发布如下部分：

- GY/T 293.1—2015《数字电影打包 第1部分：声音和图像轨迹文件》；
- GY/T 293.2—2015《数字电影打包 第2部分：MXF JPEG2000应用》；
- DY/T 2.3—2020《数字电影打包 第3部分：MXF轨迹文件基本数据加密》；
- DY/T 2.4—2020《数字电影打包 第4部分：合成播放列表》；
- DY/T 2.5—2020《数字电影打包 第5部分：打包列表》；
- DY/T 2.6—2020《数字电影打包 第6部分：资产映射和文件分割》；
- DY/T 2.7—2020《数字电影打包 第7部分：立体图像轨迹文件》。

本部分是《数字电影打包》的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO 26429-6:2008《数字电影打包——第6部分：MXF轨迹文件基本数据加密》。

为符合GB/T 1.1—2009的编写规则，本部分与ISO 26429-6:2008相比在结构上有较多调整，附录A列出了本部分与ISO 26429-6:2008章条编号变化对照一览表。

本部分与ISO 26429-6:2009的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用等同采用国际标准的GY/T 293.1—2015代替SMPTE 429-3（见第1章）。

本部分做了以下编辑性修改：

——为与现有标准系列保持一致，将本部分名称改为《数字电影打包 第3部分：MXF轨迹文件基本数据加密》；

——增加了附录A（资料性附录）“本部分与ISO 26429-6:2008相比章条编号变化对照一览表”。

本部分由国家电影局提出并归口。

本部分起草单位：北京电影学院、中国电影科学技术研究所。

本部分主要起草人：刘戈三、张鑫、刘茂英、王萃、王木旺、李铭。

引 言

本文件的发布机构提请注意，声明符合本文件时，可能涉及到相关专利使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向国际标准化组织（ISO）保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在国际标准化组织（ISO）备案。相关信息可通过以下联系方式获得：

专利持有人姓名：Eastman Kodak Company Intellectual Property Transactions

地址：343 State Street, Rochester, NY 14650, USA

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

数字电影打包 第3部分：MXF 轨迹文件基本数据加密

1 范围

《数字电影打包》标准的本部分规定了对符合GY/T 293.1—2015的数字电影非交织MXF帧封装轨迹文件进行加密的语法，和一种与之匹配的参考解密模型。这种语法采用AES密码算法对基本数据进行加密，并根据需要使用HMAC-SHA1算法对基本数据的完整性进行校验。

本部分假定解密和验证加密轨迹文件完整性所需的密钥会按需提供，不规定在数字电影发行和放映环境中密钥和密钥使用权限的管理方式，不涉及使用水印、指纹或其他安全技术来提供额外保护，未定义一种通用的MXF加密框架。

本部分适用于数字电影打包。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GY/T 293.1—2015 数字电影打包 第1部分：声音和图像轨迹文件（ISO 26429-3:2008，IDT）

SMPTE 336M-2001 电视—KLV 数据编码协议（SMPTE 336M-2001, Television — Data Encoding Protocol Using Key-Length-Value）

SMPTE 377M-2004 电视—素材交换格式（MXF）—文件格式规范（SMPTE 377M-2004, Television — Material Exchange Format (MXF) — File Format Specification）

IETF 2898 PKCS #5: 基于口令的加密技术规范（2.0版）（IETF 2898 (September 2000). PKCS #5: Password-Based Cryptography Specification -Version 2.0）

IETF 2104 HMAC: 散列消息认证码（IETF 2104 (February 1997). HMAC: Keyed-Hashing for Message Authentication）

SP 800-38A 美国国家标准与技术研究所 对分块密码模式操作方法和技术的建议（National Institute of Standards and Technology (December 1, 2001). Recommendation for Block Cipher Modes of Operation Methods and Techniques (SP 800-38A)）

FIPS 197 美国国家标准与技术研究所 高级加密标准(AES)（National Institute of Standards and Technology, FIPS 197 (November 26, 2001). Advanced Encryption Standard (AES)）

FIPS PUB 186-2 美国国家标准与技术研究所（+《修改通知单1》）数字签名标准(DSS)（National Institute of Standards and Technology, FIPS PUB 186-2 (+Change Notice 1) (January 27, 2000). Digital Signature Standard (DSS)）

3 缩略语

下列缩略语适用于本文件。

AES: 高级加密标准（Advanced Encryption Standard）

CBC: 密码块链接（Cipher Block Chaining）

DM: 描述性元数据 (Descriptive Metadata)
 EG: 工程指南 (Engineering Guideline)
 HMAC: 散列消息认证码 (Hash-based Message Authentication Code)
 ID: 标识符 (Identifier)
 IV: 初始化向量 (Initialization Vector)
 KLV: 键-长度-值 (Key Length Value)
 MIC: 消息完整性代码 (Message Authentication Code)
 MXF: 素材交换格式 (Material Exchange Format)
 NIST: 美国国家标准与技术研究院 (National Institute of Standards and Technology)
 OP-ATOM: 原子操作模式 (Operational Pattern Atom)
 SHA: 安全散列算法 (Secure Hash Algorithm)
 SMPTE: 电影和电视工程师协会 (The Society of Motion Picture and Television Engineers)
 SR: 强引用 (Strong Reference)
 UL: 通用标签 (Universal Label)
 UUID: 通用唯一标识符 (Universally Unique Identifier)

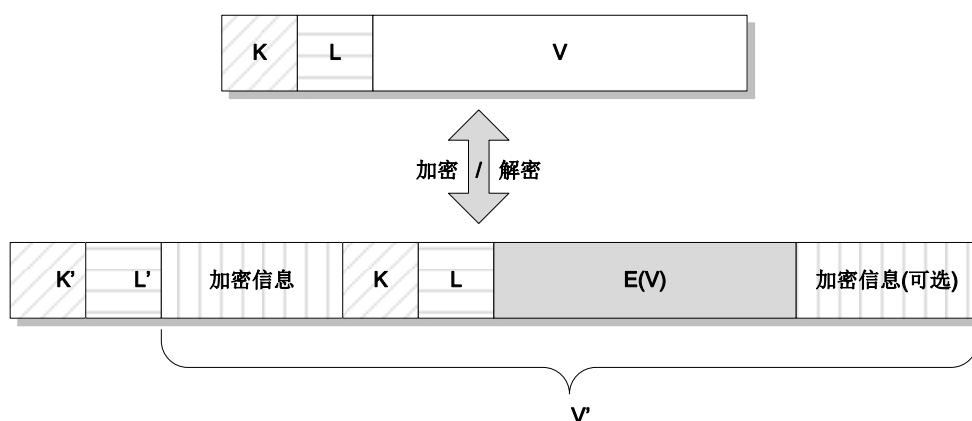
4 概述

本部分定义了采用 AES 密码算法 CBC 模式对数字电影轨迹文件中所包含的基本数据敏感信息进行加密, 其中 CBC 模式遵照 NIST SP 800-38A 中的定义。本部分也允许使用 HMAC-SHA1 算法作为选项, 对基本数据的完整性进行验证。更确切地说, 本部分允许使用单一的加密密钥, 对任意包含在明文轨迹文件中的轨迹进行加密。得到的加密轨迹文件与明文轨迹文件极其相似, 而明文轨迹文件本身是 MXF OP-ATOM 的一个受限版本¹⁾。其差别表现在以下三个方面:

a) 与明文轨迹关联的基本数据容器标签被替换为加密基本数据容器标签。替换标签表明存在加密基本数据, 并且如 SMPTE EG41 所描述, 允许任何接收基本数据的 MXF 应用程序因无法执行解密而直接失败退出。第 5 章定义了加密的基本数据容器。

b) 将与加密轨迹相关的密码信息以整体形式插入到 MXF 头部元数据中, 作为加密框架。加密框架包含一个用于加密基本数据轨迹的单个密钥的链接, 列出处理加密的基本数据所需的算法, 并包含原始的基本数据容器标签。后者使得具体应用程序不需要进一步处理就可以确定明文基本数据的特性。第 6 章定义了加密框架。

1) 本部分假定读者已经熟悉 MXF 格式和轨迹文件格式。



注：灰色区域表示加密三元组的密文部分，其他部分留作明文。只对源三元组的值项做了加密，并允许在封装前对基本数据信息进行加密。与每个加密三元组关联的密码信息的描述见第8章。

图1 源三元组与加密三元组的对应关系

c) 包含基本数据信息的明文三元组被加密三元组所取代——有关 KLV 编码的细节，见 SMPTE 336M。每个加密的三元组都可独立处理，因此允许从加密轨迹文件中任意位置开始解密。图 1 说明了明文三元组与加密三元组之间的对应关系²⁾。源明文 KLV 三元组的 V 值首先被加密产生 $E(V)$ 。加密的值 $E(V)$ 随同 K 和 L 一起封装在一个 $K' L' V'$ 加密三元组中。 K' 是所有加密三元组通用的唯一标签，与其内容无关。 L' 指 V' 的总长度。 V' 由来自源三元组的 K 、 L 和 $E(V)$ 以及与本加密三元组相关的特定加密信息所组成。该密码信息包括生成 $E(V)$ 时使用的初始化向量和用于验证三元组完整性的 MIC 等信息。加密三元组的结构在第 8 章有详细说明。

5 加密的基本数据容器

为了标识加密轨迹的存在，含有加密三元组的任意轨迹的基本数据容器标签都应该用表 1 中所示的加密的基本数据容器标签来代替。在序集 (Preface set) 和分区包 (Partition Pack) 中的基本数据容器标签均应替换，但文件描述符 (File Descriptor, SMPTE 377M) 中的基本数据容器标签应保持不变，以便识别底层的明文基本数据。

表1 加密的基本数据容器标签

(标签的完整结构，见第 11.1)

| |
|-------------------------------------|
| 060e2b34 04010107 0d010301 020b0100 |
|-------------------------------------|

6 加密框架

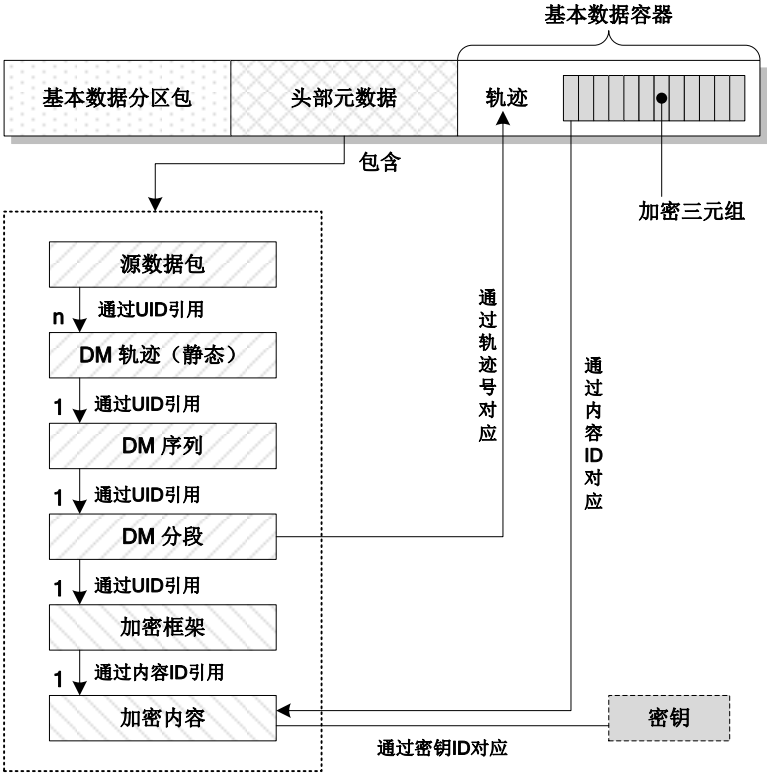
6.1 概述

如图 2 所示，加密上下文应作为一个 MXF 的 DM 框架，存在于加密的轨迹文件中³⁾。具体地说，轨迹

2) 本部分不要求为了加密基本数据而将其先封装在一个 KLV 三元组中。换言之，基本数据可先加密，然后再封装在加密的三元组内。

3) DM 框架是根据 SMPTE 377M 的插件机制定义的，且遵循 SMPTE EG 42 中描述的原则。

文件可包含一个或多个描述性元数据轨迹，每个描述性元数据轨迹各自包含一个加密框架⁴⁾。加密框架结构详见表 3。



注：DM轨迹是静态的，因为在加密轨迹中，任一给定轨迹关联单一的密钥。轨迹中的每个加密三元组必须引用相同的加密上下文。

图2 加密框架

加密框架形成一个 DM 加密结构。表 2 所列的加密框架标签应作为加密 DM 的标识符，包含在序集中。

表2 加密框架标签

（有关标签的完整结构，见第 11.2）

| |
|-------------------------------------|
| 060e2b34 04010107 0d010401 02010100 |
|-------------------------------------|

加密框架不包含实际的加密信息，而只是包含指向一个加密上下文的引用（在第 7 章中定义了加密上下文）。其目的是能与其他 MXF 描述性元数据兼容，从而允许加密上下文以一致的方式展现。

表 3 定义了加密框架集中所包含的各项。除了 InstanceID 和 GenerationUID 的定义已在 SMPTE 377M 中给出以外，描述符的所有局部标签均应按 SMPTE 377M 的 8.2.2（局部标签）的定义，动态地进行分配。局部标签向其完整 UL 的转换，可通过 SMPTE 377M 的 8.2（初始包）中定义的初始包机制来实现。

4) （资料性脚注）加密框架被规定为抽象的 DM 框架基类的一个子类（见 SMPTE 380M）。

表3 加密框架集

| 项目名称 | 类型 | 长度 (字节) | 通用标签 (UL) | 是否必备 | 含义 |
|---|---------------|------------|--|------|---------------------|
| 加密框架键 (Cryptographic Framework Key) | 集键 | 16 | 060e2b34 02530101 0d010401 02010000 | 必备 | 定义加密框架集 |
| 长度 (Length) | BER 长度 | 可变 | 不适用 | 必备 | 集长度 |
| 实例 ID (InstanceID) | UUID | 16 | 060e2b34 01010101 01011502 00000000 | 必备 | 框架的唯一标识符 |
| 生成 ID (GenerationUID) | UUID | 16 | 060e2b34 01010102 05200701 08000000 | 可选 | 可选的生成标识符 |
| 上下文 SR (Context SR) | 强引用 (描述性集) | 16 | 060e2b34 01010109 06010104 020d0000 | 必备 | 对加密上下文的强引用 (见第 7 章) |

6.2 加密框架键

本部分中，加密框架键(Cryptographic Framework Key) (见表 4) 唯一地标识加密框架。

表4 加密框架键

(键的完整结构见 11.3)

| |
|-------------------------------------|
| 060e2b34 02530101 0d010401 02010000 |
|-------------------------------------|

6.3 长度

长度 (Length) 指定加密框架的长度，根据 SMPTE 336M 使用基本编码规则 (BER) 编码。

6.4 上下文 SR

上下文 SR (Context SR) 包含一个与加密框架相关联的加密上下文的强引用。

7 加密上下文

7.1 概述

加密上下文（Cryptographic Context）集⁵⁾包含适用于整个加密基本数据轨迹的加密信息。表 5 定义了加密上下文集中所包含的各项。除了 InstanceID 和 GenerationUID 的定义已在 SMPTE 377M 中给出以外，其他所有描述符的局部标签均应按 SMPTE 377M 的 8.2.2（局部标签）的定义，动态地进行分配。局部标签值向其完整 UL 的转换，可通过 SMPTE 377M 的 8.2（初始包）中定义的初始包机制来实现。

表5 加密上下文集

| 项目名称 | 类型 | 长度 （字节） | 通用标签 UL | 是否必备 | 含义 |
|--|--------|------------|--|------|----------------------------------|
| 加密上下文键 （Cryptographic Framework Key） | 集键 | 16 | 060e2b34 02530101 0d010401 02010000 | 必备 | 定义加密上下文集 |
| 长度 （Length） | BER 长度 | 可变 | 不适用 | 必备 | 集长度 |
| 实例 ID （InstanceID） | UUID | 16 | 060e2b34 01010101 01011502 00000000 | 必备 | 上下文的唯一标识符，加密 框架使用它来引用此上下 文 |
| 生成 ID （GenerationUID） | UUID | 16 | 060e2b34 01010102 05200701 08000000 | 可选 | 可选的生成标识符 |
| 上下文 ID （Context ID） | UUID | 16 | 060e2b34 01010109 01010511 00000000 | 必备 | 加密三元组引用上下文所 用的唯一标识符 |
| 源基本数据容器标签 （Source Essence Container Lable） | UL | 16 | 060e2b34 01010109 06010102 02000000 | 必备 | 加密前，源基本数据的基本 数据容器标签 |
| 加密算法 （Cipher Algorithm） | UL 或 0 | 16 | 060e2b34 01010109 02090301 01000000 | 必备 | 三元组加密算法（如果有） |

5) （资料性脚注）加密上下文是 InterchangeObject 的一个子类（见 SMPTE 380M 的附录 C）。

| | | | | | |
|-------------------------------------|--------|----|--|----|-------------------|
| MIC 算法 (MIC Algorithm) | UL 或 0 | 16 | 060e2b34 01010109 02090302 01000000 | 必备 | 三元组完整性算法 (如果有) |
| 加密密钥ID (Cryptographic Key ID) | UUID | 16 | 060e2b34 01010109 02090301 02000000 | 必备 | 密钥唯一标识符 |

7.2 加密上下文键

在本部分中，加密上下文键 (Cryptographic Framework Key) (见表 6) 唯一地标识加密上下文。

表6 加密上下文键

(键的完整结构见 11.4)

| |
|-------------------------------------|
| 060e2b34 02530101 0d010401 02020000 |
|-------------------------------------|

7.3 长度

长度 (Length) 项指定加密上下文值的长度，根据 SMPTE 336M 使用基本编码规则 (BER) 编码。

7.4 上下文 ID

上下文 ID (Context ID) 项唯一标识这里特定的加密上下文。上下文 ID 用一个 UUID 来代表，其值由加密三元组引用。

7.5 源基本数据容器标签

源基本数据容器标签 (Source Essence Container Label) 项包含加密三元组从属的基本数据容器的原始标签。以便于确定加密容器内所包含的基本数据类型。

7.6 加密算法

加密算法 (Cipher Algorithm) ID 项标识用于加密与加密上下文相关联的加密三元组所用的算法和模式。它应包含表 7 所列值中的一个。

表7 加密算法

| 描述 | 值 |
|---------------|-------------------------------------|
| 不使用加密算法 | 00000000 00000000 00000000 00000000 |
| 128 位 AES-CBC | 060e2b34 04010107 02090201 01000000 |

表 7 的第 1 行是一个特殊值，该值应该用来指明处理与加密上下文相关的加密三元组时，无需加密算法。第 2 行标识了加密算法的唯一允许值 — 11.6 定义了该标签的完整结构。

7.7 MIC 算法

MIC 算法 (MIC Algorithm) ID 项标识计算与加密上下文相关联的加密三元组的消息完整性代码 (可选) 所使用的算法。它应包括表 8 所列值中的一个。

表8 消息完整性编码算法

| 描述 | 值 |
|-----------------|-------------------------------------|
| 不使用 MIC 算法 | 00000000 00000000 00000000 00000000 |
| 128 位 HMAC-SHA1 | 060e2b34 04010107 02090202 01000000 |

表 8 的第 1 行是一个特殊值，在处理加密上下文关联的加密三元组时，应使用该值来指明无需使用 MIC 算法。第 2 行用来标识 MIC 算法的唯一允许值——11.7 定义了该标签的完整结构。

7.8 加密密钥 ID

加密密钥 ID (Cryptographic Key ID) 项唯一标识加密密钥，该密钥用作加密三元组时加密算法和消息认证代码算法的输入。加密密钥 ID 应使用 UUID 来编码。关于其使用方法的描述，见 10.2。

8 加密三元组

8.1 概述

加密三元组可变长度包 (如表 9 所示) 包含了加密数据和三元组特定的加密信息。作为可变长度包，值域中的每一项都包含一个长度域和该域的值。同 SMPTE 336M 一致，键的第 6 个字节 (04h) 表示每一项的长度域是以 BER 短格式或者长格式进行编码的。包中的所有项都是必备的。任何标明“可选”的项表示不存在“长度-值”中的值，因此长度为零。

表9 加密三元组可变长度包

| 项目名称 | 类型 | 长度 (字节) | 通用标签 (UL) | 是否必备 | 含义 |
|---|--------|------------|--|------|---------------------------|
| 加密三元组键 (Encrypted Triplet Key) | 包键 | 16 | 060e2b34 02040101 0d010301 027e0100 | 必备 | 标识加密三元组可变长度包 |
| 长度 (Length) | BER 长度 | 可变 | 不适用 | 必备 | 包长度 |
| 加密上下文链接 (Cryptographic Context Link) | UUID | 16 | 060e2b34 01010109 06010106 03000000 | 必备 | 与本三元组相关的加密上下文的链接 (见第 7 章) |
| 明文偏移量 (Plaintext Offset) | UInt64 | 8 | 060e2b34 01010109 06090201 03000000 | 必备 | 源明文数据中加密开始位置的偏移量 |
| 源键 (Source Key) | 键 | 16 | 060e2b34 01010109 06010102 03000000 | 必备 | 源三元组的键 |

表9 加密三元组可变长度包（续）

| 项目名称 | 类型 | 长度 (字节) | 通用标签 (UL) | 是否必备 | 含义 |
|----------------------------------|--------|------------|--|------|--------------------|
| 源长度 (Source Length) | UInt64 | 8 | 060e2b34 01010109 04061002 00000000 | 必备 | 源三元组值的长度 |
| 加密源值 (Encrypted Source Value) | 字节数组 | 可变 | 060e2b34 01010109 02090301 03000000 | 必备 | 始于源明文数据偏移量处的加密源值 |
| 轨迹文件 ID (TrackFile ID) | UUID | 16 | 060e2b34 01010109 06010106 02000000 | 可选 | 包含该三元组的 轨迹文件的标识 |
| 序列号 (Sequence Number) | UInt64 | 8 | 060e2b34 01010109 06100500 00000000 | 可选 | 轨迹文件内该三元组的 序列号 |
| MIC | 字节数组 | 20 | 060e2b34 01010109 02090302 02000000 | 可选 | 散列消息认证码 (HMAC) |

8.2 加密三元组键

在本部分中，加密三元组键 (Encrypted Triplet Key) (见表 10) 唯一地标识加密三元组。

表10 加密三元组键

(键的完整结构见 11.5)

| |
|-------------------------------------|
| 060e2b34 02040101 0d010301 027e0100 |
|-------------------------------------|

8.3 长度

长度 (Length) 项指定加密三元组的长度，根据 SMPTE 336M 使用基本编码规则 (BER) 编码。

8.4 加密上下文链接

加密上下文链接 (Cryptographic Context Link) 项是指向加密上下文的链接，定义了用于生成加密源值属性的加密信息。它包含一个 UUID，即目标加密上下文的 InstanceID。

8.5 明文偏移量

明文偏移量 (Plaintext Offset) 项应指定源值中加密起始第 1 个字节的偏移量 (以字节为单位)。明文偏移量应小于或等于源长度。如 9.3.4 所述，在处理加密轨迹文件时应处理此参数的任何合法值。

设置明文偏移量项是为了允许源值的头部保留一部分不加密。明文偏移量适宜的取值可能取决于加密轨迹文件中所含基本数据的类型，因此超出本部分的范围。

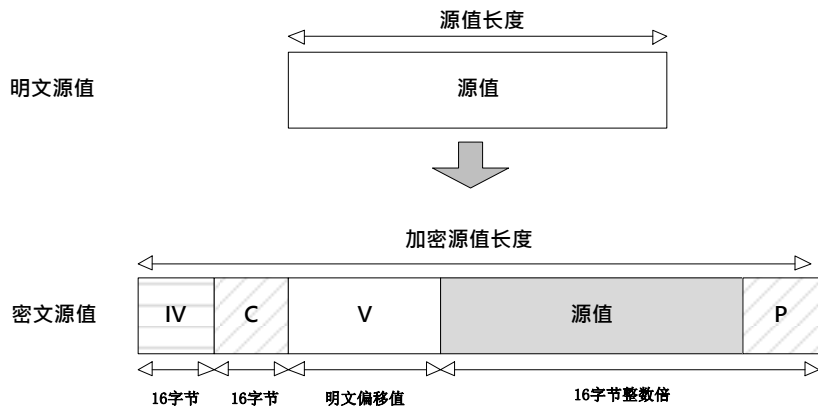
8.6 源键

源键（Source Key）项包含源明文三元组未加修改的键。注意：该键指的是三元组的标识符，而非密钥。

8.7 源长度

源长度（Source Length）项包含的是按照 UInt64 整型编码的源明文三元组的长度。它应与长度项结合使用，以确定由加密过程填充的字节数。

8.8 加密源值



注：灰色区域为加密部分。初始化向量（IV）、校验值（C）和填充值（P）是加密源值项的组成部分，并不是加密三元组包中的独立项。加密源值对应图1所示加密三元组的阴影线部分。

图3 加密源值结构

如图 3 所示，加密源值（Encrypted Source Value）项包含源三元组的加密源值，并包括初始化向量、校验值和填充值。它分为明文和密文两部分。明文部分包含一个 16 字节的初始化向量（IV）和源值最前面（明文偏移量）的若干字节⁶⁾。密文部分包含一个 16 字节的校验值（C）和源值最后面（源长度—明文偏移量）的若干字节，随后是填充值（P）。后者的大小（填充长度）至少为 1 且为必选，以使得“源长度—明文偏移量+填充长度”是 16 字节的整数倍，16 字节是 AES-128 算法的块大小。填充字节应依据 IETF 2898 的 B.2.4 中描述的 16 字节块模式来设置。加密过程应使用与加密三元组相关联的加密上下文中的加密算法与加密密钥 ID 项中分别给出的算法和加密密钥。校验值应由表 11 中列出的 16 字节值组成，该值可用于验证是否使用了正确的加密密钥。换言之，加密三元组解密时，解密应用程序便可通过对比恢复的校验值与表 11 给出的值，来验证是否使用了正确的密钥。

表11 加密三元组校验值（以网络字节顺序表示的十六进制）

| |
|-------------------------------------|
| 4348554B 4348554B 4348554B 4348554B |
|-------------------------------------|

宜为每个加密三元组随机选择初始化向量。初始化向量不应基于容易预测的序列。

6) 关于加密初始化向量的其他细节见 Bruce Schneier 著《应用密码学（Applied Cryptography）》。

8.9 轨迹文件 ID（可选）

可选的轨迹文件ID（TrackFile ID）项唯一标识加密三元组所属的轨迹文件。只有当存在MIC项时，才应存在该项。该项为一个UUID，且在一个给定的轨迹文件中，所有的加密三元组都应有相同的轨迹文件ID取值。

注：该标识符的用法在GY/T 293.1-2015的“数据包ID”中进行了描述。SMPTE RP205给出了UMID的分配指南。

如果没有轨迹文件ID与加密三元组相关联，则轨迹文件ID项长度应为0。

8.10 序列号（可选）

可选的序列号（Sequence Number）项应包含一个整数，在一个给定的基本数据轨迹内，每个相继出现的加密三元组中的该项递增1。当且仅当MIC项存在，该项存在。给定的基本数据轨迹中的首个加密三元组的序列号宜为1。

如果没有序列号与加密三元组相关联，则序列号项的长度应为0。

8.11 MIC（可选）

可选的MIC项包含一个消息完整代码，该代码是用与该加密三元组相关的加密上下文的MIC算法和密钥ID项中所包含的MIC算法和密钥计算得出的。如果存在MIC项，轨迹文件ID项和序列号项也应存在。MIC算法应适用于起始于加密源值项首字节（即IV值的首字节）的MIC项之前的每个字节。轨迹文件ID的长度字段、序列号和MIC应包括在内。

MIC算法使用的密钥（MICKey），源于加密密钥ID所引用的密钥（CipherKey），是用FIPS 186-2的附录3.1和附录3.3定义的算法推导得出的。具体地说，依据附录3.1，以CipherKey为种子密钥XKEY，设 $XSEED_3 = 0$ ；且依据附录3.3构造函数 $G(t, c)$ ，则MICKey应等于 x_1 。此外，由于附录3.1被用作通用随机数生成器，根据《修改通知单1》中附录的“通用随机数生成”，步骤3.c中的“mod q”应省略。 x_0 应舍弃。

如果没有MIC与加密三元组相关联，则MIC项的长度应为0。

9 加密轨迹文件约束

9.1 概述

加密轨迹文件除应遵循SMPTE 429-3中对明文轨迹文件的规定外，还应附加以下的约束。

9.2 加密基本数据轨迹

应该用单一的密钥以及加密上下文来加密任意给定的基本数据轨迹。换言之，与给定加密轨迹关联的所有加密三元组均应引用同样的加密上下文。

9.3 加密框架DM轨迹

MXF文件包中的轨迹文件可以包含一个或多个描述轨迹文件的DM轨迹。由于是使用同样的密钥来加密给定的加密基本数据轨迹中所有的加密三元组，加密框架DM轨迹（Cryptographic Framework DM Track）应是静态DM轨迹，见SMPTE 377M的“通用数据包规范”。

每个加密框架DM轨迹应包含一个DM序列，此DM序列由一个DM段（DMSegment）组成，参见SMPTE 377M的附录“通用数据包规范”。DM段应包含对加密框架的强引用。

加密框架DM轨迹与基本数据轨迹之间的链接，应通过使用DM轨迹中所含的DM段的TrackID属性来生成。大多数情况下，文件只包含一个单独的基本数据轨迹，因此，TrackID可安全地省略掉。如果

应用软件要求单独加密的轨迹、元数据或基本数据要有单独的加密上下文，则应指定 TrackID。

9.4 索引表

在明文轨迹文件中，索引表（Index Tables）每个条目定位一个含有单帧基本数据的三元组。同样地，在加密轨迹文件中，索引表每个条目应指向封装一个三元组的加密三元组，它本身包含一个基本数据帧。

注：由于加密的轨迹文件索引表和明文的轨迹文件索引表指向不同的数据流，所以，其内容可能有所不同。可以按照 SMPTE 377M 规定使用 KLV 填充包，来支持任何 KAG 要求和（或）填充基本数据容器的每一帧，以便允许在加密的表达与明文表达中有相同的索引表，或使用一个非零 EditUnitByteCount 值的索引表（见 SMPTE 377M 的索引表部分）。

10 解密处理参考模型

10.1 概述

本章为加密的轨迹文件规定了完整的解密处理模型。更具体地说，规定了一种将有效的加密文件映射为有效的明文轨迹文件的参考方法。然而，本章没有规定随后的操作，比如呈现基本数据。

全面规定解密模型的目的是顺应对加密过程正式规范化和便于符合性测试的需求。高级视频编码（MPEG-4 第 10 部分和 H. 264）视频压缩标准所采用的精确匹配方法就是以这种概念建模，为兼容解码处理的输出端定义了单一的正确比特模式。解密模型本身并不强制要求输出是一个有效的轨迹文件。生成输入文件是加密轨迹文件创建者的责任，而解密的时候，有效的输入文件将导致一个有效的明文轨迹文件（假设可以获得所有相关的密钥）。除遵循本部分其他规定外，加密的轨迹文件必须满足这一要求，才被认为有效。

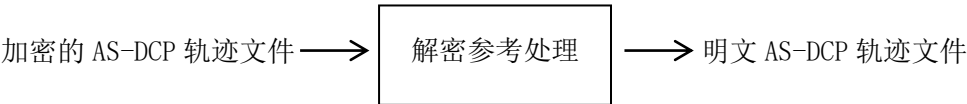


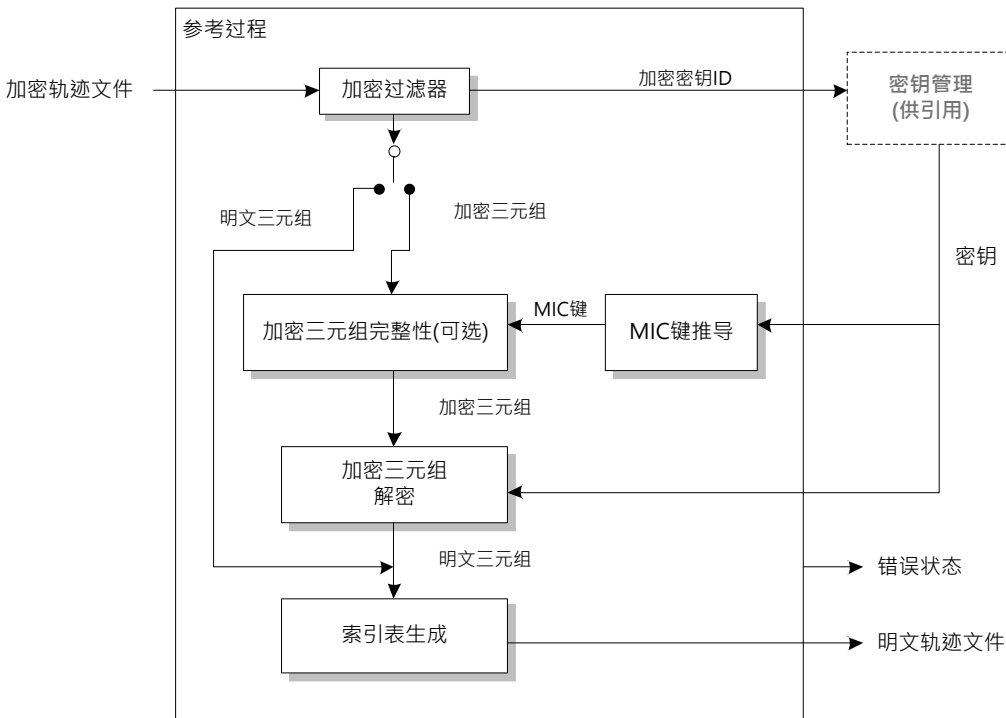
图4 解密参考模型

如果输入文件不是有效的加密轨迹文件，解密过程有可能在一个不可恢复的错误上终止。实际上，即使输入有效加密轨迹文件，没有正确的解密密钥将会中断解密过程并导致一个错误状态。解密模型将报告遇到的错误，但这种情况下的应对措施由应用决定。

10.2 总体流程

本条描述解密模型中的整个信息流程。解密模型分为使用特定的输入和输出来执行一些特定功能的几个模块。这些模块中部分是弱耦合的，可以适应不同的算法或者是本部分范围以外的一些特殊用途的需求。

在图 5 中，加密密钥 ID 提供给密钥管理模块，而它的值用来标识解密三元组所需要的密钥。密钥管理模块的定义超出了本部分的范围。



注：密钥管理模块不属于本部分的范围，上图仅供参考。

图5 解密处理流程图

10.3 模块

10.3.1 概述

参考处理模型包含多个模块，每个都有特定的接口。本章详细描述这些模块。

10.3.2 加密过滤器模块

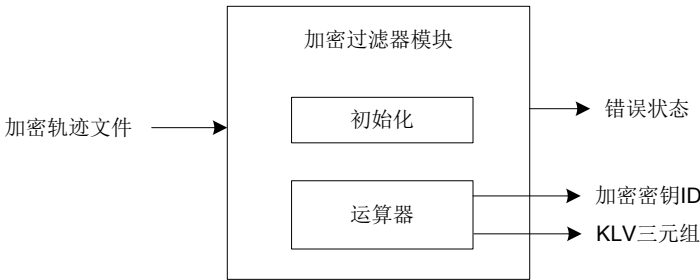


图6 加密过滤器模块

加密过滤器模块在概念上分两个阶段运行，即初始化阶段和操作阶段。在初始化阶段，从加密轨迹文件中提取加密上下文并留存在模块中。在操作阶段，模块应根据如下的规则来处理加密轨迹文件：

- 除非另有规定，每个包含在加密轨迹文件中的 KLV 三元组应保持未经修改；
- 包含一个加密框架和相应头部元数据的 DM 轨迹应予以丢弃；
- 每个与加密基本数据容器相关的索引表应予以丢弃，由索引表生成模块重新创建索引表；

- 任何包含加密三元组的轨迹及基本数据容器标签应替换为存储在相应加密上下文中的原始基本数据容器标签；
- 每个加密三元组应依据图 5 中的流程图来解密。模块应输出每个未经改变的加密三元组。它还应该输出在加密上下文集中的加密密钥 ID，加密上下文集由加密三元组的加密上下文链接元素引用。如果加密上下文链接元素不匹配，解析失败并应返回一个错误状态。

加密过滤器是参考处理模型仅有的两个模块中的一个，它将一个状态从一个三元组留存到另一个三元组（另一个是索引表生成器）。

10.3.3 MIC 键推导模块

如果可选的 MIC 项存在于加密三元组中，MIC 键推导模块应该用于准备一个密钥，供加密三元组完整性模块使用。如图 7 所示，该模块接收密钥作为输入，并以 MIC 键作为输出。



图7 MIC 键推导模块

输出键（MIC Key）应从输入密钥（CipherKey）推导出来，使用 8.11 中规定的算法。

10.3.4 加密三元组完整性模块

如果加密三元组存在可选的 MIC 项，则可使用加密三元组完整性模块来验证加密三元组中加密源值和 MIC 项的完整性。如图 8 所示，它取一个加密三元组和密钥作为输入，并生成同样的加密三元组和一个错误状态码作为输出。后者的值表明完整性检查是否成功。模块在连续的加密三元组之间不携带状态信息，亦即是无记忆的。

注：MIC 的元素可如同附录 B 中注释的那样，用来检测复制的、丢失的或更改了顺序的加密三元组。然而，该功能不包括在参考处理模型中。

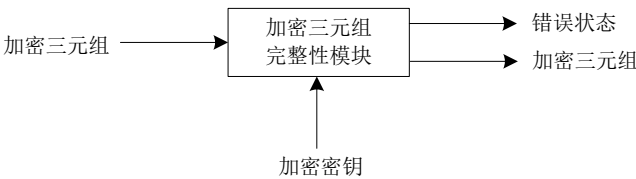


图8 加密三元组完整性模块

模块应使用 7.8 中规定的唯一算法即 HMAC-SHA1 算法来运行。

给定一个输入的加密三元组，模块应依据下述法则来创建输出的加密三元组和错误状态：

- 输出的加密三元组应与输入的加密三元组相同；
- 如果输入的三元组不是加密的（即 K 项不是表 10 中的加密三元组键），或者如果不存在可选的 MIC 项，则不应做其他处理。如果输入的三元组是加密的，且存在 MIC 项，则应遵循下面的法则；
- 使用输入的密钥，该 HMAC-SHA1 算法应该应用于从加密源值项的第 1 个字节开始的所有先于 MIC 项的字节。该计算的结果与加密三元组的 MIC 项相比较。如果两者不同，完整性检查即告失败，并应返回一个错误状态。

10.3.5 加密三元组解密模块

核心解密操作发生在加密三元组解密模块中，比如执行一个 AES 块解密。如图 9 所示，加密三元组解密模块以一个加密三元组和加密密钥为输入，并以产生一个三元组和一个错误状态码作为输出。模块不携带从一个 KLV 三元组到下一个 KLV 三元组的状态信息，亦即是无记忆的。

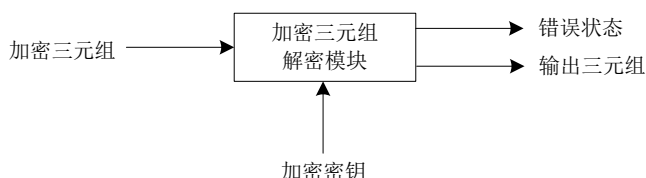


图9 加密三元组解密模块

该模块应使用 7.6 中规定的唯一算法来操作执行，即 AES-128 CBC 模式来运行（NIST 的 SP 800-38A 和 FIPS 197）。给定一个输入的加密三元组，如图 10 所示，模块应依据下面的法则来创建输出的 KLV 三元组。

- 如果输入的三元组未加密（即 K 项不是表 10 的加密三元组键），输出的三元组应等于输入的三元组，且不应发生其他的处理。如果输入的三元组是加密的，应遵循以下法则；
- 输出的 K 项应等于输入的加密三元组的源键值项；
- 输出的 L 项应等于输入的加密三元组的源长度项；
- 如果明文偏移量等于输出 L 项（即基本数据没有密文部分），则应忽略加密源值项的头 32 个字节，并将随后的 L 字节复制到输出的 V 项，且不应做其他的处理。如果明文偏移量不等于 L，则应采取下述步骤；
- 在输入的加密三元组中找到的加密源值项的头 16 个字节（按网络中的字节顺序）应作为 CBC 模式使用的初始化向量来使用；
- 加密源值项接下来的 16 个字节应依据 AES-128 CBC 模式来处理。16 字节输出块应等于表 11 的校验值；如不等于，则应返回一个错误状态，且不应输出三元组；
- 加密源值项接下来的（明文偏移量）字节应不加改动地复制到输出的 V 项的开头，即作为明文信息。如果（明文偏移量）大于输出 L，则应返回一个错误状态，且不应输出三元组；
- 加密源值输入段的剩余长度必须是 16 字节（AES-128 的块大小）的倍数。如果不是，则应返回一个错误状态，且不应输出三元组；
- 随后的各组 16 字节应作为密码块，依据 AES-128 CBC 模式，使用加密密钥来处理。
- 该过程生成的最前面的（L-明文偏移量）字节应复制到输出的 V 项。如果没有足够的密码块来生成 L-明文偏移字节，则应返回一个错误状态，且不应输出三元组。该步骤去除了加密期间为保证 AES 输入为 16 字节的整数倍长度而添加的密码填充。注意：填充字节的值是规定的，但不做校验。

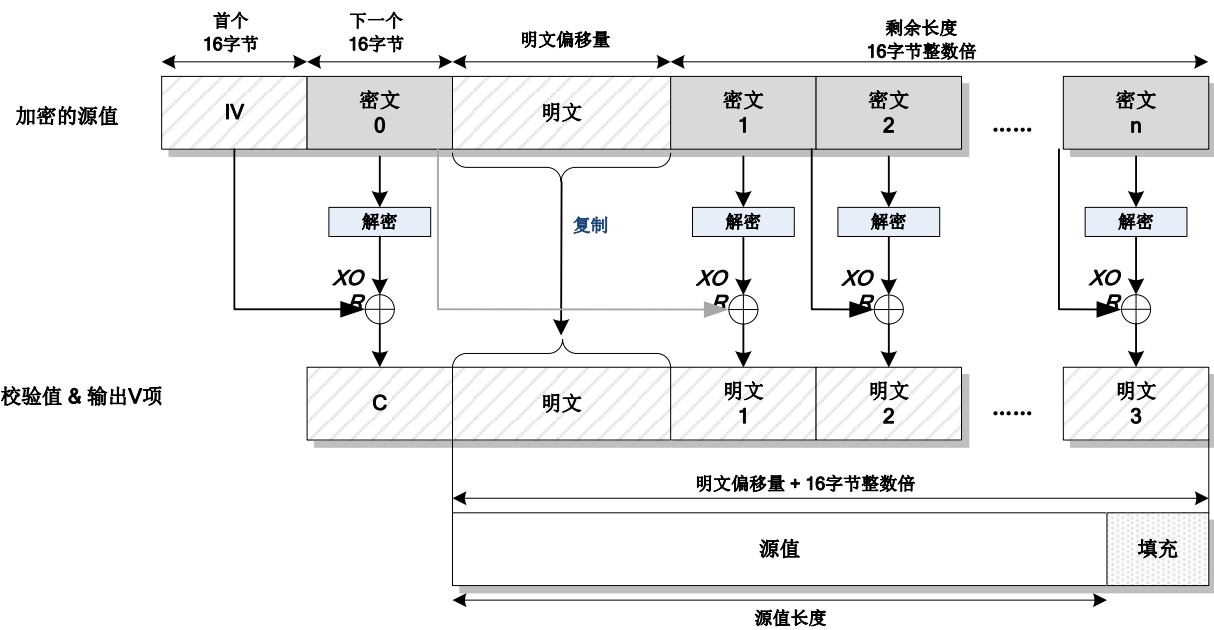


图10 加密三元组解密过程

10.3.6 索引表生成模块

索引表生成模块在概念上分为两个阶段，即操作阶段和后操作阶段。在操作阶段，明文三元组应该在位置信息被提取出来的同时不加修改的通过。在后操作阶段，模块输出一个 9.4 中规定的索引表。

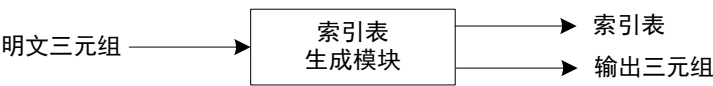


图11 索引表生成模块

11 标签和键的结构

11.1 加密基本数据容器标签

表12 加密基本数据容器标签

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|------|---------|---------|--------------|
| 1 | 目标标识符 | 06h | |
| 2 | 标签大小 | 0Eh | |
| 3 | 指示符 | 2Bh | ISO、ORG |
| 4 | 指示符 | 34h | SMPTE |
| 5 | 注册类别指示符 | 04h | 标签 |
| 6 | 注册指示符 | 01h | 标签注册 |
| 7 | 结构指示符 | 01h | 标签结构 |
| 8 | 版本号 | 07h | 该标签在注册时的注册版本 |

表12 加密基本数据容器标签（续）

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|---|----------|---------|-----------|
| 9 | 项指示符 | 0Dh | 机构注册 |
| 10 | 机构 | 01h | AAF 协会 |
| 11 | 应用 | 03h | 基本数据容器 |
| 12 | 结构版本 | 01h | 版本 1 |
| 13 | 基本数据容器种类 | 02h | MXF 通用容器 |
| 14 | 映射种类 | 0Bh | 加密的基本数据容器 |
| 15 | 局部定义 | 01h | 帧封装 |
| 16 | 保留 | 00h | |
| 注：本标签的字节 1~12 由基本数据容器标签来定义（SMPTE 379M）。 | | | |

11.2 加密框架标签

表13 加密框架标签

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|---|---------|---------|------------------|
| 1 | 目标标识符 | 06h | |
| 2 | 标签大小 | 0Eh | |
| 3 | 指示符 | 2Bh | ISO、ORG |
| 4 | 指示符 | 34h | SMPTE |
| 5 | 注册类别指示符 | 04h | 标签 |
| 6 | 注册指示符 | 01h | 标签注册 |
| 7 | 结构指示符 | 01h | 标签结构 |
| 8 | 版本号 | 07h | 该标签在注册时的注册版本 |
| 9 | 项指示符 | 0Dh | 机构注册 |
| 10 | 机构 | 01h | AAF 协会 |
| 11 | 应用 | 04h | MXF/AAF 兼容的元数据标签 |
| 12 | 结构版本 | 01h | 版本 1 |
| 13 | 方案种类 | 02h | 加密 DM 方案 |
| 14 | 方案指示符 | 01h | 加密方案版本 1 |
| 15 | 方案指示符 | 01h | 加密的轨迹文件加密框架 |
| 16 | 保留 | 00h | |
| 注：本标签的字节 1~12 是为 MXF 描述性元数据方案定义的（377M）。 | | | |

11.3 加密框架键

表14 加密框架键

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|------|-------|---------|----|
| 1 | 目标标识符 | 06h | |
| 2 | 标签大小 | 0Eh | |

表14 加密框架键（续）

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|----------------------------------|---------|---------|---------------------------|
| 3 | 指示符 | 2Bh | ISO、ORG |
| 4 | 指示符 | 34h | SMPTE |
| 5 | 注册类别指示符 | 02h | 组（集与包） |
| 6 | 注册指示符 | 53h | 局部集，2个8位字节长度字段，2个8位字节标记字段 |
| 7 | 结构指示符 | 01h | 集/包字典 |
| 8 | 版本号 | 01h | 该标签在注册时的注册版本 |
| 9 | 项指示符 | 0Dh | 机构注册 |
| 10 | 机构 | 01h | AAF 协会 |
| 11 | 应用 | 04h | MXF/AAF 兼容的集键 |
| 12 | 结构版本 | 01h | 版本 1 |
| 13 | 方案种类 | 02h | 加密 DM 方案 |
| 14 | 集指示符 | 01h | 加密框架 |
| 15、16 | 保留 | 00h | |
| 注：本键的字节 1~12 是为结构性元数据集规定的（377M）。 | | | |

11.4 加密上下文键

表15 加密上下文键

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|-------|---------|---------|----------------------------|
| 1 | 目标标识符 | 06h | |
| 2 | 标签大小 | 0Eh | |
| 3 | 指示符 | 2Bh | ISO、ORG |
| 4 | 指示符 | 34h | SMPTE |
| 5 | 注册类别指示符 | 02h | 组（集与包） |
| 6 | 注册指示符 | 53h | 局部集, 2个8位字节长度字段，2个8位字节标记字段 |
| 7 | 结构指示符 | 01h | 集/包字典 |
| 8 | 版本号 | 01h | 该标签在注册时的注册版本 |
| 9 | 项指示符 | 0Dh | 机构注册 |
| 10 | 机构 | 01h | AAF 协会 |
| 11 | 应用 | 04h | MXF/AAF 兼容的集键 |
| 12 | 结构版本 | 01h | 版本 1 |
| 13 | 方案种类 | 02h | 加密 DM 方案 |
| 14 | 集指示符 | 02h | 加密上下文 |
| 15、16 | 保留 | 00h | |

11.5 加密三元组键

表16 加密三元组键

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|------|----------|---------|-----------------|
| 1 | 目标标识符 | 06h | |
| 2 | 标签大小 | 0Eh | |
| 3 | 指示符 | 2Bh | ISO、ORG |
| 4 | 指示符 | 34h | SMPTE |
| 5 | 注册类别指示符 | 02h | 组（集与包） |
| 6 | 注册指示符 | 04h | 可变长包，BER 元素长度编码 |
| 7 | 结构指示符 | 01h | 集/包字典 |
| 8 | 版本号 | 01h | 该标签在注册时的注册版本 |
| 9 | 项指示符 | 0Dh | 机构注册 |
| 10 | 机构 | 01h | AAF 协会 |
| 11 | 应用 | 03h | 基本数据容器 |
| 12 | 结构版本 | 01h | 版本 1 |
| 13 | 基本数据容器种类 | 02h | MXF 通用容器 |
| 14 | 映射种类 | 7Eh | 加密基本数据 |
| 15 | 局部定义 | 01h | 加密三元组 |
| 16 | 保留 | 00h | |

11.6 128 位 AES-CBC 的 UL

表17 128 位 AES-CBC 的 UL

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|-------|---------|---------|--------------|
| 1 | 目标标识符 | 06h | |
| 2 | 标签大小 | 0Eh | |
| 3 | 指示符 | 2Bh | ISO、ORG |
| 4 | 指示符 | 34h | SMPTE |
| 5 | 注册类别指示符 | 04h | 标签 |
| 6 | 注册指示符 | 01h | 标签注册 |
| 7 | 结构指示符 | 01h | 标签结构 |
| 8 | 版本号 | 07h | 该标签在注册时的注册版本 |
| 9 | 项指示符 | 02h | 管理的 |
| 10 | | 09h | 加密 |
| 11 | | 02h | 数据加密 |
| 12 | | 01h | 数据加密算法 |
| 13 | 算法指示符 | 01h | AES-128 CBC |
| 14-16 | 保留 | 00h | |

注：本标签的字节 1~8 遵循 KLV 数据编码协议（SMPTE 336M）。

11.7 128 位 HMAC-SHA1 的 UL

表18 128 位 HMAC-SHA1 的 UL

| 字节编号 | 描述 | 值（十六进制） | 含义 |
|---|---------|---------|---------------|
| 1 | 目标标识符 | 06h | |
| 2 | 标签大小 | 0Eh | |
| 3 | 指示符 | 2Bh | ISO、ORG |
| 4 | 指示符 | 34h | SMPTE |
| 5 | 注册类别指示符 | 04h | 标签 |
| 6 | 注册指示符 | 01h | 标签注册 |
| 7 | 结构指示符 | 01h | 标签结构 |
| 8 | 版本号 | 07h | 该标签在注册时的注册版本 |
| 9 | 项指示符 | 02h | 管理用 |
| 10 | | 09h | 加密 |
| 11 | | 02h | 数据加密 |
| 12 | | 02h | 数据散列算法 |
| 13 | 算法指示符 | 01h | HMAC-SHA1 128 |
| 14-16 | 保留 | 00h | |
| 注：本标签的字节 1~8 遵循 KLV 数据编码协议（SMPTE 336M）。 | | | |

附录 A (资料性附录)

本部分与 ISO 26429-6:2008 相比章条编号变化对照一览表

本部分与ISO 26429-6:2008相比在结构上有较多调整，具体章条编号对照情况见表A.1。

表A.1 本部分与 ISO 26429-6:2008 相比章条编号变化对照一览表

| 本部分章条编号 | 对应 ISO 标准章条编号 |
|---------|---------------|
| 1 | 1 |
| 2 | 2 |
| 3 | 无 |
| 4 | 3 |
| 5 | 4 |
| 6 | 5 |
| 6.1 | 第 5 章的悬置段 |
| 6.2 | 5.1 |
| 6.3 | 5.2 |
| 6.4 | 5.3 |
| 7 | 6 |
| 7.1 | 第 6 章的悬置段 |
| 7.2 | 6.1 |
| 7.3 | 6.2 |
| 7.4 | 6.3 |
| 7.5 | 6.4 |
| 7.6 | 6.5 |
| 7.7 | 6.6 |
| 7.8 | 6.7 |
| 8 | 7 |
| 8.1 | 第 7 章的悬置段 |
| 8.2 | 7.1 |
| 8.3 | 7.2 |
| 8.4 | 7.3 |
| 8.5 | 7.4 |
| 8.6 | 7.5 |
| 8.7 | 7.6 |
| 8.8 | 7.7 |
| 8.9 | 7.8 |
| 8.10 | 7.9 |
| 8.11 | 7.10 |
| 9 | 8 |

表 A.1 本部分与 ISO 26429-6:2008 相比章条编号变化对照一览表 (续)

| 本部分章条编号 | 对应 ISO 标准章条编号 |
|---------|---------------|
| 9.1 | 第 8 章的悬置段 |
| 9.2 | 8.1 |
| 9.3 | 8.2 |
| 9.4 | 8.3 |
| 10 | 9 |
| 10.1 | 第 9 章的悬置段 |
| 10.2 | 9.1 |
| 10.3 | 9.2 |
| 10.3.1 | 第 9.2 条的悬置段 |
| 10.3.2 | 9.2.1 |
| 10.3.3 | 9.2.2 |
| 10.3.4 | 9.2.3 |
| 10.3.5 | 9.2.4 |
| 10.3.6 | 9.2.5 |
| 11 | 10 |
| 11.1 | 10.1 |
| 11.2 | 10.2 |
| 11.3 | 10.3 |
| 11.4 | 10.4 |
| 11.5 | 10.5 |
| 11.6 | 10.6 |
| 11.7 | 10.7 |
| 附录 A | 无 |
| 附录 B | 附录 A |
| 参考文献 | 附录 B |

附 录 B
(资料性附录)
安全属性

本部分具有下述安全属性：

- 标准允许基本数据帧值的第 1 部分不加密。该部分的大小可以为每帧独立设置。
- 每个基本数据帧的第 2 部分使用 AES 算法，以 CBC 模式加密。
- 提供部分的完整性保护（篡改检测）。假设由轨迹文件 ID（TrackFileID）序列项、序列号项和 MIC 项组成的 44 字节序列随同加密源值一起交付给一个安全处理装置，某些类型的操控可以被检测到。
- 基于序列号，改变轨迹文件中基本数据帧顺序的攻击可被检测到。
- 基于序列号，删除或重复完整帧的攻击可被检测到。
- 基于轨迹文件 ID，来自另一个不同轨迹文件的插入帧或替代帧，即使采用相同的加密和 MAC 密钥，也是可检测的。
- 删除、添加或改变密文任何比特的攻击可被探测到。
- 将不同帧的部分拼接起来的攻击可被探测到。
- 某些类型的篡改是无法使用完整性检查包来探测的。
- 攻击者不能改变 KLV 填充项的长度。
- 攻击者不能改变文件中的所有元数据，包括任何三元组的密钥和长度、三元组的值部分中的大多数字段（例如，明文偏移或加密上下文链接，但不包括完整性检查包），以及加密上下文和加密框架中的所有字段。
- 导出的 MIC 密钥可以在一个安全的上下文中计算出来，并交付给一个不太安全的完整性检测装置，而没有暴露加密内容本身的密钥的风险。
- 只有知道解密密钥的实体能够辨别文件是否将被正确地解密。例如，攻击者可能干扰密钥交付或同步（例如加密上下文包在服务器上是对齐进行修改），并且只有在播放过程中才将注意到这个问题。

参 考 文 献

- [1] ANSI/SMPTE 298M-1997, Television — Universal Labels for Unique Identification of Digital Data
 - [2] SMPTE 390M-2004, Television — Material Exchange Format (MXF) — Specialized Operational Pattern "Atom" (Simplified Representation of a Single Item)
 - [3] SMPTE RP 205, Application of Unique Material Identifiers in Production and Broadcast Environments
 - [4] SMPTE RP 210, Metadata Dictionary Registry of Metadata Element Descriptions
 - [5] SMPTE RP 224, SMPTE Labels Registry
 - [6] SMPTE EG 41-2004, Material Exchange Format (MXF) — Engineering Guideline
 - [7] SMPTE EG 42-2004, Material Exchange Format (MXF) — MXF Descriptive Metadata
 - [8] ISO/IEC 14496-10:2005, Information Technology — Coding of Audio-Visual Objects — Part 10: Advanced Video Coding (AVC)
 - [9] Bruce Schneier, Applied Cryptography (Second Edition), Wiley, 1996
-