国 际 电 信 联 盟

ITU-T H.235.6

国际电信联盟
电信标准化部门

(09/2005)

H系列：视听和多媒体系统

视听业务的基础设施 — 系统概况

H.323安全性：具有本地H.235/H.245密钥管理的话音加密概要

ITU-T H.235.6建议书

国际电信联盟

ITU-T H系列建议书

视听和多媒体系统

可视电话系统的特性	H.100-H.199
视听业务的基础设施	
概述	H.200-H.219
传输多路复用和同步	H.220-H.229
系统概况	**H.230-H.239**
通信规程	H.240-H.259
活动图像编码	H.260-H.279
相关系统概况	H.280-H.299
视听业务的系统和终端设备	H.300-H.349
视听和多媒体业务的号码簿业务体系结构	H.350-H.359
视听和多媒体业务的服务质量体系结构	H.360-H.369
多媒体的补充业务	H.450-H.499
移动性和协作程序	
移动性和协作、定义、协议和程序概述	H.500-H.509
H系列多媒体系统和业务的移动性	H.510-H.519
移动多媒体协作应用和业务	H.520-H.529
移动多媒体应用和业务的安全性	H.530-H.539
移动多媒体协作应用和业务的安全性	H.540-H.549
移动性互通程序	H.550-H.559
移动多媒体协作互通程序	H.560-H.569
宽带和三网合一多媒体业务	
在VDSL上传送宽带多媒体业务	H.610-H.619

欲了解更详细信息，请查阅*ITU-T*建议书目录。

ITU-T H.235.6建议书

H.323安全性：具有本地H.235/H.245密钥管理的话音加密概要

摘　要

本建议书包含话音加密概要（原在附件D/H.235中）的安全规程，包括附属的本地H.235/H.245密钥管理。

在 H.235 子系列的较早版本中，该概要被包含在 H.235 正文及其附件 D 中。H.235.0 的附录 IV、V 和 VI 示出 H.235 第 3 版和第 4 版之间对应的全部章节、图和表。

来　源

ITU-T 第 16 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2005 年 9 月 13 日批准了 ITU-T H.235.6 建议书。

关键词

认证，证书，数字签名，加密，完整性，密钥管理，多媒体安全性，安全概要，话音加密。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

		页
1	范围	1
2	参考文献	1
2.1	规范性参考文献	1
2.2	资料性参考文献	2
3	术语和定义	3
4	符号和缩写	3
5	惯例	4
6	系统概况	5
6.1	话音加密安全概要	5
7	H.245 信令和规程	7
7.1	安全 H.245 信道操作	7
7.2	非安全 H.245 信道操作	7
7.3	能力交换	7
7.4	主控方角色	7
7.5	逻辑信道信令	8
7.6	快速连接安全性	8
7.7	加密 H.245 DTMF	11
7.8	Diffie-Hellman 操作	12
8	信令和规程	16
8.1	修订版 1 的兼容性	17
8.2	第3版的特性指示	17
8.3	密钥传送	18
8.4	增强型 OFB 模式	19
8.5	密钥管理	20
8.6	密钥更新和同步	21
8.7	非终端交互	25
8.8	多点规程	26
9	媒体流加密规程	26
9.1	媒体对话密钥	27
9.2	媒体反滥发	28
9.3	RTP/RTCP 问题	30
9.4	外 CBC 方式的三倍 DES	32
9.5	在 EOFB 方式内操作的 DES 算法	33
9.6	外 EOFB 方式的三倍 DES	33
10	合法拦截	34
11	对象标识符一览	34

页

附录 I — H.323 实施详情 36
I.1 密文填充方法 36
I.2 新密钥 38

ITU-T H.235.6建议书

H.323安全性：具有本地H.235/H.245密钥管理的话音加密概要

1 范围

本建议书规定了使用本地 H.235/H.245 密钥管理的话音加密的安全概要。用于话音加密和相关本地 H.245 密钥管理的规程在本建议书中规定。

2 参考文献

2.1 规范性参考文献

下列 ITU-T 建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的 ITU-T 建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

– ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems.*

– ITU-T Recommendation H.235 version 1 (1998), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals.*

– ITU-T Recommendation H.235 version 2 (2000), *Security and encryption for H series (H.323 and other H.245-based) multimedia terminals.*

– ITU-T Recommendation H.235 version 3 (2003), *Security and encryption for H series (H.323 and other H.245-based) multimedia terminals* plus Corrigendum 1 (2005).

– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems.*

– ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile.*

– ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile.*

– ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile*.

– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication.*

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems.*

– ITU-T Recommendation H.323 Annex F (1999), *Simple endpoint types*.

– ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*

– ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

– IETF RFC 2198 (1997), *RTP Payload for Redundant Audio Data.*

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0.*

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol.*

– IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals.*

– IETF RFC 3546 (2003), *Transport Layer Security Protocol (TLS) Extensions*.

– US National Institute of Standards, "Advanced Encryption Algorithm (AES)", *Federal Information Processing Standard, (FIPS)* Publication 197, November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

– ISO/IEC 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.*

– ISO/IEC 9797-2:2002, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.

– ISO/IEC 10118-3:2004, *Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*

– ISO/IEC 10116:2006, *Information technology – Security techniques – Modes of operation for an n-bit block cipher.*

2.2 资料性参考文献

[DES FIPS-46-2] US National Institute of Standards, Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 46-2, December 1993, http://www.itl.nist.gov/fipspubs/fip46-2.htm.

[DES FIPS-74] US National Institute of Standards, Guidelines for Implementing and Using the Data Encryption Standard, *Federal Information Processing Standard*, (FIPS) Publication 74, April 1981, http://www.itl.nist.gov/div897/pubs/fip74.htm.

[DES FIPS-81] US National Institute of Standards, DES Modes of Operation, *Federal Information Processing Standard*, (FIPS) Publication 81, December 1980, http://www.itl.nist.gov/fipspubs/fip81.htm.

[FIPS PUB 180-1] NIST, FIPS PUB 180-1: *Secure Hash Standard*, April 1995 http://csrc.nist.gov/fips/fip180-1.ps.

[LI] ETSI TR 101 772 V1.1.2, Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Independent requirements definition; Lawful interception – top level requirements.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

[RFC2268] IETF RFC 2268 (1998), *A Description of the RC2$^{(r)}$ Encryption Algorithm*.

[RFC2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[WEBOIDs] http://www.alvestrand.no/objectid/top.html.

[Daemon] DAEMON (J.), *Cipher and Hash function design*, Ph.D. Thesis, Katholieke Universiteit Leuven, March 1995.

[ESP] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

[IKE] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[ISAKMP] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

[J.170] ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.

[RTP] IETF RFC 3550 (2003), *RTP: A transport Protocol for Real-Time Applications*.

[Schneier] SCHNEIER (B.), *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995.

[SRTP] IETF RFC 3711 (2004), *The Secure Real-Time Transport Protocol*.

3 术语和定义

出于本建议书的目的，第 3 节/H.323、第 3 节/H.225.0 和第 3 节/H.245 中给出的定义适用。本建议书中使用的一些术语也在 ITU-T X.800 建议书| ISO 7498-2、X.803 建议书| ISO/IEC 10745、X.810 建议书| ISO/IEC 10181-1 和 X.811 建议书| ISO/IEC 10181-2 中定义。

另一方面，加密媒体流的**对话密钥**由主控方仅对一个特定的 RTP 对话生成（在 OLC 上）；至多对一次呼叫。生成的对话密钥采用源起于两个端点已计算过的协商一致的 Diffie-Hellman **共享秘密**的密钥加密。在此情形，DH 共享秘密充当主控方密钥的角色来保护对话密钥。

4 符号和缩写

本建议书采用下列缩写：

3DES 三倍 DES

AES 高级加密算法

ASN.1 抽象句法记法 1

CBC 密码块链接

CFB 密码反馈模式

DES 数据加密标准

DH Diffie-Hellman

DTMF 双音多频

ECB 电子码书方式

EOFB 增强型 OFB 模式

EP 端点

FEC 前向纠错

GK 网守

HMAC 散列消息认证码

IPsec	网际协议安全性
ITU	国际电信联盟
IV	初始化矢量
KS	EOFB 模式中的补白
MAC	消息认证码
MC	多点控制器
MCU	多点控制单元
MPS	多有效载荷流
OFB	输出反馈模式
OID	对象标识符
OLC	开放逻辑信道
RAS	注册、认可和状态
RC	密钥算法
ROC	轮滚计数器
RSA	Rivest、Shamir 和 Adleman
RTP	实时协议
RTCP	实时控制协议
SDU	业务数据单元
SEQ	序列号
SHA	安全散列算法
TCP	传输控制协议
TLS	传输层安全性
TSAP	传输业务接入点
UDP	用户数据报协议
XOR	异运算

5 惯例

本建议书中使用下列惯例：

— “须（Shall）”表明是强制性要求。

— “应（Should）”表明是推荐采取的非强制性措施。

— “可（May）”表明是非强制性措施，但并未建议采取这种措施。

当采用媒体加密和有效载荷填充时，报文有时候会说“填充的值必须由加密算法的通常惯例确定”；见例如 7.6.1、8.3 和图 I.7。这意味着有些加密算法（如 DES）为发送方怎样选择填充字节的值提供进一步的实施建议。例如，可以是随机填入的值、统计值或其他生成模式。无论采用哪种方法，都不要影响互操作性，也不要让安全质量可能产生不同。这被认为是实施事务，在本建议书中不进一步规定。

6 系统概况

6.1 话音加密安全概要

话音加密安全概要不是同基线安全概要一样的独立概要。确切地它是前面提到的安全概要的选项并可以与基线安全概要一起使用。该概要也依赖于作为呼叫信令和连接建立规程一部分的某些安全性业务；例如 Diffie-Hellman 密钥协议和其他密钥管理功能。

H.323 实体可以实施话音加密概要以实现话音机密性。提供了三种加密算法：推荐的方案是使用基于商业模型和输出能力需求的 RC2 兼容、DES 或三倍 DES 加密。已经提供某种程度机密性的环境可以不要求话音加密。在此情形，Diffie-Hellman 密钥协议和其他密钥管理规程同样不是必要的。

对于任选的话音机密性，推荐的方案是使用基于商业模型与出口能力需求的 RC2 兼容、DES 或三倍 DES 算法来加密。在已经提供某种程度机密性的某些环境中可以不要求话音加密。在此情形，Diffie-Hellman 密钥管理和其他密钥管理规程同样不是必要的。

本建议书进一步提供 ITU-T H.235 建议书第 2 版附件 D 或 ITU-T H.235 建议书第 3 版附件 D 已经提供的候选话音加密算法的列表概况。

注 1 — 这更进一步的加密算法概要考虑到有关加密算法强度的已知密码分析学和安全性判定以及加密输出政策的改变。特别地，本建议书的加密算法的模型考虑到与遵循 H.235 第 2 版或第 3 版的系统的互操作性要求。

实施 H.235 第 4 版或更高版本的本建议书的 H.323 实体在其为达到最高性能和最佳安全性提供的安全能力中必须提供 128 比特 AES 作为首选话音加密算法。另外，这些 H.323 实体可任选地也提供 168 比特三倍 DES 作为话音加密算法，以达到与已经实施了附件 D/H.235 第 2 版和第 3 版中的话音加密特性地 H.323 系统的较高的互操作性。由于 56 比特 DES 和 56 比特 RC2 兼容（可输出的）加密算法不再被认为足够安全，所以 H.323 实体应不提供那些特殊的弱加密算法，除非有特殊的需要，例如达到与附件 D/H.235 第 2 版和第 3 版中的话音加密系统的互操作性。

实施 ITU-T H.235 建议书第 4 版的本建议书的 H.323 实体必须首选接受提供的 128 比特 AES，如果其安全性政策允许的话。另外，出于安全性原因，那些 H.323 实体应不接收 56 比特 DES 或 56 比特 RC2 兼容性，除非其安全性政策明确允许这样的不安全加密算法，或可输出性需要要求这样的算法，且未提供其他较安全的替代如 128 比特 AES 或 168 比特三倍 DES。

接入控制手段未明确描述；它们可以在 H.235 信令字段内（ClearToken，CryptoToken）所传送的接收信息上局部实施。

就运行和管理而言，本建议书未描述基于预订的口令/密钥分配规程。此规程通过不属于本建议书范围的手段实施。

涉及的通信实体能够隐含地确定或基线安全概要或签名安全概要的用法，通过估算该消息中签署的安全性对象标识符（**tokenOID** 和 **algorithmOID**；也见第 11 节）。

表 1 概述了话音加密概要的安全性特性。话音加密概要在第 7、8 和 9 节中规定。

表 1/H.235.6－话音加密概要

<table>
<tr><th rowspan="2">安全性业务</th><th colspan="4">呼叫功能</th></tr>
<tr><th>RAS</th><th>H.225.0</th><th>H.245</th><th>RTP</th></tr>
<tr><td>认证和完整性</td><td></td><td></td><td></td><td></td></tr>
<tr><td>不可否认</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>56 比特 DES | 56 比特 RC2 兼容的 | 168 比特三倍 DES | 128 比特 AES</td></tr>
<tr><td>机密性</td><td></td><td></td><td></td><td>CBC 模式或 EOFB 模式</td></tr>
<tr><td>接入控制</td><td></td><td></td><td></td><td></td></tr>
<tr><td>密钥管理</td><td></td><td>认证 Diffie-Hellman 密钥交换</td><td>完整的 H.235 对话密钥管理（认证 Diffie-Hellman 密钥交换、密钥更新）</td><td></td></tr>
</table>

在连接初始化期间通用规程在两个通信同线用户之间建立共享秘密（Diffie-Hellman 交换）。然后使用该共享秘密保护用于加密媒体（RTP）对话的（一系列）媒体密钥。

话音加密安全概要是对基线安全概要和签名安全概要的任选增强；它的使用可以作为终端安全能力协商的一部分来协商。在通过其他手段确保话音机密性的环境中，不存在任何需要实施的媒体加密以及相关的密钥管理规程（Diffie-Hellman 密钥协议、密钥更新和同步）。

选择的加密算法是 RC-2 兼容的，DES 和三倍 DES 算法。

注 2 — 由于三倍 DES 算法实施也可以供 DES 算法使用，因此这将导致一个紧凑的实施。

不考虑特定媒体加密算法的选择，必须明确遵循以下选项：

- 如 9.3.1 所规定的，只要需要就要生成初始化矢量（IV）。
- 如 9.3.2 所描述的，只要需要就应填充。

使用协商的加密算法（“X”，“Y”，“Z3”或“Z”）依照第 11 节中描述的规程对音频有效载荷加密。也可以使用协商的加密算法（“X1”，“Y1”，“Z1”或“Z2”）以流密码方式（EOFB）对音频有效载荷加密。

7 H.245信令和规程

一般而言，媒体信道的保密性能采用与任何其他编码参数同样的方式来控制；每个终端指示其能力，数据源选择使用格式，而接收者确认或否认该方式。该体系的所有与传输无关的领域（诸如算法选择）均在通用逻辑信道单元中指示。传输细节（如密钥/加密算法同步）以传输特定的结构传送。

7.1 安全H.245信道操作

假定前一节（连接建立规程）中连接规程指示安全的运行方式，在任何其他的 H.245 消息交换之前，该 H.245 逻辑信道的协商的信号交换和认证必须完成。若协商，则必须使用任何适合于 H 系列终端的机制实现证书的任何交换。完成 H.245 信道安全之后，该终端以这样的方式使用 H.245 协议，即处于非安全方式下的终端会采取的方式。

7.2 非安全H.245信道操作

H.245 信道也可以采用非安全方式运行，并且双方实体开放安全逻辑信道用于实施认证和/或共享密钥的衍生。例如，通过 **dataType** 字段的值为 **h235Control** 的逻辑信道使用 TLS 或 IPSEC。然后该信道可用于衍生保护任何媒体对话密钥的共享密钥或用于传输 **EncryptionSync**。

7.3 能力交换

遵从 5.2/H.245（能力交换规程）以及适当的 H 系列系统建议书中的规程，端点使用 H.245 消息交换能力。这些能力集现在可以包含指示安全性和加密参数的那些定义。例如，端点可以提供发送和接收 H.261 视频的能力。它也可以签署发送和接收加密 H.261 视频的能力。

每个与特殊媒体编译码器一起使用的加密算法均隐含一种新的能力定义。与任何其他能力一样，端点可以在其交换中提供独立或非独立的加密编译码器。这将允许端点根据开销和可用的资源来调节其安全能力。

能力交换完成之后，端点可以处于非安全方式下的终端会采取的方式为媒体开放安全逻辑信道。

7.4 主控方角色

为了解决双向信道运行以及其他冲突问题，使用 H.245 主从确定规程建立主控方实体。此主控方角色也在安全性方法中使用。媒体流的安全方式由信源设置（遵从该接收者的能力），但是主控方是生成加密密钥的端点。生成该加密密钥，不考虑主控方是否是加密媒体的接收者或源起方。为了允许组播信道采用共享密钥运行，MC（也指主控方）应生成密钥。

7.5 逻辑信道信令

端点以它们开放非安全媒体逻辑信道的同样方式开放安全媒体逻辑信道。每个信道均可以采用与其他信道完全独立的方式操作，特别在该信道隶属安全性的场合。这种特殊的方式必须在 **OpenLogicalChannel** 的 **dataType** 字段中定义。根据 **OpenLogicalChannel** 的始发方的主/从关系，初始加密密钥必须在 **OpenLogicalChannel** 中或者在 **OpenLogicalChannelAck** 中传送。

OpenLogicalChannelAck 必须充当加密方式的批准角色。若接收者不接受 **OpenLogicalChannel**，则在 **OpenLogicalChannelReject** 的 cause 字段中将返还或 **dataTypeNotSupported** 或 **dataTypeNotAvailable**（瞬间条件）。

建立逻辑信道的协议交换期间，加密密钥必须从主控方向从属方传送（不考虑谁始发该 **OpenLogical Channel**）。对于由端点（而不是由主控方）开放的媒体信道，主控方必须在 **OpenLogicalChannelAck** 消息中（在 **EncryptionSync** 字段中）返还初始加密密钥和初始同步点。对于由主控方开放的媒体信道，**OpenLogicalChannel** 必须在 **EncryptionSync** 字段中包含初始加密密钥和该同步点。

7.6 快速连接安全性

端点可以采用快速连接规程（见 8.1.7 和 8.1.7.1/H.323），该规程使用快速起动单元安全地交换密钥资料（主密钥和对话加密密钥）。7.6.1 中给出的规程描述了不使用多个提供的加密算法的“平面”快速起动，而 7.6.1.1 描述了使用多个提供的加密算法从而使得消息编码更紧凑的快速起动的特定实例。

7.6.1 单向快速起动安全性

这一规程描述了如何建立从主叫方到被叫方的（半双工）的单向安全逻辑信道。

主叫方规程

主叫方（**Setup** 的源）表示其 DH 令牌和支持的 **FastStart** 结构。DH 令牌必须在嵌入的 **ClearToken** 内作为 **CryptoToken** 的一部分或一个单独的 ClearToken 传送，也见 7.8。在 SETUP-to-CONNECT 序列中，必须执行 Diffie-Hellman（DH）交换：这将共享的密码散布到各端点中。**CryptoToken** 子节的 **ClearToken** 子节必须包含一个 **dhkey**，如本建议书所规定的，它用于传送参数。**Halfkey** 包含一方的随机公钥，**modsize** 包含 **DH-prime**，**generator** 包含 DH 群。将使用的 DH 参数在表 4 中示出。更多细节，请参见[RFC2412]，附录 E2。

注 1 — 由于 H.225.0 消息被认证（如先前由规程 I 描述的），DH 交换也是一个认证过程。

在携载 Diffie-Hell 半密钥的 H.225.0 呼叫信令消息的任一方向上，当可获得鉴别信息时，主叫方或被叫方在被注册时必须也包括一个单独的端到端 **ClearToken**，其 **sendersID** 设置为发送者的端点标识符，**tokenOID** 设置为“E”。任何中级 H.323 信令实体必须前送未修改的特定端到端令牌。

FastStart 结构包含所提供的开放逻辑信道和提议的安全性能。H235Cap 和 nonH235Cap 信道都应提供。在 H.245 Cap 交换过程中，端点表示其支持的编解码器的 **H235SecurityCapability** 入口。每个编解码器与一个单独的 H.235 安全能力相关。依据附件 D，这些能力应标识支持 128 比特 AES-CBC（OID—“Z3”）和 56 比特 RC2 兼容的 CBC（OID—“X”），应标识支持 56 比特 DES-CBC（OID—“Y”），可标识支持 168 比特三倍 DES-CBC（OID—“Z”）或 168 比特三倍 DES-EOFB（OID—“Z1”），RC2 兼容的 EOFB（OID—“X1”）、DES-EOFB（OID—“Y1”）或 AES-EOFB（OID—“Z2”）。

OpenLogicalChannel 传送 **forwardLogicalChannelParameters** 和 **reverseLogicalChannelParameters** 以及提供 **h235Media** 和 **encryptionAuthenticationAndIntegrity** 的 **dataType**，其中在 **encryptionCapability** 中，最多必须有一个 **MediaEncryptionAlgorithm**。

出于安全关系的目的，被叫方首先应是主控方，也见 7.4。

主叫方应设置 **mediaWaitForConnect** 为真，以确定对话密钥资料可以获得，且接收到的加密媒体可以解密。在这些情况中，在需要“超前媒体”的地方，这样的被叫方传送加密或未加密的媒体，同时发送响应消息和加密密钥资料，主叫方应准备好不能解密内容，除非密钥资料可以获得。

注 2 — 在这一情况下，如果被叫方发送加密媒体给主叫方（理论上可以这么做，因为它有主叫方的 RTP/RTCP 地址），没有在（告警、呼叫处理）连接消息中提供的共享密码，则主叫方不能破译它。

被叫方规程

在 FastStart 启动过程中，被叫方提出其 DH 令牌（也见 7.8）和接收的 FastStart 结构。在应用 Diffie-Hellman 规程的情况下，建议被叫方尽早将其 DH 令牌作为响应消息的一部分返回，即在响应消息中紧接着 SETUP。这允许主叫方从 DH 共享密码中计算出主密钥，并准备好接收对话密钥和加密媒体。

注 3 — 在两边都没有加密算法可获得的情况下，媒体流可留着不加密或连接可以中断，视安全政策而定。

每个实体必须从用于密钥加密密钥（主密钥）的通用共享 Diffie-Hellman 密码中抽出适当最不重要的比特，即 OID“X”、OID“X1”、OID“Y1”或 OID“Y”的 Diffie-Hellman 密码的最不重要的 56 比特和 OID“Z”、OID“Z1”或 OID“Z2”的 Diffie-Hellman 密码的最不重要的 168 比特以及 OID“Z3”或 OID“Z2”的 Diffie-Hellman 密码的最不重要的 128 比特，也见表 6。

OpenLogicalChannel（Ack）响应与包含在 **encryptionSync** 字段中的（主控）创造的对话一起发布。这一 **encryptionSync** 包含从主叫方到被叫方的直接逻辑信道的对话密钥。密钥传送必须按照 8.3 中描述的规程执行，使用 **KeySyncMaterial** 或 **V3KeySyncMaterial**（也见 8.3.1）。对话密钥必须以下述的方式用 DH 共享密码加密。

注 4 — 这里没有被用来加密媒体、生成对话密钥的规定方法。这些值的生成是受本地资源、政策和使用的加密算法影响的实施事务。应注意避免生成弱密钥。

使用 8.3 的规程，加密对话密钥必须在 **encryptionSync** 字节内的 **H.235Key/sharedSecret** 中携载。对话密钥必须在 **KeySyncMaterial** 的 **keyMaterial** 字段中携载 — 如果不是块尺寸的倍数的话 — 必须在加密前填充为块的倍数。填充的值应按照加密算法的通常惯例确定。（填充的）**KeySyncMaterial** 必须用以下的加密：

— 共享密码的 56 比特，以 OID“X”、OID“X1”、OID“Y1”或 OID“Y”的 Diffie-Hellman 密码的最不重要的比特起始；

— OID“Z”、OID“Z1”或 OID“Z2”的共享密码的所有比特，以来自 DH 密码的最不重要的比特起始。

交替地和更好地，依据 8.3.1，由于标识规程的第 3 版的结果，应使用改进的密钥传送（见 8.2）。

在两个单向信道之外的全双工安全媒体信道要使用快速起动确立的情况下，被叫方必须向主叫方开放一个次级的逻辑信道。这一逻辑信道必须在单独的 fastStart 单元中发信令。使用可获得的 DH 共享密码作为主密钥，被叫方包括一个在 **encryptionSync** 内的逻辑信道的不同的对话密钥。

7.6.1.1 在快速连接中使用多重加密算法

媒体加密作为快速连接规程的一部分的协商导致在 SETUP 消息的 **fastConnect** 单元中无效地扩展 **OpenLogicalChannel** 的数字。这会发生是因为每个编解码器（**dataType**）的组合和加密算法（包括“无”）都需要单独的 **OLC**。

应用于媒体流的加密算法通过在 **OLC** 中包括 **dataType.h235Media.encryptionAuthenticationAndIntegrity.encryptionCapability dataType** 来规定。H.235v2 操作要在 **encryptionCapability** 中仅包括一个单独的 **MediaEncryptionAlgorithm**，尽管后者定义为前者的一个序列。这一规程允许在每个提供的 **OLC** 中包括加密性能的优先级序列。然后 **OLC** 的接收者必须从中选择一个单独的算法，必须回送 **OLC** 和选出的惟一一个算法指示（以及合适的传送地址和加密密钥信息）。

为了提供最大的有效性，对象 ID“NULL-ENCR”（见表 2）表示“NULL”加密算法，这意味着没有加密操作发生。使用这一特定算法仅需要一个 **OLC**，每个方向上每个 OLC 提供编解码器。

表 2/H.235.6－NULL加密的对象标识符

对象标识符 参考符	对象标识符值	描　　述
“NULL-ENCR”	{itu-t（0）recommendation（0）h（8）235 version（0）3 26}	指示“NULL 加密算法”

主叫方规程（见 *8.1.7.1/H.323*）

如果提供的 **dataType** 单元经由 **h235Media** 选择规定加密，则包括的 **encryptionAuthenticationAndIntegrity** 单元可包括 **encryptionCapability** 单元，该单元包含多个加密算法（包括 NULL 算法）。必须采用这一构造来为任何人提供对相关媒体性能的加密的特定算法的选择。

被叫方规程（见 *8.1.7.1/H.323*）

如果为一个信道提供多个加密算法，被叫的端点务必选择一个，并修改 **OpenLogicalChannel** 以移除其他的算法。

7.6.2 双向快速起动安全性

双向 T.120 数据信道的安全性有待进一步研究。

7.7 加密H.245 DTMF

端点可以选择发送加密 DTMF 信号以获得机密性。使用对话加密密钥，端点可以在 **UserInputIndication** 中加密 DTMF 信号，如：

- 加密的基本串：**encryptedAlphanumeric**；
- 加密的 iA5 串：**Signal** 中的 **encryptedSignalType**；
- 加密的通用串：**extendedAlphanumeric** 中的 **encryptedAlphanumeric**。

注 1 — 在 iA5 串中 RTP 的额外的参数具有时间标记和逻辑信道数或随音频时长更新的信号，它们不加密，因为考虑到它们不传送敏感信息。

协商的性能 **secureDTMF** 与加密的 iA5 串有关。

如第 6.1 节所规定的密钥管理应用来生成一个对话加密密钥。在加密 H.245 DTMF 信号时必须使用这一对话加密密钥。

注 2 — 这不是必需意味着对话密钥应同样应用于 RTP 有效载荷加密。

然而，当也通过设置 **rtpPayloadIndication** 标记经由 RTP 使用 DTMF（RFC 2833）时，强烈地建议使用 6.1 的话音加密概要保证 RTP 有效载荷的安全。

表 3 提供可获得的加密算法（DES、3DES 或 AES），这些算法应采用 EOFB（包括 OFB 作为一个具体实例，见 8.4）。为了避免 DTMF（RFC 2833）字符的潜在填充，不建议对 DTMF（RFC 2833）信号的加密使用 CBC、CFB 或可能必需填充的其他块链模式。

7.7.1 加密的基串

如果在 **UserInputCapability** 中选择了 **encryptedBasicString**，则 **encryptedAlphanumeric** 必须指示在 **algorithmOID** 内采用了加密算法，**paramS** 包含加密操作的初始值。加密的文字数字串必须放在 **encrypted** 中。

7.7.2 加密的iA5串

如果在 **UserInputCapability** 选择了 **encryptedIA5String**，则 **encryptedSignalType** 必须包含加密的 **ClearSignalType**，其中 **sig** 传送明文 **signalType** 字符。**signalType** 必须包含一个叹号“！”，它必须被接收者丢弃。

algorithmOID 必须指示采用的加密算法，**paramS** 包含加密算法的初始值。

7.7.3 加密的通用串

如果在 **UserInputCapability** 中选择 **encryptedGeneralString**，则 **extendedAlphanumeric** 内的 **encryptedAlphanumeric** 必须指示在 **algorithmOID** 内的加密算法，而 **alphanumeric** 必须包含一个空串，**paramS** 包含加密操作的初始值。

7.7.4 对象标识符一览

表 3/H.235.6－H.245 DTMF加密的对象标识符

对象标识符 参考符	对象标识符值	描　　述
“DES-EOFB-DTMF”	{itu-t（0）recommendation（0）h（8）235 version（0）3 12}	在 EOFB 模式中用 DES-56 的 H.245 DTMF 加密
“3DES-EOFB-DTMF”	{itu-t（0）recommendation（0）h（8）235 version（0）3 13}	在 EOFB 模式中用 3DES-168 的 H.245 DTMF 加密
“AES-EOFB-DTMF”	{itu-t（0）recommendation（0）h（8）235 version（0）3 14}	在 EOFB 模式中用 AES-128 的 H.245 DTMF 加密

7.8 Diffie-Hellman操作

本建议书支持端到端密钥协定的 Diffie-Hellman 协议。根据不同的情况，协商的 Diffie-Hellman 密钥可以作为主密钥（见 6.1）或作为动态对话密钥（ITU-T H.235.3 和 H.530 建议书）动作。

Diffie-Hellman 系统用系统参数 g 和 p 表征，其中 p 必须是一个大素数，g 表示以模 p 的乘法组的生成器或模 p 的强子组的生成器。g^x 除以 p 表示主叫方的（公共）Diffie-Hellman 半密钥，而 g^y 除以 p 表示被叫方的（公共）Diffie-Hellman 半密钥。RFC 2412 提供进一步的背景信息和如何选择安全的 Diffie-Hellman 参数的建议。

ITU-T H.235.0 建议书传送一个 Diffie-Hellman 实例（g，p，g^x），它在 **ClearToken** 中编码，其中对于一些随机密码 x（或者 y）、在 **modsize** 和 **generator** g 中的素数 p，**dhkey** 掌握 **halfkey** g^x 除以 p（或者 g^y 除以 p）。一个特殊的情况是三元组（0，0，0）或空 **dhkey**，空 **dhkey** 不代表任何 DH 实例，但在不使用话音加密概要的信令中必须使用。

通常，DH 系统参数 p 和 g 一起用于一系列完好定义的值的应用，但是端点系统也可以选择其自己的参数集。被叫方应关注非标准化的 DH 参数可以提供的安全性不如第一眼看见的那些参数能提供的安全性这一事实，例如，主叫方可能已经选择了非素数，或 g 只生成较小的子组。而广延参数测试在实践中不能实行，它依据被叫方的安全性政策接受或拒绝这样的提议。

对于固定的 DH 系统参数，通过对象标识符进行的速记描述可以得出比包括字面上的值更紧凑的编码消息。传送具有固定、标准化的 DH 参数的 DH 实例的 **ClearToken** 可以参考在 **tokenOID** 字节中具有 DH-OID 的 DH 实例；除非 **tokenOID** 用于其他目的（如第 7 节/H.235.1 中的著名的 **CryptoToken**）。另外发送者可以包括字面上的 DH 值，但不需要这样做。

在几个 DH 实例中的每个要通过一个 DH-OID 指示的情况下，在著名的 **CryptoToken**（通过 H.235.1 占用）中的 DH 参数必须通过让 **dhkey** 缺省置之不理，而所有的 DH 实例必须在单独的 **ClearToken** 中传送，其中，**tokenOID** 包含 DH-OID，而 **dhkey** 可能缺省；在那个 **ClearToken** 中的其他字节不应使用。

注 1 — 这不排除在一个著名的 **CryptoToken** 中或通过逐字地包括 DH 参数值在其他可以获得的 **ClearToken** 中传送一个 DH 实例的可能性。

在要指示非标准化的 DH 实例的情况下，DH-OID“DH dummy”必须使用，非标准化的 DH 群参数必须明确地在 **ClearToken** 中提供。

主叫方可以提交一个或多个 **ClearTokens**，它们每一个传送一个不同的 Diffie-Hellman 实例。鼓励主叫方像其安全性政策允许的那样提供尽可能多的 DH 实例。这允许被叫方选择一个适当的实例响应，因此增加了找到一个成功的通用参数集的可能性。

被叫方必须选择和接受一个单独的 DH 实例（如果根本的话），该实例从在 SETUP 消息中由呼叫者提供无序的 DH 实例集中选择。在被叫方能够选择适配其安全性需求的 DH 实例，被叫方不得修改提议的 DH 实例或返回不是由主叫方发送的 DH 实例。在呼叫过程中 EP 均可获得的加密算法的强度应对应于被叫方返回的所选的 DH 实例所提供的强度；见表 4。被叫方必须指示在响应消息中选择的 DH 实例。

在被叫方拒绝任何出于安全理由的提议或由于缺乏处理性能，被叫方必须在响应消息中让 **dhkey** 缺省。

呼叫方必须在 SETUP-to-CONNECT 响应中包括 DH 令牌。被叫方可以在紧随 SETUP 的立即响应消息中包括 DH 令牌，或可能在某些后来的阶段中包括 DH 令牌，按在 CONNECT 消息中只是在最近的阶段中包括 DH 令牌。

注 2 — 关于当被叫方在 SETUP-to-CONNECT 响应过程中可能包括 DH 令牌有几个方面要考虑：响应时间、在被叫方上的处理负荷、初期媒体的性能和其他方面。这些问题要依据实施考虑。

但是，出于某些理由，某些选路 GK 可能不向主叫方传送所有的 SETUP-to-CONNECT 响应。因而，包括一个可能的 DH 令牌的一个或多个 H.225.0 呼叫信令响应消息可能会丢失，而不能到达主叫方。那么主叫方就不能计算 DH 主密钥和媒体对话密钥。为了防止这种情况的发生，被叫方应总是在每个 SETUP-to-CONNECT 响应消息中包括同一个 DH 令牌。

在 DH-OID 指示一个不同的 DH 实例而不是实际在 **modsize** 和 **generator** 中被传送的实例的情况下，在 **modsize** 和 **generator** 中传送的字面上的值必须在令牌中优于 DH-OID。为了响应，被叫方应用静态 DH-OID 取代有冲突的 DH-OID，即“DH1024”，它对应于 **modsize** 和 **generator** 或“DHdummy”，如果没有相应的 DH-OID 的话。

7.8.1 在呼叫中请求重新协商DH参数

H.323 网守可在呼叫中用本节中定义的规程请求 DH 参数的重新协商。可能需要这样的重新协商规程来建立已经连接到网守的端点和将要连接到网守的端点之间的 DH 密钥协定（见图 1）。支持几个增补的业务需要重新协商 Diffie-Hellman 的规程。所有在本节中定义的规程必须仅当 H.323 端点在 8.4.6/H.323 中定义的“传送侧停止”状态下时执行。

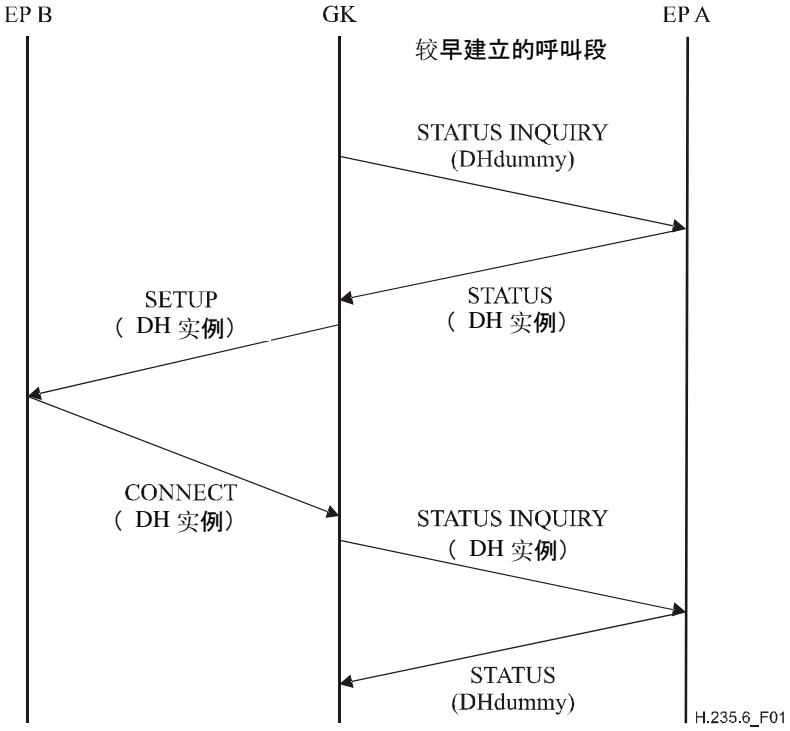


图 1/H.235.6－增补业务使用“在呼叫中请求DH参数”

为了在呼叫中请求 DH 参数，H.323 实体必须发送包含在 **tokenOID** 字段中具有 DH-OID "DHdummy" 的 **ClearToken** 字段的 STATUS INQUIRY 消息，字段其余部分省略。

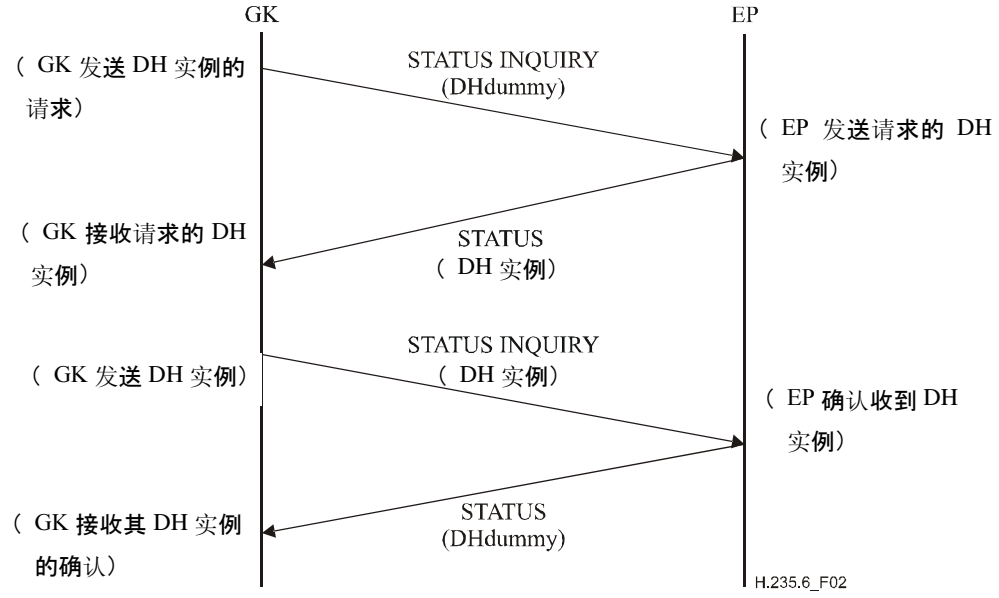


图 2/H.235.6－在呼叫中请求DH参数

如果一个 H.323 实体接收到包含具有 **tokenOID** 字段中的 DH-OID“DHdummy”的 **ClearToken** 字段的 STATUS INQUIRY 消息，则 H.323 端点必须用包含 DH 实例集的 STATUS 消息响应，见图 2。按照关于 SETUP 消息的第 7.8 节中定义的规则，DH 实例必须在这一 STATUS 消息中规定。

注 1 — 不支持这一规程的 H.323 实体假定用无 DH 实例的 STATUS 消息响应 STATUS INQUIRY。

为了在呼叫中传送接受的 DH 实例，H.323 实体必须发送包含接受的 DH 实例的 STATUS INQUIRY，见图 2。按照关于响应 SETUP 消息的第 7.8 节中定义的规则，DH 实例必须在这一 STATUS INQUIRY 消息中规定。

如果一个 H.323 端点收到这样一个包含具有 DH 实例的 **ClearToken** 字段的 STATUS INQUIRY 消息，则 H.323 端点必须用包含在 **tokenOID** 字段中具有 DH-OID“DHdummy”的 **ClearToken** 字段的 STATUS 消息响应，字段其余部分省略。

注 2 —不支持这一规程的 H.323 实体假定用无 DH 实例的 STATUS 消息响应 STATUS INQUIRY。

接收具有 DH 实例的 STATUS INQUIRY 消息的 H.323 端点必须重新计算来自这一 DH 实例的 DH 共享密钥以及已经由 H.323 端点在特定呼叫中发送的最新的 DH 实例。

如果一个 H.323 GK 接收到包含具有 DH 实例或是在 **tokenOID** 字段中具有 DH-OID 的 **ClearToken** 字段的 STATUS INQUIRY 消息，那么，除了以下列出的几种情况外，它必须在已经收到的消息的环境下前送消息到呼叫的第二段。

如果一个 H.323 GK 收到其前送的 STATUS INQUIRY 消息的 STATUS 响应，则 GK 必须返回 STATUS 消息给已经收到 STATUS INQUIRY 消息的呼叫段。

如果等待响应包含具有其已经发送的 **tokenOID** 字段中的 DH-OID“DHdummy”的 **ClearToken** 字段的 STATUS INQUIRY 消息的 H.323 GK 接收到包含具有 **tokenOID** 字段中的 DH-OID "DHdummy"的 **ClearToken** 字段的 STATUS INQUIRY 消息，且 CRV 标志被设置为值 1，则 GK 必须用包含具有 **tokenOID** 字段中的 DH-OID “DHdummy”的 **ClearToken** 字段的 STATUS 消息响应（见图 3）。

如果当呼叫的另一端未确定，一个 H.323 GK 接收到包含具有 DH 实例或具有 **tokenOID** 字段中的 DH-OID“DHdummy”的 **ClearToken** 字段的 STATUS INQUIRY 消息，则 GK 必须等待呼叫另一端确定，发送有关这一呼叫侧的空能力集，然后将其发送给接收的 STATUS INQUIRY 消息（见图 3）。

H.323 GK 在其已经发送了包含 DH 实例的 STATUS 消息后，以及在其已经接收包含 DH 实例的 STATUS INQUIRY 消息前，不得始发本节中定义的规程。

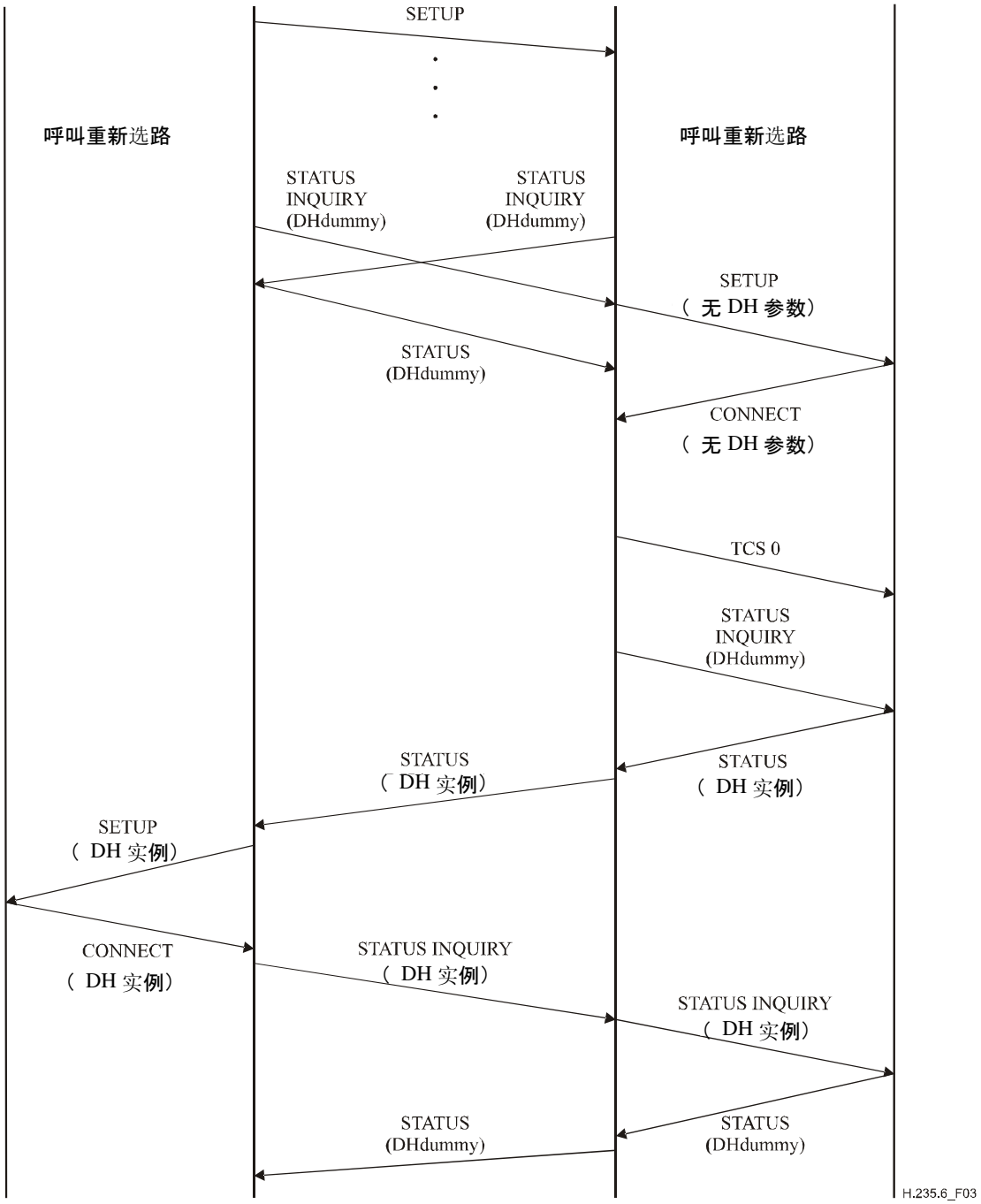


图 3/H.235.6－对于两个GK同时呼叫重新选路使用“在呼叫中请求DH参数”

8 信令和规程

必须遵从第 8 节/H.323 中概述的规程（呼叫信令规程）。对于 H.225.0 消息中所签署的（对于 H.245 信道的）安全性需求的存在（或不存在），H.323 端点必须具备编码和识别的能力。

在 H.225.0 信道自身被保护的情形中，也必须遵从第 8 节/H.323 中同样的规程。运行中的差别仅在于该通信必须仅在连接至安全的 TSAP 标识符并使用预先确定的安全方式（例如 TSL（RFC 2246，RFC

3546）后发生。由于建立 H.323 通信时首先交换 H.225.0 消息的这一事实，对 H.225.0 不能存在任何的带内安全性协商。换句话说，双方用户务必事先知道他们所使用的特殊安全方式。对于 IP 上的 H.323，可以使用供 TLS 安全通信所任意选择的熟知端口（1300）。

就 H.225.0 交换与 H.323 安全性关系而论，H.225.0 交换的用途之一就是提供建立安全 H.245 信道的机制。作为任选项目，认证可在 H.225.0 消息交换期间发生。该认证可以是基于证书或口令的，使用加密和/或散列（即签名）的方法。这些操作方式的细节在 8.1 到 8.2.3/H.235.0 中描述。

伴随 **h245SecurityCapability** 集接收建立消息的 H.323 端点务必采用连接消息中相应可接受的 **h245SecurityMode** 响应。在不存在任何交叠能力的情况下，被叫终端可以通过发送具有原因代码设置为 ***SecurityDenied*** 的 **Release Complete** 消息来拒绝连接。此类错误意指不传送任何有关安全性失配的信息以致主叫端不得不通过某些其他手段来确定原因。主叫端在接收连接消息而又无足够的或可接受的安全方式的情况下，可采用具有 ***SecurityDenied*** 的 **Release Complete** 消息来终止呼叫。主叫端在接收无任何安全能力的连接消息的情况下，可采用具有 ***undefinedReason*** 的 **Release Complete** 来终止呼叫。

主叫端若接收可接受的 **h245SecurityMode**，则务必以该指定的安全方式开放并操作 H.245 信道。未能以这种指定的安全方式建立 H.245 信道应被认为是协议误差并终止连接。

8.1 修订版1的兼容性

具有安全能力的端点将不得对无安全能力的端点返还任何与安全有关的字段、指示或状态。若主叫方接收不包含 **h245SecurityCapability** 和/或认证令牌的建立消息，则它可通过返还 **Release Complete** 来拒绝连接；而且在此情况下它必须使用 ***undefinedReason*** 的理由代码。以相应的方式，若主叫方接收无任何 **h245Security** 和/或认证令牌的连接消息并曾发送具有 **h245Security** 和/或认证令牌的建立消息，则它也可以通过发布具有 ***undefinedReason*** 的理由代码的 **Release Complete** 来终止连接。

8.2 第3版的特性指示

H.235 第 3 版和更高版本的端点提供在 H.235 第 1 版和 H.235 第 2 版中不提供的改进的在媒体上的安全规程。这些改进的安全规程有：

- 改进的密钥的传送（**V3KeySyncMaterial**，见 8.3.1）；
- 改进的密钥更新，见 8.6.2。

因为端点通常不知道它们与 H.235 第 3 版相互支持，所以在所有的呼叫建立过程中增加明确的版本指示。

为了确定第 3 版的性能（改进的密钥传送、改进的密钥同步），H.235 第 3 版和更高版本的端点应总是使用本节中描述的规程。依据逻辑信令规程的结果，为了与第 1 版和第 2 版的端点后向兼容，端点可使用规程（见 8.3）。

为了指示是否使用改进的 H.235 第 3 版的规程，主叫和被叫的端点必须包括一个另外的 **ClearToken**，它在呼叫信令过程（SETUP、CONNECT，等等）中指示第 3 版。没有这样一个 **ClearToken** 会指示仅支持 H.235 第 1 版或第 2 版。在这一情况下，端点必须使用 8.3 中的规程。否则，端点可使用 8.3.1 中描述的改进的规程，或使用 8.3 中的第 1 版和第 2 版的规程。

ClearToken 必须使用设置为“V3”的 **tokenOID**，它被赋予下列值：

“V3”	{itu-t (0) recommendation (0) h (8) 235 version(0)3 24}	在呼叫信令过程中 ClearToken 中的第 3 版性能标识符。

ClearToken 中的任何其他字节必须保持未使用，除非被用来传送 DH 参数。

8.3 密钥传送

主密钥必须对话密钥资料，将其分配给对等方。为密钥传送提供了两个规程：

- 主要用于 H.235 第 1 版和 2 端点的规程；在本节中描述。
- 用于 H.235 第 3 版和更高版本端点的改进的规程，在 8.3.1 中描述。

H.235 第 1 版或第 2 版端点采用下列规程来进行对话密钥传送：

KeySyncMaterial 在 **generalID** 包含主控方的端点标识符，传送在 **keyMaterial** 内的对话密钥资料。应包括 **generalID** 值以提供对话密钥源的认证最低水平（也见 8.6）。接收者应检验接收到的 **generalID** 的正确性。

注 — 本建议书假定每个端点已用一个网守注册，获得一个可以在 **generalID** 内传送的端点标识符。本建议书不支持没有网守的情况；这有待进一步研究。

KeySyncMaterial 必须使用协商的主密钥加密。**KeySyncMaterial** 在加密前必须总是填充为块的倍数，其中最后一个字节必须被设置为填充八比特组的数（包括最后一个八比特组）。填充的值应由加密算法的通常惯例确定。加密的结果必须存储在 **H235Key** 的 **sharedSecret** 中。

8.3.1 在H.235第3版中改进的密钥传输

已观察到 **KeySyncMaterial** 的 ASN.1 句法定义和 ENCRYPTED{}操作应用 H.235 第 1 版和 2 的数据的方式，展现大量已知的明文：首先是主控方的，而且还有一些结构的编码比特。**generalID**，即使是正在被加密，已从信令信息（如 **senderID**）中的非加密部分被得知。相信这样的已知明文的存在以这样一种方式，即攻击者可以通过“强力”更容易地攻击对话，强烈地削弱了安全方案，对于有较短块尺寸的块密码，如 DES-56 或 RC2 兼容的，更是如此。

更进一步地，H.235 的第 2 版必须能够传输额外的密钥资料：

- 补白密钥到对等方的安全传输。这样的补白密钥引入用于增强型的 OFB 模式，见 8.4。

H.235 第 3 版扩展了具有 **secureSharedSecret** 的 **H235Key**，它包含具有下列参数的 **V3KeySyncMaterial**：

如果可以获得的话，**generalID** 包含起始发送者的端点标识符，否则这一字节保留不使用。

algorithmOID 指示采用的加密算法和操作模式。

paramS 包含初始化的值，它应用于传送的密钥的加密。

注 1 — **paramS** 内的 IV 不应与不被信令控制的每个 RTP 分组 IV 混淆。**ClearSalt** 任选地包含用于对话密钥加密的未加密的补白密钥（如 EOFB）。

encryptedSessionKey 包含加密的原始对话密钥的密文。

encryptedSaltingKey 包含加密的原始媒体补白密钥的密文。补白密钥对于增强型的 OFB 模式是必需的。

clearSaltingKey 可包含未加密的原始补白密钥。实施必须确定 **encryptedSaltingKey** 和 **clearSaltingKey** 不得同时使用。

paramSsalt 包含加密的补白密钥的初始值。**ClearSalt** 任选地包含一个用于补白密钥加密的未加密的补白密钥（如 EOFB）。

注 2 — **generalID**、**algorithmOID** 和 **paramS** 总是在明文中发送，然而 **encryptedSessionKey** 和 **encryptedSaltingKey** 包含加密的密钥资料的密文。

主控方依据协商的终接性能生成密钥，使用 **V3KeySyncMaterial** 将密钥发送给对等端点。因此，当存在时，**V3KeySyncMaterial** 必须由中间网守未加改变地前向发送。

H.235 第 3 版或更高版本端点应总是使用 **H235Key** 内的 **secureSharedSecret**，但是取决于 8.2 的逻辑信令规程的结果，使用指示第 3 版 **ClearToken**，可使用用于与 H.235 第 1 版或第 2 版后向兼容的 **sharedSecret**。

8.4 增强型OFB模式

OFB 模式（ISO/IEC 10116）定义了一个操作模式，它采用使用块加密算法的流密码的操作模式。OFB 模式提供：

- 通过减少加密处理延迟改进性能；
- 不完整块的较容易和较少复杂性处理；
- 对比特误差的好的误差弹性。

增强型 OFB 模式是稍微修改了的 OFB 模式，被称为“增强型输出反馈模式”（EOFB），它具有与 OFB 一样的特征，还增加了：

1） 除了加密密钥 KE 外还使用了一个补白密钥 KS；和

2） 引入了固定的分组指标。

与反馈消息做异或操作的额外秘密的密钥 KS 的使用产出对已知明文分析的另外的安全。这是一个其他标准操作（如 CBC、FB 等）模式不能提供的主要的安全性收益。EOFB 模式的使用因此对高冗余度明文和已知明文分下的增加的安全性强度。

定义 EOFB 为 $C_i = P_i \oplus S_i$ with $S_i = E_{KE}（KS \oplus S_{i-1}）$，其中 $i = 1 \ldots n$，$S_0 = IV$，C_i I 是第 I 个密文块，P_i 是第 I 个明文块，S_i 是第 I 个密钥串块，KE 加密密钥和⊕ bitwise XOR。EOFB 在图 I.6 中阐述。

EOFB 也可以标准 OFB 模式运作，使 EOFB 与 OFB 后向兼容。在期望与标准 OFB 后向兼容的那些情况下，补白密钥 KS 必须设置全 0 或平等地在 **V3KeySyncMateria** 内让 **encryptedSaltingKey** 为空。但是，强烈建议当加密 RTP 有效载荷具有较短块尺寸（DES-56 或 RC2 兼容的）的块密码的那些情况下，使用实际的补白密钥。

在已经处理了最多 2^{48} 个分组之后，必须使用一个新的对话加密密钥 KE 和一个新的补白密钥 KS，否则会发生加密串的重复使用，从而危及安全性。

第 11 节为 DES-56-EOFB、RC2 兼容的 EOFB、3-DES-EOFB 和 AES-EOFB 定义了对象标识符。

8.5 密钥管理

符合本建议书的端点应依据 7.6.1 使用快速连接规程。如果快速起动不适用，则本建议书必须使用 H.245 隧道传送以安全化 H.245 呼叫控制消息。快速连接规程允许确立一个或两个单向逻辑信道。对于作为主密钥动作的通用共享秘密（共享的 DH 秘密）的分配和加密密钥的安全分配来说，快速起动程序关心安全性能的协商。

表 4 提供分配给各种加密算法的 OID 以及它们与 Diffie-Hellman 组的分配的 OID 的关联。通过一个 OID 识别 3 个 DH 群：

- “DHdummy”：无论何时，只要设计可输出的（512 比特）安全性或使用任何非标准化的 DH 群，应采用这个 DH 群的例子。

  注 1 — 未定义特殊的 DH 群；OID 涉及任何非标准化的组。

- 对于 RC2 兼容的（“X”）的对话密钥的分配或对于 DES-56 比特加密算法（“Y”），必须用 512 比特 DH 群的例子来生成一个主密钥。

- “DH1024”：当关心高（1024 比特）安全性时，这个 DH 群适用。OID 涉及一个标准化、固定的 DH 群。对于三倍 DES（“Z”）加密算法的对话密钥的分配来说，必须用这一 DH 群来生成一个主密钥。

- “DH1536”：为具有超过 1024 比特 DH 群的安全性的很高安全要求的第 3 版提供这一 DH 群。OID 涉及一个固定的 DH 群。对于三倍 DES（“Z”，“Z1”）加密算法的对话密钥或 AES-128（“Z2”，“Z3”）加密算法的分配来说，必须用这一 DH 群来生成一个主密钥。

建议采用定义的 1024 或任选采用 1536 比特 DH 群，除非其他安全性需要会优先使用其他 Diffie-Hellman 参数。更进一步地，建议考虑使用标识 DH 群的定义的 OID，见 7.8。不过，应准备好实施以获得 DH 群参数，字面上无需 OID 指示。在这一情况下，实施应确定正确的 DH 群正按照表 4 传送。

端点可使用非标准化的 DH 群参数。使用 OID“DHdummy”应指示这样的非标准化 DH 群。有待被叫方决定是否接受这样的 DH 群。

注 2 — DH 群的选择不排除协商实际的媒体加密算法的需要。这必须与 H.245 终端性能协商规程一起完成。

注 3 — 在连接建立期间（SETUP-to-CONNECT），加密 algorithmOID 的使用不得用来指示 Diffie-Hellman 例子。

表 4/H.235.6－Diffie-Hellman群

加密算法OID	DH-OID	D-H群描述
“X”，“X1”（RC2 兼容的“Y”，“Y1”（DES）	“DHdummy”	Mod-P，任意适当的 512 比特基集
“Z”，“Z1”（三倍 DES），“Z2”，“Z3”（AES）	“DH1024”	Mod-P，1024 比特基集 Prime = $2^{1024} – 2^{960} – 1 + 2^{64} \times \{ [2^{894}$ pi] + 129093 } =（179769313486231590770839156793787453197860296048756011706444 42368419718021615851936894783379586492554150218056548598050 3 64644054819923910005079287700335581663922955313623907650873 5 75991482257486257500742530207744771258955095793778424442426 61733472762929938766870920560605027081084290769293201912819 4 467627007）$_{10}$ 生成码（注）= 2
“Z”，“Z1”（三倍 DES），“Z2”，“Z3”（AES）	“DH1536”	Mod-P，1536 比特基集 Prime = $2^{1536} – 2^{1472} – 1 + 2^{64} \times \{ [2^{1406}$ pi] + 741804 } =（241031242692103258855207602219756607485695054850245994265411 69419581088316826122288900938582613416146732271414779040121 9 65036489570505826319427307068050092230627347453410734066962 4 60145893616597740410271692494532003787294341703258437786591 9 81437631937768598695240889401955773461198435453015470437472 0 77499697637500843089263392955599688824578724129938101291302 9 45929999479263652640592846472097303849472116814344647144384 8 85209401274598442888593365268963209196339 19）$_{10}$ 生成码（注）= 2
注 — 生成码用于生成 DH 令牌。		

8.6 密钥更新和同步

对于 64 比特块密码，密钥更新率必须如此，即使用相同密钥加密的块数不多于 2^{32} 块。已经使用相同密钥加密 2^{30} 块之前，设备应更新密钥（见 9.1）。对于 128 比特块密码，密钥更新率必须如此，即使用相同密钥加密的块数不多于 2^{64} 块。已经使用相同密钥加密 2^{62} 块之前，设备应更新密钥（见 9.1）。出于其安全性方针，每当考虑必要时涉及的双方实体均可以自由变更媒体对话密钥。例如，主控方可以使用 **miscellaneousCommand** 消息的 **encryptionUpdate** 分发新的对话密钥。另一方面，通过使用 **miscellaneousCommand** 消息的 **encryptionUpdateRequest** 从属方也能够请求来自主控方的新的对话密钥变更。

MiscellaneousCommand 消息包含 **encryptionUpdate**，其中 **encryptionUpdate** 的 **encryptionSynch** 设置如下参数：

- **synchFlag**：该新的动态 RTP 有效载荷数指示密钥转换。
- **h235Key**：携带该新的加密对话密钥。这是作为一个八比特组串所传送的 H.235 ASN.1 编码的 **h235Key**。

H235Key 结构内 **sharedSecret** 字段使用以下字段：

- **algorithmOID**：对 56 比特 RC2 兼容设置为“X”，对 56 比特 DES 设置为“Y”或对 168 比特三倍 DES 设置为“Z”。这是正在加密媒体对话密钥的加密算法。

  注 1 — 对话密钥加密算法与协商的媒体加密算法相同。

- **paramS**：设置为初始值。对于 64 比特块流密码，**iv8** 掌握启动方生成的随机 64 比特块比特模式。对于 128 比特块流密码，**iv8** 掌握启动方生成的随机 128 比特块比特模式。该字段不供 CBC 方式使用并设置为空，对于对话密钥加密，这意味着 CBC-IV 必须设置为 0；对于 EOFB 模式，它必须仅用于携载。
- **encryptedData**：设置为加密的 **KeySyncMaterial** 的结果。

作为 **KeySyncMaterial** 的一部分：

- **generalID**：分发该密钥的源标识符。

  注 2 — 本建议书假定每个端点已用一个网守注册，获得一个可以在 **generalID** 内传送的端点标识符。本建议书不支持无网守的情况；这有待进一步研究。

- **KeyMaterial**：设置为新的对话密钥。对于 DES 和 RC2 兼容算法此为 56 比特密钥，对于三倍 DES 算法此为 168 比特密钥。主控方必须生成新的对话密钥，该密钥至少满足以下的安全准则：不是弱或半弱的 DES 密钥，并且使用足够安全的随机源。

MiscellaneousCommand 消息包含 **encryptionUpdateRequest** 字段，该字段包含 **keyProtectionMethod** 其中该标志 **sharedSecret** 被设置为 TRUE。

注 3 — 由于密钥更新和同步依赖于快速连接期间非级联的 H.245 消息，因此它要求 H.245 隧道传送用于安全的 H.323 实体。

媒体对话密钥不会永远存在。在某些时间点上，每个对话密钥期满。那么应使用一个新的对话密钥来保护正在进行的安全对话。在会议环境下，当组成员加入或离开一个安全的会议时，应定义和分配一个新的组对话密钥，从而防止它们访问过去或将来的数据。

- 基于有效载荷类型的密钥更新和同步定义了一个用于新的对话密钥的新的动态有效载荷类型；见 8.6.1、8.6.2 和 8.6.3。

对于密钥更新，本建议书提供了一个未确认的握手，它也应用于 H.235 第 1 版和第 2 版端点，也是一个用于 H.235 第 3 版和更高版本端点的健壮的、未确认的握手。

8.6.1 未确认的密钥更新

图 4 示出了用于对话密钥分配/密钥更新的未确认的握手。如果从属方期望一个更新的对话密钥，从属方可通过发送一个 **encryptionUpdateRequest** 给主控方向其请求一个新的对话密钥。主控方必须在 **EncryptionUpdate** 消息中发送一个（有或没有之前的来自从属方的 **encryptionUpdateRequest** 的）新的对话密钥给从属方。

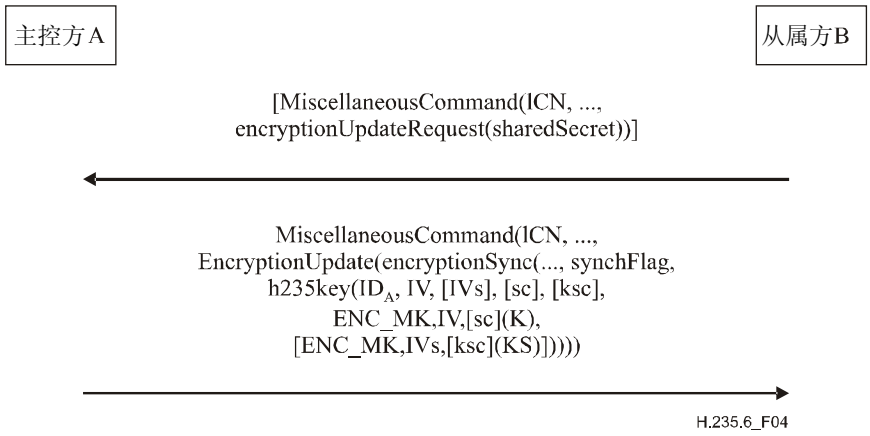


图 4/H.235.6－从主控方到从属方的未确认的对话密钥分配/密钥更新

其中：

lCN	是逻辑信道数；
synchFlag	是新的动态 RTP 有效载荷数；
ID_A	是源的 **generalID**；
IV	是对话密钥加密的初始值/矢量；
IVs	是多个补白密钥加密的初始值/矢量；
ENC_MK，IV，sc（K）	意味着使用密钥 *M*、初始矢量 *IV* [和补白密钥 *sc*，仅用于 EOFB]的明文 *K* 加密；
KS	是媒体的补白密钥（仅用于 EOFB 模式）；
K	是明文对话密钥；
sc	是未加密的补白密钥，当 EOFB 正用于加密对话密钥时；
ksc	是未加密的补白密钥，当 EOFB 正用于加密补白密钥时；
s2M/m2S	是 **direction** 标记（仅用于 H.235 v3 和更高版本）（s2m =从属方到主控方，m2s = 主控方到从属方）；
[]	代表任选的部分。

在下列各节中描述的密钥更新方法可以配置 EOFB 加密模式来保护发送的密钥资料。为了以与媒体有效载荷保护密钥资料相同的方式配置 EOFB 模式来保护密钥资料，使用了额外的补白密钥（sc 或 ksc）。

8.6.2 改进的密钥更新

H.235 第 3 版和更高版本端点必须执行明确的/含糊的确认的密钥更新程序。这提供了可靠的密钥更新方法，该方法基于由前基于 H.235v3 版本提供的未答复的密钥更新方法。这样的规程的性能必须遵循 8.2 使用第 3 版的特征标识符协商。

图 5 示出由从属方拥有的逻辑信道的密钥更新程序。在从属方初始化密钥更新和向主控方请求一个新的对话密钥的情况下，从属方必须向主控方发送一个 **MiscellaneousCommand**，其中 **logicalChannelNumber** 必须包含逻辑信道数（如由从属方所定义的），**sharedSecret** 必须设置为 TRUE，**direction** 标记必须设置为 **slaveToMaster**，必须在 **EncryptionUpdateRequest** 的 **synchFlag** 中请求动态有效载荷数。否则，如果主控方初始化密钥更新，则这一 **EncryptionUpdateRequest** 不得被发送。

主控方响应从属方的请求或为其自己的利益，必须发出一个 **EncryptionUpdateCommand**，其中 **logicalChannelNumber** 必须包含逻辑信道数，**direction** 必须在 **MiscellaneousCommand** 内设置为 **slaveToMaster**，**encryptionSync** 内的 **synchFlag** 反映新的动态有效载荷数。

h235key 必须传送新的对话密钥。**h235key** 必须在 **generalID** 内包含主控方的标识符，在 **paramS** 中包含应用的初始化矢量 *IV*。加密的媒体对话密钥必须在 **encryptedSessionKey** 中发送，其中加密功能必须将主控对话密钥和 **paramS** 中的初始值应用到对话密钥 *K*。对于 EOFB，在 **paramS**（*sc*）内的 **ClearSalt** 中发送一个未加密的补白密钥。**encryptedSaltingKey** 必须发送加密的媒体补白密钥，其中加密功能必须将主控对话密钥和初始值 **paramSsaltIV** 应用到补白密钥 *KS*。对于 EOFB，未加密的补白密钥（*ksc*）在 **paramSsalt** 内的 **ClearSalt** 中发送。**clearSaltingKey** 可包含一个未加密的媒体补白密钥，在这一情况下，**encryptedSaltingKey** 必须保持空，反之亦然。未加密补白密钥的传送必须仅当不经受安全性时完成，在其他情况下，建议媒体补白密钥加密。

主控方必须准备好接收加密媒体，假借新的对话密钥提交 **EncryptionUpdateCommand** 但是应继续使用旧的对话密钥直至接收到 **EncryptionUpdateAck**。主控方可采用以 **encryptionUpdateAck** 的接收开始的新的对话，而从属方可采用以 **EncryptionUpdateCommand** 的接收开始的新的对话。

注 1 — 主控方可以为从属方选择任何动态有效载荷类型值，因为有效载荷类型正受媒体信道的端口的约束。

注 2 — 不需要从属方明确地知道接收到新的密钥。当接收到在新的有效载荷类型下加密的媒体时，主控方能够推论出由从属方发送的密钥的接收。

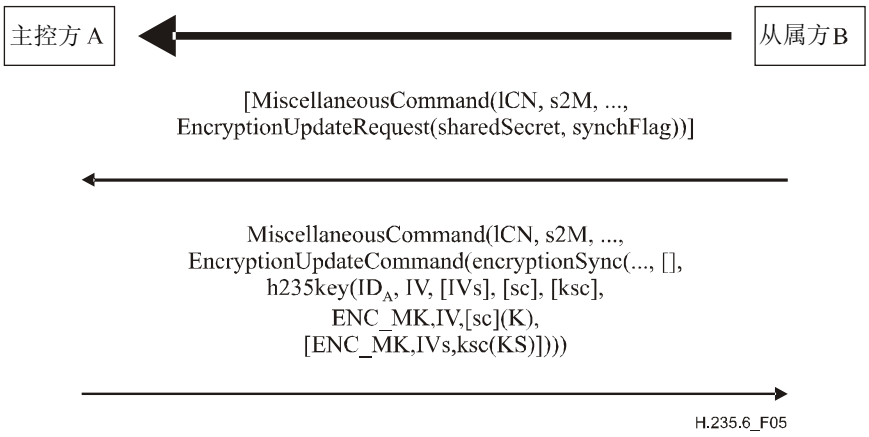


图 5/H.235.6－从属方逻辑信道上的对话密钥更新

图 6 示出主控方所拥有的逻辑信道的密钥更新规程。在从属方初始化密钥更新，请求来自主控方的新的对话密钥的情况下，从属方必须发送一个 **MiscellaneousCommand** 给主控方，其中 **logicalChannelNumber** 必须包含逻辑信道数（如由主控方所定义的），**sharedSecret** 必须设置为 TRUE，**direction** 标记必须设置为 **masterToSlave**。否则，如果主控方初始化密钥更新，则不得发送这个 **EncryptionUpdateRequest** 消息。

主控方响应从属方的请求或出于其自己的目的，必须发送一个 **EncryptionUpdateCommand**，其中 **logicalChannelNumber** 必须包含逻辑信道数，**direction** 必须设置为 **masterToSlave**，**encryptionSync** 必须提供具有动态有效载荷数的 **synchFlag**。**h235key** 必须传送新的对话密钥。**h235key** 必须在 **generalID** 内包含主控方的标识符，在 **paramS** 中包含应用的初始化矢量 *IV*。加密的媒体对话密钥必须在 **encryptedSessionKey** 中发送，其中加密功能必须将主控对话密钥和 **paramS** 中的初始值应用到对话密钥 *K*。对于 EOFB，在 **paramS**（*sc*）内的 **ClearSalt** 中发送一个未加密的补白密钥。**encryptedSaltingKey** 必须发送加密的媒体补白密钥，其中加密功能必须将主控对话密钥和初始值 **paramSsaltIV** 应用到补白密钥 *KS*。对于 EOFB，未加密的补白密钥（*ksc*）在 **paramSsalt** 内的 **ClearSalt** 中发送。**clearSaltingKey** 可包含一个未加密的媒体补白密钥，在这一情况下，**encryptedSaltingKey** 必须保持空，反之亦然。未加密补白密钥的传送必须仅当不经受安全性时完成，在其他情况下，建议媒体补白密钥加密。

从属方必须通过用 **MiscellaneousCommand** 响应知道接收到新的对话密钥，其中 **logicalChannel Number** 必须包含逻辑信道数，**encryptionUpdateAck** 必须在 **synchFlag** 中反映新的动态有效载荷数。

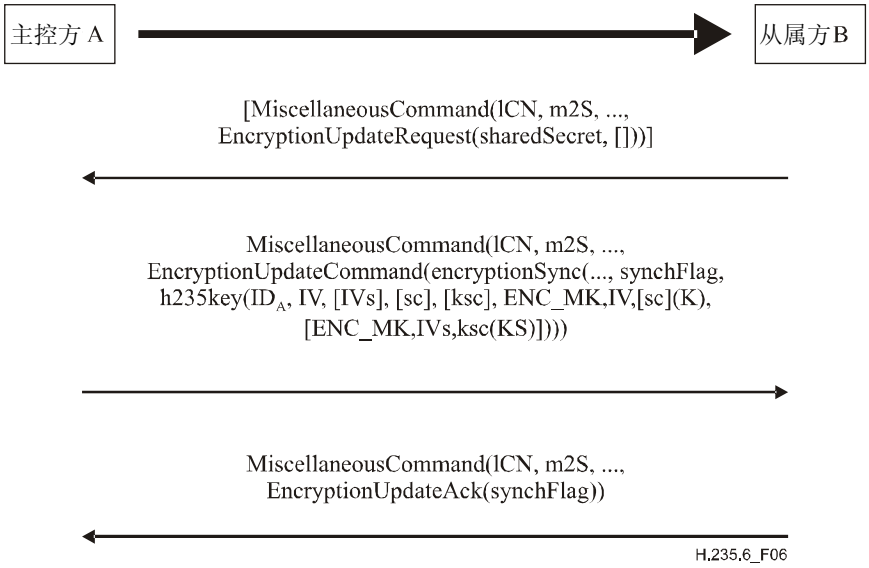


图 6/H.235.6－主控方逻辑信道上的对话密钥更新

8.6.3 基于有效载荷类型的密钥更新和同步

初始化加密密钥与 **synchFlag**（经由 ITU-T H.245 建议书中的 **EncryptionSync**）中的动态有效载荷数一起由主控方提出。媒体流的接收者必须依据接收的 RTP 头中的有效载荷数开始初始化密钥的使用。

如果协商的逻辑信道仅传送单一的有效载荷类型，则 **synchFlag** 的值可代替 RTP 头中协商的有效载荷类型。另一方面，如果协商的逻辑信道可传送不止一个有效载荷类型（即使只在不同的 RTP 分组中），RTP 分组必须如 RFC 2198 中所描述的那样格式化，它具有作为封装有效载荷类型的 **synchFlag** 值，以及如 RFC 2198 所规定的在额外头块中的实际有效载荷类型。

新的密钥可由主控方端点在任何时间分配。较新的密钥与媒体流的同步必须由有效载荷类型的变化指示一个新的动态值。

注 — 规定的值无关紧要，只要对于每一个分配的新密钥都改变。

8.7 非终端交互

8.7.1 网关

如 6.6/H.235.1 中所阐述的，H.323 网关应被认为是可信单元。这包括协议网关（H.323-H.320 等）和安全性网关（代理服务器/防火墙）。该媒体保密可以在该通信端点和网关设备之间确保；但在该网关远端所发生的应被默认为是非安全的。

8.7.2 新密钥

为了把某个参与方逐出会议由 MC 完成 8.5/H.323 中概述的规程。主控方可以生成逻辑信道的新的加密密钥（并且不向逐出的参与方分发）；这可用于防止逐出的参与方监视媒体流。

8.7.3 H.323可信单元

通常，就控制信道的保密而言，MC（U）、网关及网守（只要实施网守选路模型）是可信的。若该连接建立信道（H.225.0）是安全的并且通过网守选路，则它肯定也是可信的。若任何这些 H.323 成分务必在媒体流上操作（如混合，代码转换），则根据定义，对媒体保密而言，它们也必须是可信的。

防火墙代理服务器（尽管不是 H.323 特定单元）也可能是可信的，因为它们终止连接，并且可以妥善处理消息和媒体流。

8.8 多点规程

8.8.1 认证

在端点和 MC（U）之间认证必须采用与端到端会议中的同样方式发生。MC（U）必须制定有关认证级别和严格程度的策略。如 6.6/H.235.0 中所阐述的，MC（U）是可信的；会议中现存端点可以由 MC（U）所使用的认证级别来限制。新的 **ConferenceRequest**/**ConferenceResponse** 指令允许端点从 MC（U）获得会议其他参与方的证书。如 H.245 规程所概述的，多点会议中的端点可以经由 MC 请求其他端点的证书，但或许不能在 H.245 信道内实施直接的密码认证。

8.8.2 保密

MC（U）必须力争所有的主/从交换并因此向多点会议的参与方提供加密密钥。对于公共对话内（假定组播）单个信源的保密可以采用私钥或公钥来实现。这两种方式可以由 MC（U）任意选择，并且不得受任何特殊端点的控制，采用 MC（U）策略所允许的方式除外。换言之，公钥可以用于由不同信源所开放的多路逻辑信道。

9 媒体流加密规程

媒体流必须使用 H.245 信道采用的算法和密钥编码。图 7 和图 8 显示一般流程。注意 SDU 加密后，传输头附着到该传输 SDU 上。不透明部分指示保密。当传输方接收新的密钥并用于加密时，该 SDU 头必须以某种方式向接收者表明目前正在使用新密钥。例如，ITU-T H.323 建议书中，该 RTP 头（SDU）会通过改变其有效载荷类型来指示到新密钥的切换。

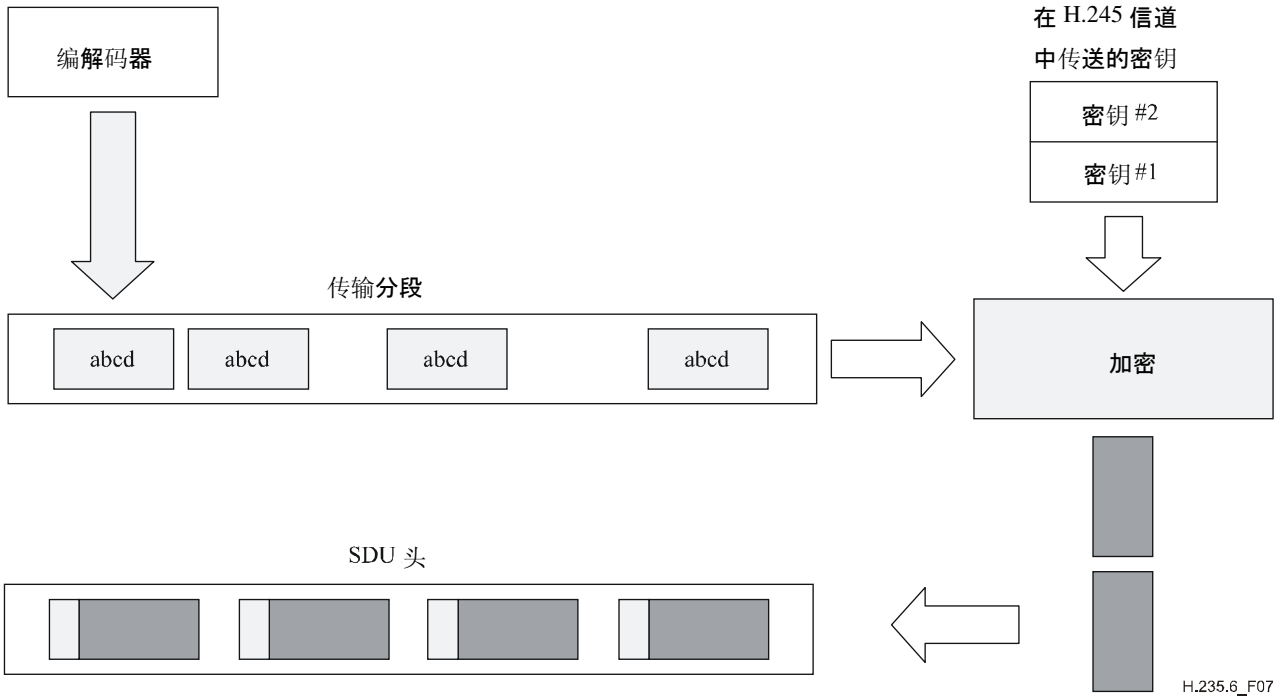


图 7/H.235.6—媒体加密

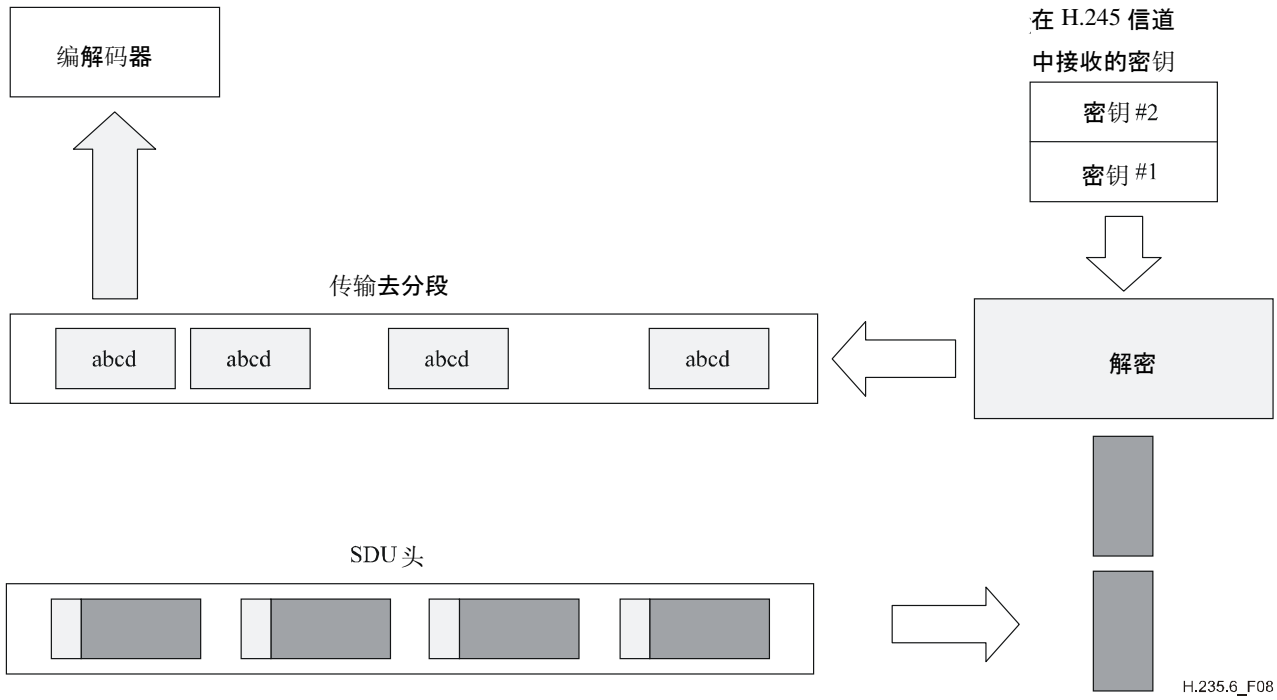


图 8/H.235.6—媒体解密

9.1 媒体对话密钥

encryptionUpdate 中所包含的是 **h235Key**（**h235** 密钥）。该 **h235Key** 在 H.235 ASN.1 生成树的语境内采用 ASN.1 编码，并作为相对于 H.245 不透明的八比特组信息串传送。密钥在两个端点之间传送时，可以采用以下三种可能的机制之一加以保护。

- 若 H.245 信道是安全的，则不得对密钥资料采取任何附加的保护措施。相对于该字段密钥“以透明方式”传送；利用 **secureChannel** 的 ASN.1 选择。
- 从整体来看，若秘密密钥和算法已在整个 H.245 信道外部（即，H.323 外部或在 **h235Control** 逻辑信道上）建立，则使用共享秘密对密钥资料加密；这里包含合成的加密密钥。在此情形下，使用 **sharedSecret** 的 ASN.1 选择。
- H.245 信道非安全时可以使用证书，而且除安全 H.245 信道之外证书均可以使用。采用证书时，密钥资料使用该证书的公钥及 ASN.1 结构的 **certProtectedKey** 加密。

在会议中的任何时间，接收者（或传输方）可以请求新的密钥（**encryptionUpdateRequest**）。这样做的一个理由是怀疑是否某个逻辑信道已经失步。接收该请求的主控方必须生成新的密钥以响应该指令。主控方也可异步地决定分配新密钥。只要如此它就必须使用 **encryptionUpdate** 消息。

接收 **encryptionUpdateRequest** 后，主控方必须发送出 **encryptionUpdate** 消息。若会议为多点会议，则 MC（也为主控方）应在它给传输方发送该密钥之前向所有的接收者分发新的密钥。接收该消息后，逻辑信道上的该数据传输方务必尽可能早地采用新的密钥。

传输方（假定它不是主控方）也可请求新的密钥。若该传输方为多点会议的一部分，则该规程必须如下：

- 传输方必须向 MC（主控方）发送 **encryptionUpdateRequest**。
- MC 应生成新的密钥并且向除该传输方之外的所有会议参与方发送 **encryptionUpdate** 消息。
- 向所有其他参与方分发新的密钥之后，MC 必须向该传输方发送 **encryptionUpdate** 消息。然后该传输方必须采用新的密钥。

9.2 媒体反滥发

RTP 媒体流的接收者可能希望在公开的 RTP/UDP 端口上反击拒绝服务和扩散式攻击。已经具备反滥发能力的接收者可以快速地确定获得的 RTP 分组是否源出于非授权信息源并抛弃它。

在设置反滥发能力时，应表明：

- 或者对无任何媒体加密的明文媒体数据使用反滥发机制（见以下情况 1）；
- 或者当 **EncryptionCapability** 表征该加密算法时，与加密媒体数据结合在一起使用反滥发机制（见以下情况 2）。

通过计算的消息认证码（MAC），以上两种选项均在所选字段上提供轻便式的 **RTP packet authentication（RTP 分组认证）**。该 MAC 可以使用 9.2.1 子节中定义的对象标识符计算。密码算法是根据：

- 加密算法（例如，MAC 方式的 DES，见 ISO/IEC 9797-1 和 9797-2）。DES-MAC 使用 OID“S”来指示，而 triple-DES-MAC 使用 OID“O”来指示。
- 或使用密码单向函数（例如 SHA1）。将使用的 OID 为“M”。

MAC 算法在 **antiSpamAlgorithm** 的对象标识符中指定。**algorithmOID** 也隐含地指定 MAC 的长度；例如对于 DES MAC，1 块＝64 比特。为了节省带宽，尽管牺牲某些安全性该 MAC 可以有限截断；例如截断成 32 比特的 MAC，然后它请求不同的对象标识符。反滥发方法与任何附加的有效载荷加密无关（见以下的情况 1 和 2）。

反滥发使用以下 RTP 分组格式（见图 9），其中该 RTP 填充序列解释如下（见 RFC 3550 第 5 节）。

- RTP 头中 P 比特必须设置为 1。
- 填充字节必须附加在该有效载荷的末尾，具有以下含义：

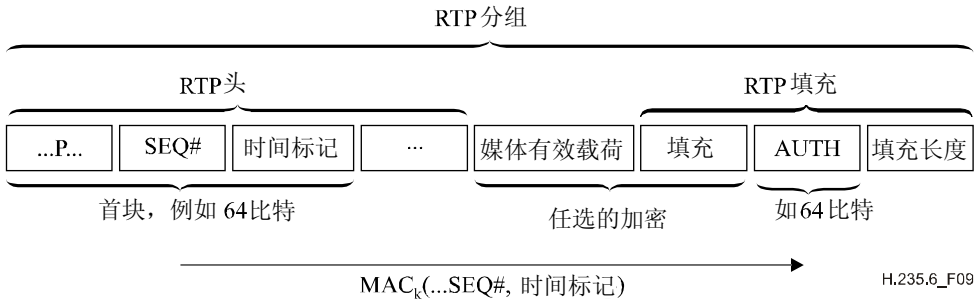


图 9/H.235.6－媒体反滥发的RTP分组格式

注 1 － 若不使用反滥发，则这个 AUTH 和填充长度字段也不使用，并采用常规的 RTP 分组格式。

1） *仅反滥发的情形：*

当媒体数据未加密且该填充字段保留为空时此情况适用。RTP 填充字段的最后一个八比特组包含一项计数，表明在 RTP 分组的结尾多少填充八比特组应予忽略。其他的填充字节携载 MAC。计算 MAC 必须使用 **antiSpamAlgorithm** 的协商 MAC 算法并采用对称秘密在 RTP 头的第一个密码块上（包括可变时间标记与序列号）计算。静态的或手工设置的共享秘密或动态协商的共享秘密 k 可依照 H.235.0 的规程使用。对于更大的块尺寸（大于 64 比特），必须去掉该 RTP 头的足够多的附加比特，甚至是第一个媒体有效载荷。

作为 MAC 计算的密钥，推荐使用从 H.235 媒体对话密钥分配中所获取的密钥；尽管采用的对话密钥不供有效载荷加密使用。伴随密钥建立（见附件 J/H.323）或手工加锁的安全快速连接可供密钥管理使用。在 RTP 填充 AUTH 字段中，发送者如上所述计算 MAC 并在该 MAC 字段中包含此结果。发送者和接收者通过 **antiSpamAlgorithm** 均知道 AUTH 字段的尺寸以及 MAC 的长度。

接收端一方的 MAC 核实应尽可能早地实施，只要可能应早在 RTP 堆栈的时候或至少在有效载荷解密或解压之前完成。接收者首先采用与发送者同样的方法再次计算 MAC，并将所计算的 MAC 与 RTP 填充中所交付的 MAC 相比较。若 MAC 失配，则 RTP 头在传输中被窜改，或由不拥有该密钥的非授权实体发送。这样误认证的 RTP 分组务必抛弃，该事件可以登录；这可能表明一次拒绝服务攻击尝试。否则，该认证的 RTP 分组可进一步处理，去除 RTP 填充并将有效载荷通过编译码器馈入。

注 2 — 采用 DES 加密的轻便式 MAC 计算/核实仅只涉及单一的加密操作；可供选择的，SHA1 MAC 在固定长分组的短部分上计算，这样加密操作绝对消耗极少的处理资源。

2） *反滥发方法和有效载荷加密的情形：*

当媒体数据加密并且反滥发方法被激活时此情况适用。当有效载荷没有落在偶数块边界上时，一些附加的填充字节不得不附加在该 MAC 之前的有效载荷上。媒体有效载荷加密依照本节的规程。

EncryptionCapability 规定有效载荷加密算法而 **antiSpamAlgorithm** 定义反滥发方法。出于安全性原因，媒体加密和 MAC 必须使用不同的对话密钥。MAC 密钥 *k* 由馈入加密密钥 *K* 经由该 SHA1 单向散列函数来计算；

k = SHA1（*K*）；必须从散列的结果中依网络字节顺序取出足够多的比特。当 **antiSpamAlgorithm** 指示加密算法时，该集成的比特必须构成正确的加密密钥；例如设置 DES 奇偶校验比特。

接收者成功核实 RTP 分组的认证过程后，该有效载荷被解密并抛弃 RTP 填充。通用规程依照以上情形 1。

9.2.1 对象标识符一览

表 5 列出所有引用的 OID。

表 5/H.235.6－供反滥发所使用的对象标识符

对象标识符参考符	对象标识符值	描　　述
“M”	{itu-t（0）recommendation（0）h（8）235 version（0）2 8}	使用 HMAC-SHA1-96 的反滥发
“N”	{iso（1），identified-organization（3），oiw（14），secsig（3），algorithm（2），desMAC（10）}	伴随 64 比特 MAC 使用 DES（56 比特）MAC 的反滥发（见 ISO/IEC 9797-1 和 9797-2）
“O”	{iso（1）identified-organization（3）oiw（14）secsig（3）algorithm（2）desEDE（17）}	使用三倍 DES（168 比特）MAC 的反滥发（见 ISO/IEC 9797-1 和 9797-2）

9.3 RTP/RTCP问题

在 RTP 流上使用加密应遵循[RTP]所引用的文献中推荐的通常的方法论。该媒体的加密务必单独地按逐个分组的形式进行。

该 RTP 头（包括有效载荷头）不加密。新密钥与加密文本的同步依据动态有效载荷类型。

对于视频/音频编解码器而言，必须加密包括任何视频/音频编解码器头的完整的视频/音频编解码器有效载荷。新密钥的同步和加密的报文是基于动态有效载荷类型（见 8.6.3）。

假定仅只对每个 RTP 分组中的有效载荷使用加密，RTP 头以透明形式保持。假定所有 RTP 分组务必是整八比特组的整数倍。RTP 分组如何在传输层或网络层被封装与本建议书无关。除了将分组填充成适当的整数倍八比特组外，所有方式均务必容许丢失（或乱序）分组。

基于分组可能会丢失的事实，解密该媒体流务必是无状态的；每个分组应依据其自身特点解密。操作块算法方式的两个要求如下：

9.3.1 初始化矢量

大多数块方式包含某些“链接”；每个加密周期以某种方式与先前周期的输出有关。因此在分组起始为了开始加密进程务必提供某些初始块值[通常称为初始化矢量（IV）]。与每个加密周期处理多少个流字节无关，IV 的长度始终等于块长度。除了电子码书（ECB）方式外，所有方式均需要一个 IV。在所有情形中，IV 务必通过来自（Seq# +时间标记）的前 B 个字节来构造（其中 B 为块尺寸）。该模式应不断重复直至生成足够多的八比特组时为止。应予注意以此方式生成的 IV 对于某些特殊算法而言可能产生被认为“弱”的密钥模式。

9.3.1.1 CBC初始化矢量

当在 CBC 模式中使用块密码来加密 RTP 分组有效载荷时，请求初始化矢量（IV）。IV 的尺寸与特殊的块密码的块尺寸一样。例如，DES 和 3-DES 的 IV 尺寸是 64 比特，而 AES 的 IV 尺寸则是 128 比特。

对于 CBC 的情况下，IV 必须从以下的第一个 *B*（其中 *B* 是块尺寸）八比特组中构建：与时间标记连接的 Seq#。这形成了模式 *SSTTTT*，其中 *SS* 是 2 八比特组 RTP Seq# ，*TTTT* 是 4 八比特组 RTP 时间标记。这一模式必须重复直至已经生成 *B* 八比特组，根据需要截短。例如，64 和 128 比特的 IV 会分别包含 *SSTTTTSS* 和 *SSTTTTSSTTTTSSTT*。应注意在这一方法下生成的 IV 可创造出一个密钥模式，这一模式被认为是“弱”的特定算法。

9.3.1.2 EOFB初始化矢量

在 EOFB 模式下每个 RTP 分组的惟一初始化矢量 IV 必须按照以下的规定计算：

每个在[SRTP]中定义的 RTP 分组与固有的 48 比特分组指标 *i* 关联，其中 $i = 2^{16} \times \text{ROC} + \text{SEQ}$，SEQ 是从 RTP 头中取出的序列号，而 ROC 是 32 比特转滚计数器，它计算序列号 SEQ 多久一次已经包装到 65535。

最初，转滚计数器必须设置为 0。每次 SEQ 包装到模 2^{16}，发送者必须将 ROC 增加一个模 2^{32}。

按照（$i \parallel T$ [$\parallel i \parallel T \parallel \ldots$]）计算初始化 IV，其中 48 比特指标 *i* 和 32 比特时间标记 *T* 是从 RTP 头中取出，该头串联数次直至块尺寸被填满。|| 符号代表串联。

注 — 在每个对等边本地地保持和计算轮滚计数器和 IV，且不发送。

当面对丢失或重新排序的分组时，接收者应如下计算估计的指标 *i*：

$i = 2^{16} \times v + \text{SEQ}$，其中 *v* 从模 2^{32} 的 {ROC−1， ROC， ROC+1}中选出，以便于 *v* 与（在 2^{48} 意义上）值 $2^{16} \times \text{ROC} + s_l$ 最接近，其中 s_l 是接收者保持的序列数。分组已使用估计的指标处理后，接收者必须决定 s_l 和 ROC 是否应更新。例如，一个简单的（但不是误差稳健）方法会简单地设置 s_l 为 SEQ（如果 SEQ＞ s_l），如果使用值 $v = \text{ROC} + 1$，更新 ROC 为 *v*；更多信息也见 [SRTP]，第 3.2.1 节。

9.3.2 填充

ECB 和 CBC 方式自始至终每次处理输入流的一个块，而 CFB 和 OFB 能够处理任意数目的输入八比特组 *N*（≤*B*），建议令 *N* = *B*。

处理其有效载荷不是块整数倍的分组，以下两种方式有效：

1） ECB 和 CBC 的密文侵占；CFB 和 OFB 的零填充。

2） 以[RTP，第 5.1 节]所规定的方式填充。

[RTP]第 5.1 节中描述将有效载荷填充成块整数倍的填充方法，最后八比特组设置成填充八比特组数（包括该最后字节），并且在 RTP 头中设置 P 比特。该填充值由加密算法的通常惯例来确定。

所有 H.235 设施务必支持两种方案。使用的方案可以如下推断：若 RTP 头中设置 *P* 比特，则该分组被填充；若分组不是 *B* 的整数倍并且 *P* 比特未设置，则采用密文侵占，否则，分组为 *B* 的整数倍并且未采用填充。

9.3.3 RTCP保护

适用于 RTCP 单元的加密技术有待进一步研究。

9.3.4 安全有效载荷流

当使用基于 H.323 的网络时，例如对于在 IP 上传调制解调器，采用 H.245 信令以确立和协商话带数据信道和 RTP 实现复用有效载荷流（MPS）的分组。

对于具有单一有效载荷类型的单一媒体流或另一信道的 FEC，在 **encryptionSync** 中的动态有效载荷类型必须替代默认的有效载荷类型。

对于封装流，（即冗余编码或 RFC 2198 编码 FEC）**encryptionSync** 内的动态有效载荷类型必须替代封装有效载荷类型。

对于多个有效载荷流，**encryptionSync** 的 **syncFlag** 中的动态有效载荷类型必须置之不理，（任选地）**multiplePayloadStreamElement** 内的有效载荷类型必须替代使用。

EncryptionUpdateCommand 必须用于改进的密钥更新规程以分配新的对话密钥资料（见 8.6.2）。**MultiplePayloadStream** 仅当复用有效载荷再次使用加密密钥时使用，在这一情况下，**EncryptionSync** 内的动态有效载荷类型必须置之不理。

9.3.5 与J.170的相互作用

有待进一步研究。

9.4 外CBC方式的三倍DES

外 CBC 方式的 168 比特三倍 DES，如图 10 中所示，应在此安全概要内使用。图中，每个 k_i 涉及一个 56 比特密钥。在每个加密（E）和解密（D）块内必须使用不同的 56 比特密钥。没有一个 DES 的 64 弱密钥已知引起三倍 DES 内的任何弱点。然而，服从该概要的设施在涉及到弱 DES 密钥时应拒绝该密钥（见 RFC 2405）。

三倍 DES 的更进一步的信息可以从[Schneier]和[RFC 2405]中获得。

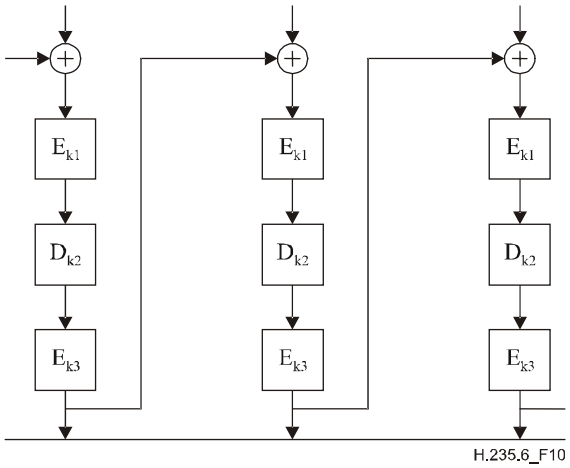


图 10/H.235.6－外CBC方式的三倍DES加密

9.5 在EOFB方式内操作的DES算法

话音可以使用在 EOFB 流密码块链接方式中操作的 DES 算法加密。EOFB 方式允许在实施中使用并联机制。当在 EOFB 方式中操作时，出于性能和安全原因，建议返回完整的密码块（即用于 DES 的完整 64 比特，例如 $n = j = 64$）。然而，由于 EOFB 不提供穿越块和比特的链接，EOFB 可能易受特定攻击的影响，视输入明文数据的统计特性而定。因此，密钥更新（见 8.6）应有规律地执行，但最近一次在初始化值卷绕之前。对于初始值的计算，见 9.3.1.2。

9.6 外EOFB方式的三倍DES

外 CBC 方式的 168 比特三倍 DES，如图 11 中所示，可在此安全概要内使用。图中，每个 k_i 涉及一个 56 比特密钥。在每个加密（E）和解密（D）块内必须使用不同的 56 比特密钥。没有一个 DES 的 64 弱密钥已知引起三倍 DES 内的任何弱点。然而，服从该概要的设施在涉及到弱 DES 密钥时应拒绝该密钥[RFC 2405]。

三倍 DES 的更进一步的信息可以从[Schneier] [RFC 2405]中获得。

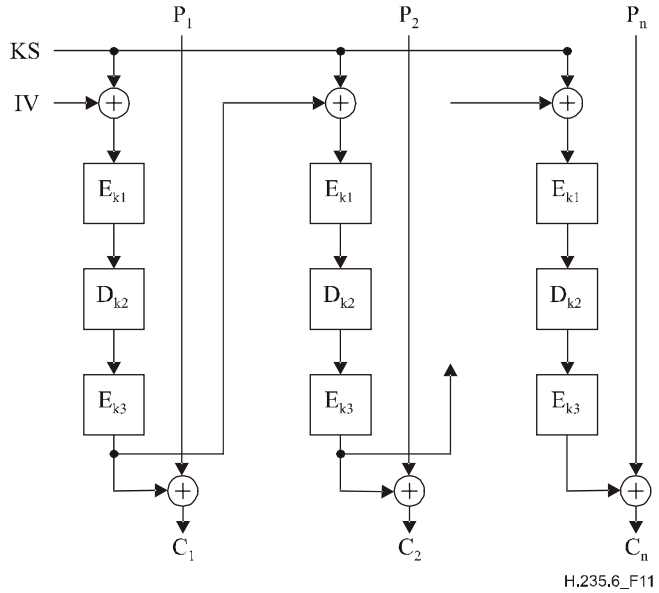


图 11/H.235.6－外EOFB方式的三倍DES加密

10 合法拦截

有待进一步研究（见 [LI]）。

11 对象标识符一览

表 6 列出所有参考的 OID（也见[OIW]和[WEBOIDs]）。包括用于 H.235v1（ITU-T H.235 建议书第 1 版）和 H.235v2（ITU-T H.235 建议书第 2 版）的对象标识符。

表 6/H.235.6－对象标识符

对象标识符参考符	对象标识符值	描　　述
"DHdummy"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 40} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 40}	明确提供非标准的 DH 组
"DH1024"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 43} {itu-t (0) recommendation (0) h (8) 235 version (0) 3 43}	1024 比特 DH 组
"DH1536"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 44}	1536 比特 DH 组
"X"	{iso(1) member-body(2) us(840) rsadsi(113549) encryptionalgorithm(3) 2}	使用 RC2-兼容（56 比特）或在 CBC 模式和 512 比特 DH 组中的 RC2-兼容的话音加密
"X1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 27}	使用 RC2-兼容（56 比特）或在 EOFB 模式和 512 比特 DH 组中的 RC2-兼容的话音加密。
"Y"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) descbc(7)}	使用在 CBC 模式和 512 比特 DH 组中的 DES（56 比特）的话音加密。

表 6/H.235.6－对象标识符

对象标识符参考符	对象标识符值	描　　述
"Y1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 28}	使用 RC2-兼容（56 比特）或在 EOFB 模式和具有 64 比特反馈的 512 比特 DH 组中的 DES（56 比特）的话音加密
"Z1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 29}	在外部 EOFB 模式和具有 64 比特反馈的 1024 比特 DH 组中使用三倍 DES（168 比特）的话音加密
"Z2"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 30}	在 EOFB 模式和 1024 比特 DH 组中使用 AES（128 比特）的话音加密
"Z3"	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) 3 nistAlgorithm(4) aes(1) cbc(2)}	在 CBC 模式和 1024 比特 DH 组中使用 AES（128 比特）的话音加密
"Z"	{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) desEDE(17)}	在外部 CBC 模式和 1024 比特 DH 组中使用三倍 DES（168 比特）的话音加密

附 录 I

H.323实施详情

I.1 密文填充方法

在[Schneier] 191 和 196 页中，存在密码报文侵占的描述。图 I.1 到图 I.5 说明该技术。

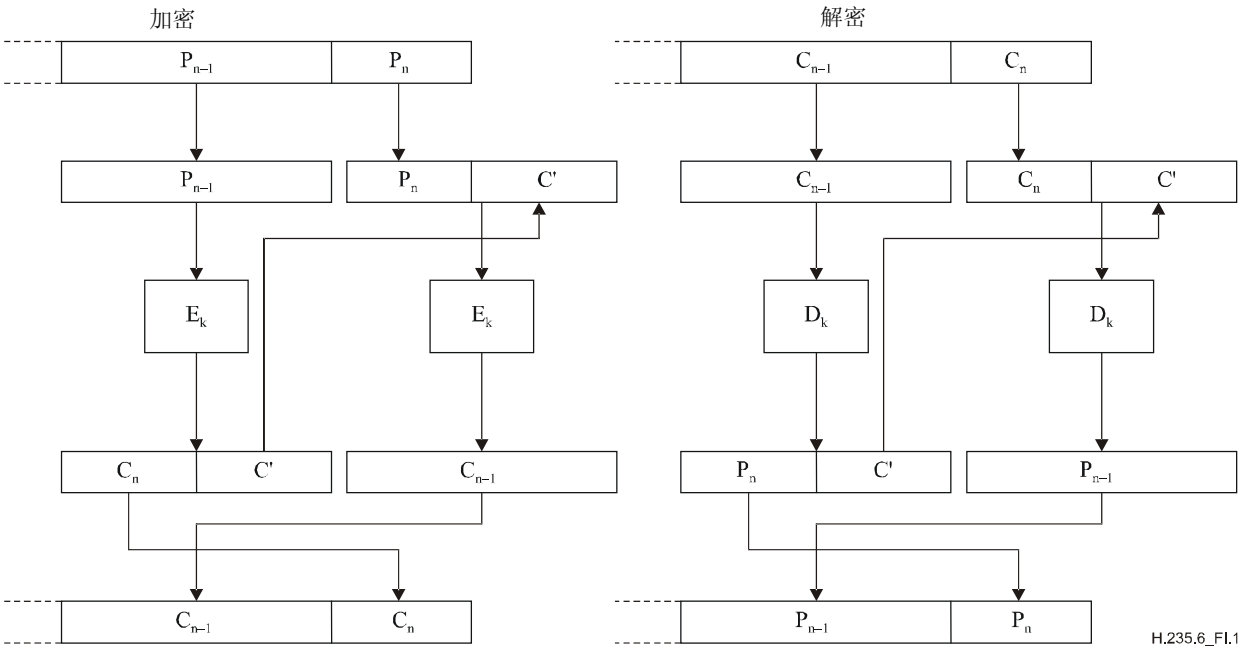


图 I.1/H.235.6－ECB方式的密文侵占

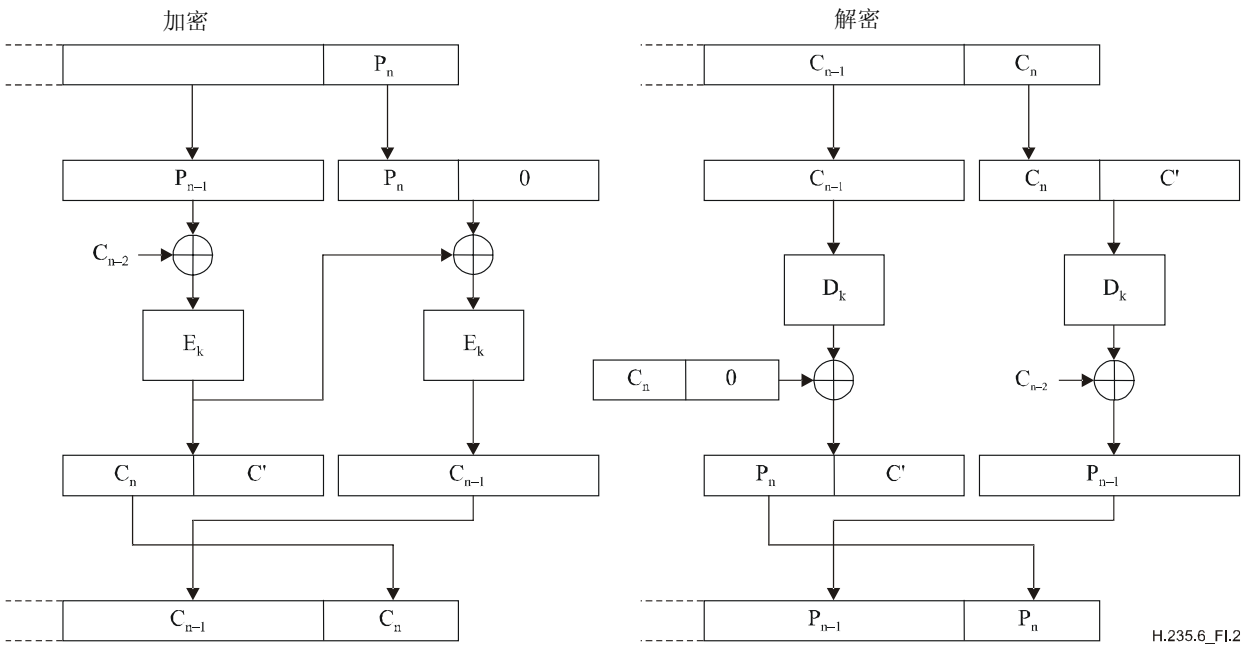


图 I.2/H.235.6－CBC方式的密文侵占

注 — ECB 或 CBC 方式的密文侵占需要有效载荷来传送至少一个完整的时钟。在 ECB 方式或 CBC 方式中实施采用密文侵占应确定有效载荷总是传送至少一个密码块，例如，通过正确地选择取样/分组化速率或选择加密算法。

在有效载荷跨越不到一个单独的块时，当密文侵占以 CBC 方式应用时，初始化矢量（IV）必须作为前一个密文块使用。

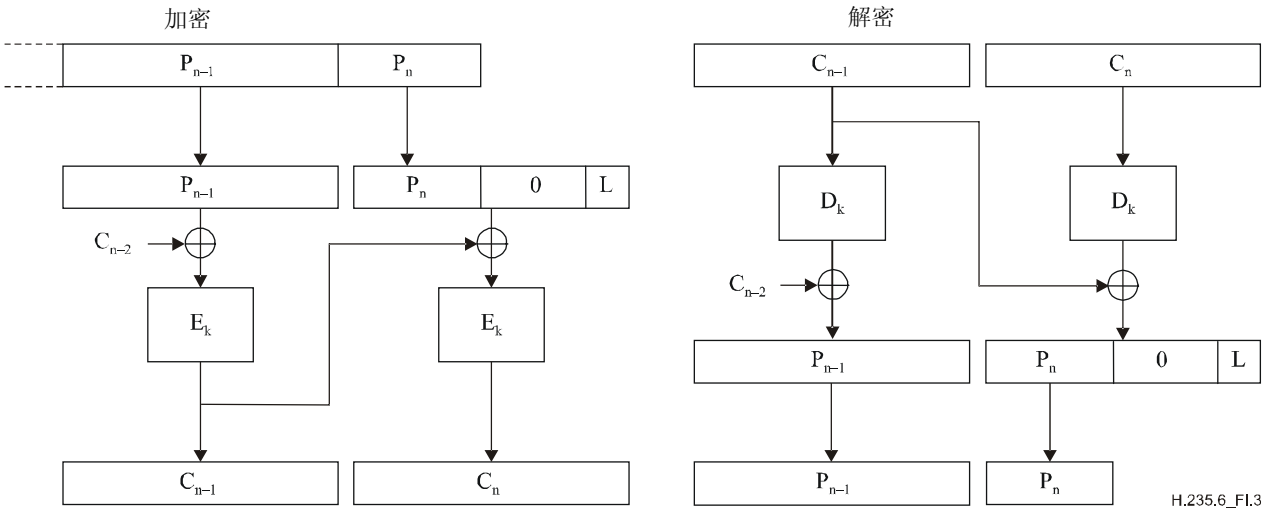


图 I.3/H.235.6－CBC方式的零填充

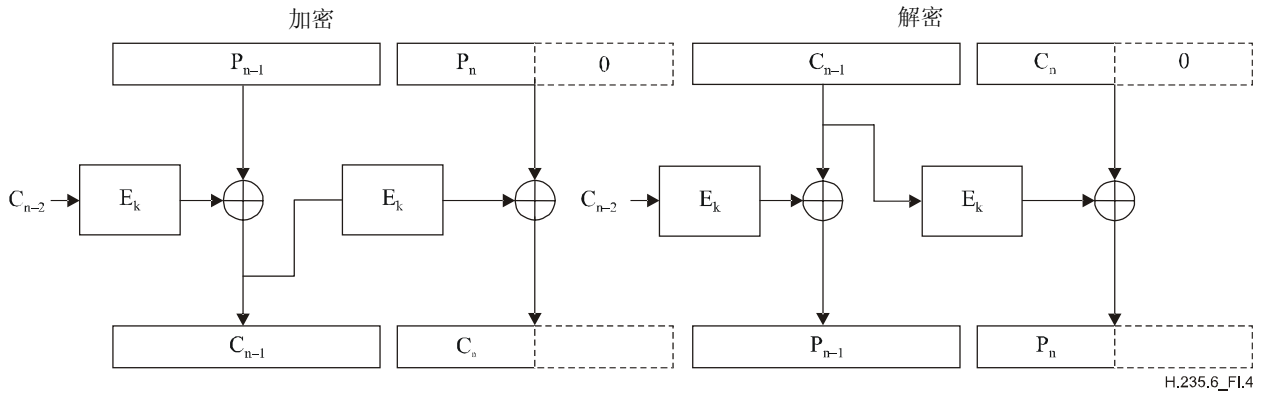
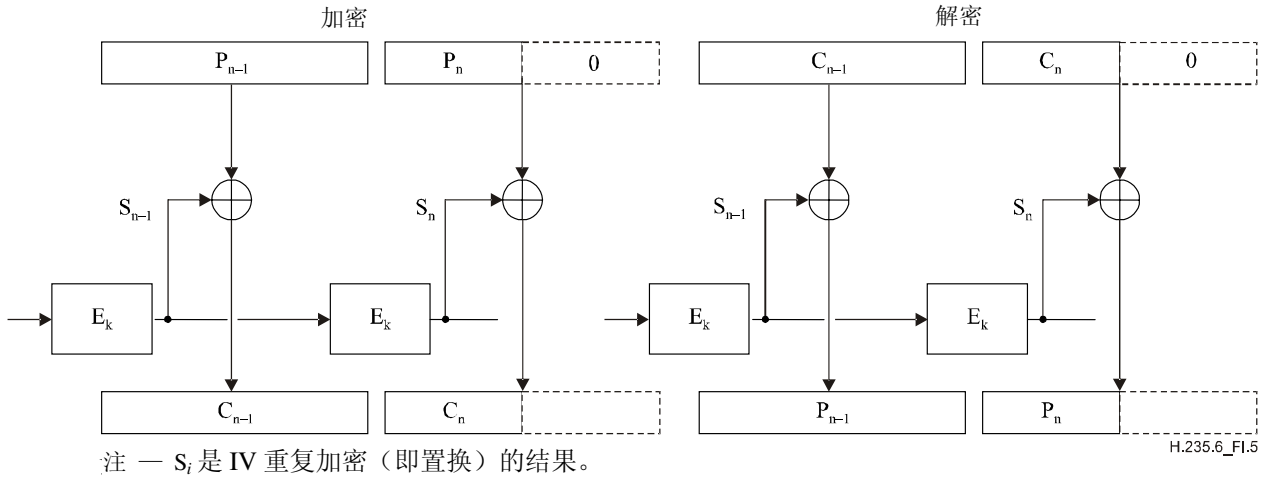


图 I.4/H.235.6－CFE方式的零填充



注 — S_i 是 IV 重复加密（即置换）的结果。

图 I.5/H.235.6－OFB 方式的零填充

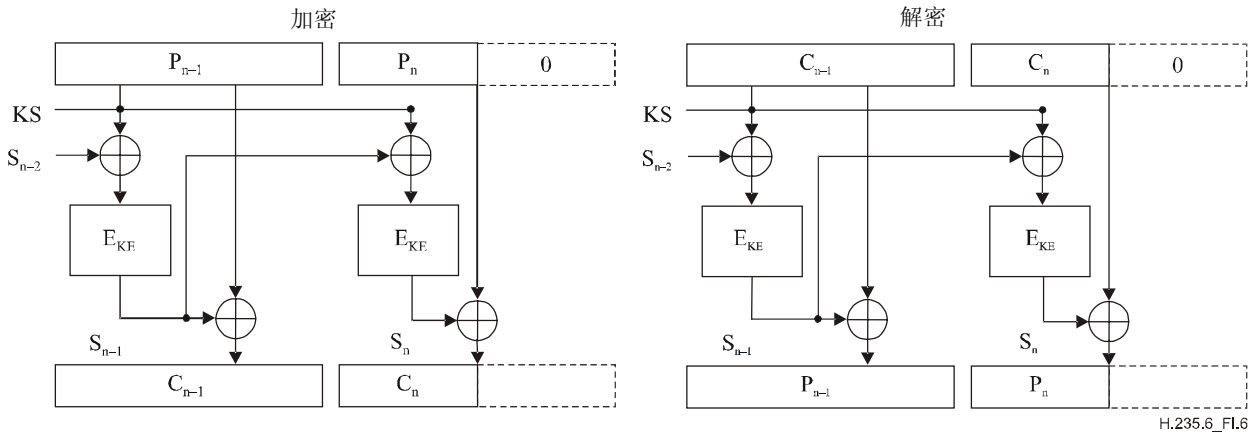


图 I.6/H.235.6－EOFB方式的零填充

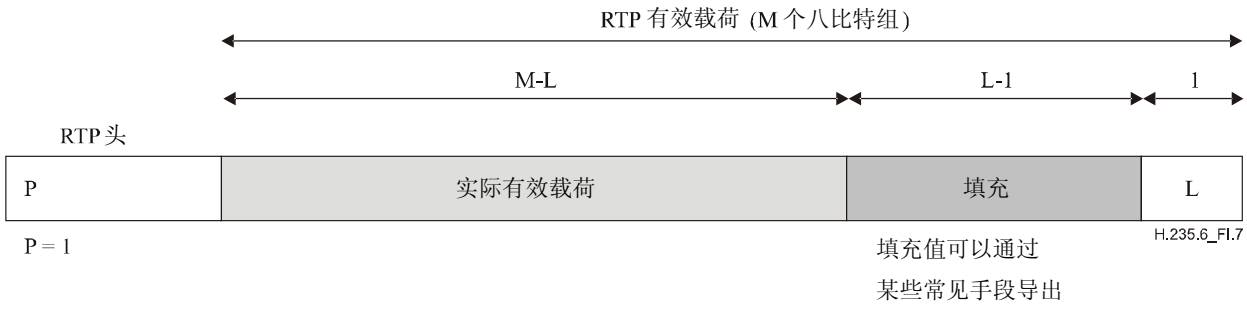


图 I.7/H.235.6－RTP所规定的填充

I.2 新密钥

为了把某个参与方逐出会议由 MC 完成 8.5/H.323 中概述的规程。主控方可以生成逻辑信道的新的加密密钥（并且不向逐出的参与方分发）；这可用于防止逐出的参与方监视媒体流。

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	**视听和多媒体系统**
I系列	综合业务数字网
J系列	有线网和电视、声音节目和其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置和本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2006年，日内瓦