国　　际　　电　　信　　联　　盟

ITU-R
国际电联无线电通信部门

ITU-R BT.1852-1 建议书
(10/2016)

用于数字广播的有条件接收系统

BT 系列
广播业务
(电视)

前言

无线电通信部门的职责是确保卫星业务等所有无线电通信业务合理、平等、有效、经济地使用无线电频谱，不受频率范围限制地开展研究并在此基础上通过建议书。

无线电通信部门的规则和政策职能由世界或区域无线电通信大会以及无线电通信全会在研究组的支持下履行。

知识产权政策（IPR）

ITU-R的IPR政策述于ITU-R第1号决议的附件1中所参引的《ITU-T/ITU-R/ISO/IEC的通用专利政策》。专利持有人用于提交专利声明和许可声明的表格可从http://www.itu.int/ITU-R/go/patents/en获得，在此处也可获取《ITU-T/ITU-R/ISO/IEC的通用专利政策实施指南》和ITU-R专利信息数据库。

ITU-R 系列建议书

（也可在线查询 http://www.itu.int/publ/R-REC/en）

系列	标题
BO	卫星传送
BR	用于制作、存档和播出的录制；电视电影
BS	广播业务（声音）
BT	**广播业务（电视）**
F	固定业务
M	移动、无线电定位、业余和相关卫星业务
P	无线电波传播
RA	射电天文
RS	遥感系统
S	**卫星固定业务**
SA	空间应用和气象
SF	卫星固定业务和固定业务系统间的频率共用和协调
SM	频谱管理
SNG	卫星新闻采集
TF	时间信号和频率标准发射
V	词汇和相关问题

说明： 该ITU-R建议书的英文版本根据ITU-R第1号决议详述的程序予以批准。

电子出版
2017年，日内瓦

ITU-R BT.1852-1 建议书

用于数字广播的有条件接收系统

(ITU-R 第49-1/16号课题)

（2009-2016年）

范围

本建议书描述用来协助制定采用MPEG-2传输流或MPGE媒体传输协议（MMTP）的数字广播有效的有条件接收方法的原则。它提供了关于可靠保护广播服务免受未经授权接收影响的信息。

关键词

有条件接收、加扰系统、接收控制、内容保护、MPEG-2 TS、MMT

国际电联无线电通信全会，

考虑到

a) 许多国家保护广播节目不受未经授权接收影响的需求日益增长；

b) 确保保护此类根据ITU-T H.222.0建议书复用的MPEG-2传输流封包的有效方法是采用有条件接收广播系统；

c) 采用有条件接收系统是确保根据ITU-R BT.2074建议书对MMTP封包进行保护的有效方法；

d) 已设计了有条件接收系统的样例且已开始操作数字地面、数字有线、数字卫星和IP（互联网协议）电视以及声音、多媒体和数据业务的有条件接收系统；

e) 存在许多根据BT和BO系列建议书实施数字广播系统的情况，如卫星数字广播系统的ITU-R BO.1516建议书；

f) 在考虑各种广播业务和传输系统不同需求的同时，有必要限制不同有条件接收系统的数量；

g) 从一开始就尽可能多地纳入有条件接收的共同要素，可为普通大众提供以较低的成本获得受保护服务的最大潜力；

h) 有条件接收系统提供了保护版权所有人、节目提供商和业务提供商非常需要安全的广播/分配网络，通过访问控制来保护其节目，

做出建议

1 用于保护MPEG-2传输流封包或MMTP封包的数字广播业务有条件接收系统应：

– 仅向授权接收机提供可用业务；

– 在接收机内最大限度地共享通用要素；及

– 根据附件1所列的基本原则进行设计。

说明 1 – 附件2给定了数字广播有条件接收系统的实施范例。

附件1

设计数字广播有条件接收系统的基本原则

1 引言

本附件所述原则应有助于为数字广播开发为用户和业务提供商提供便利、可靠保证信息不被非法接收的高效有条件接收系统。

原则通常适用于数字电视、声音以及多媒体和数据广播业务的交付。这些原则适用于ITU-T H.220.0建议书传输流封包和MMTP封包的交付，适用于地面数字、有线数字、卫星数字和IP（互联网协议）广播等各种媒体的用户。

2 规范性参考文献

ITU-T H.222.0建议书 | ISO/IEC 13818-1 –信息技术 — 活动图像及相关音频信息的通用编码：系统

ITU-R BT.2074建议书：用于基于MMT广播系统的业务配置、媒体传输协议和信令信息

3 术语、定义和缩写词

3.1 术语和定义

数字广播的*加扰*（Scrambling）

包含视频、声音、数据的广播内容的密码编码旨在防止未经授权，信息不被以非加密格式接收。这种密码编码是在有条件接收系统（发送端）控制下的精确过程。

数字广播的*解扰*（Descrambling）

包含视频、声音、数据的广播内容的密码编码旨在允许以非加密格式接收信息。这种密码编码是在有条件接收系统（接收端）控制下的精确过程。

有条件接收（Conditional access）

用户通过与接收机的有条件接收功能互动，访问受保护的服务。如果在会话中满足了所有的接收条件，给予授权，发放密码解码密钥，内容被恢复。

用户认证、账户确认以及服务可用度的验证或其他程序控制参数激活了会话加密/解密密钥，使得会话可以完成授权过程。

有条件接收控制（Conditional-access contro）

发送端有条件接收控制的功能是生成加扰控制信息和与服务有关的加密“密钥”。

接收端有条件接收控制的功能是生成解扰控制信息以及与服务有关的加密“密钥”。

加密和解密（Encryption and decryption）

这些术语用于描述保护（或解释）“接收相关讯息”（access-related messages）中一些信息的方法，这些讯息必须从有条件接收控制功能的发送端传送到接收端。

起点（Point of origination）

此点为分配系统中节目或其他内容首次变为其最终广播/分配格式的点。它标志着端到端保护的起始。输入内容（Entry content）可为任意格式，不一定是人类可感知的形式。内容输入自身不需要明白易懂。

说明 1 – 版权所有人、服务提供商和分配商在信息流向用户过程中，并进而在加扰内容和加密密钥流向用户的过程中形成了由许多可能起点构成的一个巨大等级。起点应由版权所有人或制作人开始。在实践中，出于商业和运作考虑，绝大多数起点即为系统中任意的输入点。尽管可能有许多这样的输入点，但每个点都是独特唯一的，信息可从此点以任意形式输入，连贯保有并最终抵达用户。

显示点（Point of presentation）

此为节目或其他内容在接收机屏幕和扬声器变为可为人所感知的格式前，最后作为分配系统中的信号而存在的点。它标志着保护的输出。

内容（Content）

可被获取并由设备显示的任意格式的数字数据。

服务（Service）

用于一起显示的一个或多个数据流。

服务保护（Service protection）

只有经过授权的设备才能接收和解码的服务保护。

3.2 缩写词

Ks 加扰键（Scrambling key）

Kw 工作密钥（Work key）

Km 主密钥（Master key）

EMM 授权管理讯息（ment management message）

ECM 授权控制讯息（Entitlement control message）

CRC 循环冗余码校验（Cyclic redundancy check）

DES 数据加密标准（Data encryption standard）

AES 高级加密标准

CBC 密码块链接

CTR 计数

MAC 消息认证码

MMT MPEG媒体传输

MMTP MPEG媒体传输协议

OFB 输出反馈

RMP 权限管理和保护

4 有条件接收系统概述

数字广播有条件接收系统包含两项基本功能：加扰和接收控制。在有条件接收系统中，这两项功能是截然不同且在许多情况下相互独立的组成部分，每一项都是完全分开的信息过程。

4.1 参考模型

有条件接收要求在广播之前对信息加扰。通过采用密码编码来广播比特流，以此获得该过程。

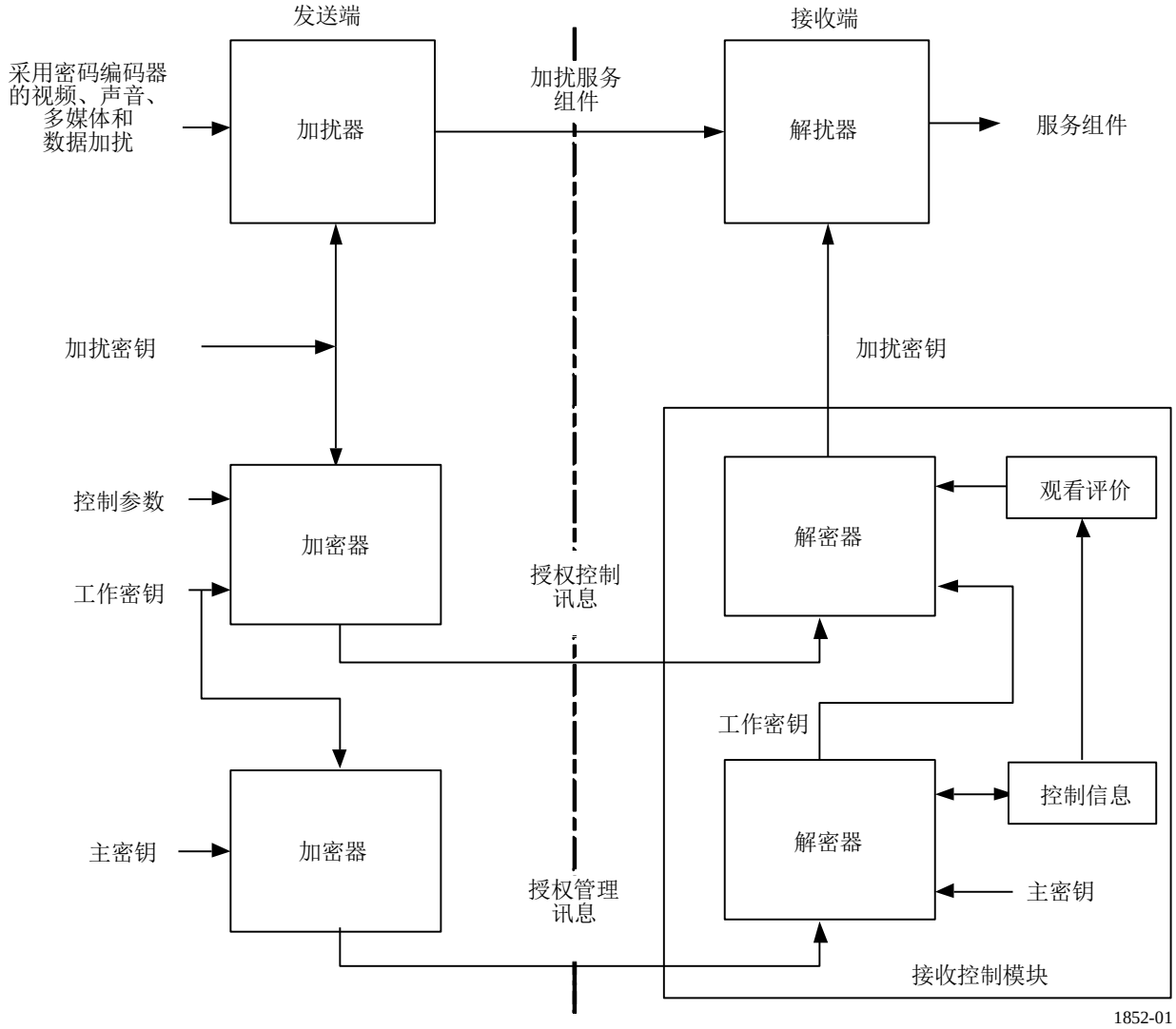
接收端的解扰过程要求相同的密码解码（在这种情况下，为解扰过程）来恢复原始的比特流。

为提供该连续事件并确保发送端和接收端之间的同步，密码解码的条件由密码编码器根据特殊协议发给解码器的数据控制。

该过程的详细结构如图1所示。

图 1

数字广播有条件接收系统结构图的示例



4.2 加扰

此为在发送端有条件接收系统的控制下，为应对未经授权的接收而保护服务的一些或全部组成部分的过程。

4.3 接收控制

此为提供信息，以便授权用户解扰受保护的服务。该信息的可用度由有条件接收系统控制。

在接收机和发射机之间，信息构造为可在广播比特流自身内复用或可通过电信线路等其他方式传输的特殊讯息。

在接收端，这些讯息由有条件接收系统翻译，以便控制经授权接收机所收到比特流中经授权部分的解扰。

5 用户需求

5.1 加扰器和解扰器密码的反破解强度

加扰器和解扰器部件中采用的密码应经过反破解能力的认真测试。建议从国际标准中选择密码。

5.2 安全

系统的安全指未经授权用户在试图接收受保护服务时遇到的困难程度。

– 不考虑接收控制过程的信号解扰。这是服务属性和加扰方法的一种功能。电视、声音和数据广播服务在性质上主要是数字的，因此允许高度安全的加扰过程。

– 以未经授权的方式获得访问控制。这是密钥加密算法安全的一种功能。

5.3 通用或专门加扰算法的选择

通过一种通用（普通）或专门的加扰算法，为任何满足接收要求的授权用户提供接收。

采用通用加扰算法意味着对于所有接收机而言，解扰是通用的，基于一种标准的解扰算法，独立于所采用的传输介质，如此可以实现低成本和灵活的设备选择，但仍可通过业务提供商独有的实施进行竞争。

采用专门解扰算法意味着在接收机上仅用所采用的特殊算法执行解扰过程。

5.4 接收模式

有条件接收系统可支持一系列接收模式，如：

– 周期可用度（period availability）（订购服务）– 从起始时间到结束时间的授权；

– 节目和服务项目（购买事件）– 无论是否完全使用，可用度针对一个具体服务项目；

– 服务收费（基于令牌）– 收费或信用的使用与使用期间和/或所涉服务价值成比例；

– 免费接收 – 服务受保护，但免费供接收。

接收模式需根据以下几个参数变化：

– 时间；

– 服务的各个部分；

– 针对用户群。

5.5 设备标准化

为提供接收设备最大的生产规模效应并简化管理和维护：

– 通用设备应标准化，以便其适应尽可能多的服务选项；

– 需要用户接收机架构，以支持所选有条件接收系统的有条件接收功能。根据所选系统的不同，功能可能需要嵌入或可分离安全功能（如智能卡）等支持。

5.6 接收管理

有条件接收的定义基于*授权*接收的正式概念，后者可以各种形式实施。授权给予其持有者接收相关服务的*授权*（authorization）。应避免由于管理或传输开销造成的资源不经济使用。

5.7 避免业务中断

应避免由于故障或不可靠获取接收控制数据而造成的中断。

6 授权控制讯息（ECM）

ECM提供加扰密钥，以解扰受保护的服务。

ECM中加扰密钥的访问通过授权或EMM提供的权限方式进行控制。

通常，在广播流中与受保护服务一起提供ECM。

通常，经常变换加扰密钥来尽量减小加扰密钥泄漏而造成的损害。

ECM的内容根据系统的不同而变化。

7 授权管理讯息（EMM）

授权管理讯息的处理验证或提供解扰受保护服务所需的授权。EMM可能包含提供工作密钥，对加扰密钥进行加密和解密。针对单个接收机的讯息和/或工作密钥是加密的。加密可能采用主密钥。主密钥可能存储在接收设备中。

在数字广播有条件接收系统中，授权管理讯息通过广播或其他媒介进行分配。

– 通过广播服务进行的分配称为“空中寻址”（over-the-air addressing）。与分配空中密钥相关的周期可通过应用共享密钥加密原则予以缩减。授权管理讯息也可通过其他媒介分配。

– 通过其他媒介分配通常通过点对点连接完成，由此提供一种额外的安全措施，确保讯息仅为目标设备所接收。

以下为操作的示例：

在每单位时间或每个节目付费的情况下，管理讯息可传送一个加密的费用代码，作为服务的一部分进行传送。赊欠款可存储在接收机中，可采用加密的钱款令牌形式，作为空中寻址服务的一部分传输。或者，赊欠款可采用以其他介质分配的存储钱款令牌的形式。付款包括根据接收到的费用代码减少存储的赊欠款。

EMM的内容视系统的不同而相异。

8 接收机接收控制功能

在接收端，可以包括以下在内的形式引入有条件接收：

类型 1：在接收机内执行安全功能（可能包括加密算法和主密钥）和解扰功能。

类型 2：安全功能是可分拆的（如智能卡），解扰功能在接收机中执行。

类型3：安全和解扰功能是可分拆的；所有执行输入数据流恢复的功能在可分拆模块中实施，通过标准化界面（如通用界面）与接收机通信；在这种情况下，可采用带有此类界面的任何接收机。

当被请求时，安全功能检查各项条件，如果满足，向描述符提供加扰密钥。这些条件包括：

– 期间要求，控制参数中的日期位于授权参数起始和终止日期之间；

– 价格要求，仅在如果安全模块接受了费用时，借此可提供授权。

有条件接收系统可实现包括涉及以下不同阶段安全功能的处理程序：

– 初步指示，如果有的话（如口令、用户认可等）；

– 采用安全模块的操作指示；

– 结果处理（如交付加扰命令）。

附件2（资料性）

数字广播有条件接收系统实施示例

表 1

实施示例

附件1中的参考	“Roscrypt”系统	“CAS-R”系统	“ARIB B61-CAS”	“DVB系统的IEC 62455”
§ 4 加扰器和解扰器的密码类型	基于俄罗斯联邦标准28147-89	MULTI2 (ISO/IEC 9979)	– AES (128-bit 秘钥长度) (ISO/IEC 18033-3) – Camellia (128-bit 秘钥长度) (ISO/IEC 18033-3)	DVB-CSA或AES-128（设备强制要求）；DES、3DES和 MULTI2也有可能（设备可选要求）
§ 4 加扰过程	基于采用64次多项式移位寄存器的循环多步转换 基于非线性算法且几乎为随机序列（没有解析式）	a) 对于64比特编码的序列，原始编码由另一个采用64和256比特变量的二进制码串代替 b) 对于码串小于64比特的，采用上述a)中所述方法来生成一系列伪随机编码序列，合并后生成加扰信号	– 对于MPEG-2 TS封包，CBC+OFB模式 – 对于MMTP封包，CTR模式	DVB-CSA：遵从ETSI ETR-289；AES-128：遵从FIPS PUB 197:2001，采用ECB或CBC模式；DES或3DES：遵从FIPS PUB 46-3:1999和FIPS PUB 81:1980；MULTI2 遵从ISO/IEC 9979
§ 4 加扰过程的同步	随机序列的互同步和DVB流整形电路	ECM中的相关信息（节目和控制信息）、EMM（个别信息）、EMM通用讯息且EMM个别讯息用来同步加扰过程	ECM中的相关信息（节目和控制信息）、EMM （个别信息）、EMM通用讯息且EMM个别讯息用来同步加扰过程	Odd_even_flag和initial_vector包括在密钥流讯息，传送服务加密密钥，协助同步。transport_scrambling_control比特和pes_scrambling_control比特的对应值表示在某个时刻采用的密钥

表 1（续）

附件1中的参考	“Roscrypt” 系统	“CAS-R”系统	“ARIB B61-CAS”	“DVB系统的IEC 62455”
§ 6 授权控制讯息 (ECM)	ECM内容： – 工作密钥标识符 – 加扰密钥（奇/偶） – 加密计数器和密码检验和 采用了DVB流结构性冗余或附加指定储备	ECM部分及ECM负载的基本架构： – 整个ECM部分需经各部分循环冗余码校验 – ECM负载包括一直传输的固定部分以及根据传输对象不同而内容变化的可变部分 – 仅在ECM可变部分插入必要的ECM功能信息	ECM部分及ECM负载的基本架构： – 整个ECM部分需经各部分循环冗余码校验 – ECM负载包括一直传输的固定部分以及根据传输对象不同而内容变化的可变部分 – 仅在ECM可变部分插入必要的ECM功能信息	ECM携载密钥流讯息，后者包括承载以下信息的 域： – content_key_index – odd_even_flag – 密码模式（cipher mode） – next_initial_vector – encrypted_traffic_key_material – traffic_key_lifetime – 时间戳（timestamp） – access_criteria_descriptors – permissions_category – encrypted_programme encryption key – programme_CID_extension – programme_MAC – service_CID_extension – service_MAC 在具体的密钥流中包括这些域的哪些，取决于服务提供商是否希望在单个节目基础上授权接收等多个因素

表 1（续）

附件1中的参考	“Roscrypt” 系统	“CAS-R”系统	“ARIB B61-CAS”	“DVB系统的IEC 62455”
主密钥	256比特	主密钥长度取决于业务运营商	主密钥长度取决于业务运营商	没有这样的“主密钥”。服务加密密钥（SEK）或节目加密密钥（PEK）的保护基于RSA密钥。根据认证中心（trust authority）的不同，前述后者具有1 024、2 048或4 096比特。在广播模式中，128比特推断密钥（IEK）具有类似的作用。它源自于注册过程中传送给接收机的一组密钥。这些密钥的保护基于1 024、2 048或4 096比特RSA密钥
§ 6 加扰密钥和标记的变更	根据需要变更加扰密钥。采用所有四种加扰标记的状态	加扰密钥（奇/偶）通常两秒钟变更一次	加扰密钥（奇/偶）通常一秒钟以上变更一次	业务加密密钥按照每分钟一次到每秒一次的频率经常变更
§ 7 授权管理讯息(EMM)	EMM内容： – 协议编号 – 广播设备群标识符 – 工作密钥 – 节目标识符 – 安全模块标识符 – 接收权利 – 加密计数器和密码校验和 – 采用了DVB流结构性冗余或附加指定储备	EMM部分可承载多多个负载。 整个ECM部分需经各部分循环冗余码校验。 ECM负载包括一直传输的固定部分以及根据传输对象不同而内容变化的可变部分 仅在ECM可变部分插入必要的ECM功能信息The 在EMM固定部分（未加密部分）的开头发送卡的(6字节)和相关信息字节长度(1字节)。 接收机过滤这一区域，确定发给自己的EMM负载。	EMM部分可承载多多个负载。 整个ECM部分需经各部分循环冗余码校验。 ECM负载包括一直传输的固定部分以及根据传输对象不同而内容变化的可变部分 仅在ECM可变部分插入必要的ECM功能信息The 在EMM固定部分（未加密部分）的开头发送设备ID号（8字节）（RMP情况下）或模块ID（6字节）（CAS情况下）以及相关信息字节长度(1字节)。 接收机过滤这一区域，确定发给自己的EMM负载。	在交互模式中，采用了OMA DRM 2.0权限对象，而不是授权管理讯息来向接收机传送权限和服务加密密钥（SEK）或节目加密密钥（PEK）。通过互动信道传输这些密钥和权限/ 在广播模式中，采用了这些权限对象的特别二进制版本（称为BCRO）

表 1（完）

附件1中的参考	“Roscrypt” 系统	“CAS-R”系统	“ARIB B61-CAS”	“DVB系统的IEC 62455”
§ 8 接收控制功能	位于有条件接收模块(CAM)中或内置于机顶盒（STB）中	类型 2：安全模块可分拆且加扰模块内置在接收机中	类型 1：安全和加扰模块在接收机内 类型 2：安全模块可分拆且加扰模块内置在接收机中	有可能是类型 1，但也不排除其他类型的实施
加密计数器和密码校验和	ECM、 EMM	讯息认证码（MAC）包括在ECM和EMM封包中	讯息认证码（MAC）包括在ECM和EMM封包中 MAC也可增添到每个MMTP封包中	讯息认证码（MAC）包括在密钥流讯息和广播模式权限对象中。用签名保护互动模式的权限对象
§ 8 安全功能	位于有条件接收模块(CAM)中或内置于机顶盒（STB）中	智能卡和接收机互认证	类型1和类型2中智能卡和接收机均互认证 对于类型1，可通过下载并更新接收控制系统维持并改进其安全	标准未规定实施。合规和鲁棒性规则（robustness rule）由认证中心制定

1 “Roscrypt”系统的描述

与数字电视广播的转换一起，俄罗斯正在实施有条件接收系统（CAS）的“Roscrypt”。“Roscrypt”系统设计用来保护DVB数据流不被非法接收。它拥有各种DVB系列卫星和地面广播的大量应用以及管理其用户的灵活性。

“Roscrypt”系统包括：

- 加扰器，对预选的DVB传输流部件进行加密；它可自行工作，或在计算机控制下工作；
- CAM模块，插入到接收机的通用接口（CI）插槽中，对所选部件进行解扰；
- 安全模块，具有内置的机顶盒。

通用控制和监控系统工作所需的设备安装在发送端。

“Roscrypt”解决了以下问题：

- 农村地区的广播限制，保护节目所有者限制广播的权利；
- 保护企业和部门广播不受非授权接收的影响；
- 组织商业广播。

“Roscrypt”考虑了被保护不被非法接收的电路的特性。

1.1 “Roscrypt”的功能和技术特征：

- CAS “Roscrypt”的通用工作模块对应着附件1的图1。
- 加扰算法：有两种专用加扰算法，在CAS “Roscrypt”加扰和解扰中得以实现。运营商可在任意地点改变现有的加扰算法。
- 安全密钥：CAS“Roscrypt”中采用了以下密钥：
  - 加扰密钥和工作密钥提供了内容的加扰/解扰。
  - 唯一主密钥的基础提供了ECM解密（工作密钥）和用户的接收控制。
  - 节目密钥组允许将不同运营商的用户互相隔离，并通过任意标准对用户进行分割。
  - 运营商可在不进行物理和电子分配的情况下，快速变更密钥。
- 接收模式：有两种有效管理用户的接收模式：期间可用度、节目和服务项目。
  - 接收模式参数：用户管理时间为每秒1 000个用户；用户数量没有限制；加扰组件的数量为150；预期用户组 – 64 000。

– EMM和ECM: EMM和ECM信号的结构符合附件1的第6和第7段。

  – 在每一个EMM和ECM封包的末端，有一个加密的计数器和密码检验和。

  – 对于管理控制（EMM和ECM）传送，DVB流带宽和DVB传输流结构速度储备（结构冗余）两种额外资源都可使用。

– 接收设备: 在接收端，有两种可能的有条件接收系统“Roscrypt” 类型：

  – 包含安全密钥的密钥解密算法和解扰模块的安全模块，内置在机顶盒中。

  – 包含安全和解扰模块的有条件接收模块（CAM），与接收机通过标准化通用接口（CI）进行通信，可拆卸。单个CAM模块可同时恢复加扰的输入传输流组件。

1.2 其他：

– 单个传输设备装置“Roscrypt”可对数个独立提供商的内容加密。该特性用于大型卫星和地面广播运营商。

– 通用控制和监控系统允许控制用户对内容的接收。

– 通用控制和监控系统允许远程集中操作并在全网中监控发射设备装置“Roscrypt”。该特性用于大型卫星和地面广播运营商。

2 “CAS-R”系统的描述

2.1 系统的用途

ARIB STD-B25涉及用于数字广播的有条件接收控制系统，对于在信号接收过程（以下称为“CAS-R”）提供控制的系统，定义其加扰和相关信息规范以及有关接收规范。

该标准规定了目前日本在用的地面和卫星数字广播系统的CAS系统。

2.2 CAS-R的要求及其协商系统

ARIB STD-B25规定了CAS系统，实现以下要求：

1 用户最大数量：

系统可扩展，为覆盖区内的所有家庭提供用户管理功能。

2 系统寿命：

系统可通过支持性、可适用的广播媒介进行管理。

3 应对非法接收

系统提供高级安全功能，可在安全攻击中采取措施。

4 系统可适用于特定领域内所有的数字广播系统。

5 接收类型：

a) A/V流和采用文件格式的数据广播等实时接收。（CAS-R）。

b) 存储接收（非实时接收）。

c) 录制接收（包括预约接收）。

6 系统可用于以下资费结构：固定收费/按级收费（flat/tier）、按次计费（即时付费收视（IPPV））和免费。

2.3 安全模块的要求

1 相关的信息加密：

加密系统采用与DES等同的三层架构和个人密钥。从智能卡实施的角度考虑，加密系统应以节目短小为特征，可有助于采用至少8比特微控制器进行高速处理。

2 管理功能：

系统可改变加密协议，以便应对非法接收。

3 在智能卡和接收机之间应采用相互认证：

在采用该有条件接收系统作为数字广播授权保护技术的应用中，当采用CAS智能卡来排除未对权限保护信息做出回应的接收机时，应提供在智能卡和接收机之间用于相互认证的系统。

2.4 以下文件提供了系统的详细描述

ARIB STD B-25有条件接收系统的规范可查阅：
http://www.arib.or.jp/english/html/overview/doc/6-STD-B25v5_0-E1.pdf。

3 基于ARIB STD-B61的第二代CAS（ARIB B61-CAS）的描述

3.1 系统特征

ARIB STD-B61 规定了第二代 CAS 数字广播的加扰系统、内容保护系统和 CAS 节目下载系统。第二代 CAS 具有以下特征：

– 支持MPEG-2 TS和MMT作为基础性媒体传输协议；

– 支持128-bit长度AES和Camellia作为加密算法；

– 支持相关信息的安全传输；

– 具有通过CAS节目下载机制不断维持并改进接收控制系统安全水平的能力。

3.2 系统要求

1 加扰子系统的要求

– 该子系统提供高级安全功能并在发生安全攻击时采取措施。

2 相关信息子系统的要求

– 相关信息尽可能格式统一。
– 单个接收机的信息可以传输。
– 相关信息可安全传输。
– 可不断维持并改进接收控制系统的安全。

3.3 加扰子系统

在加扰子系统中，选择了两种加密算法，以保持系统的高安全性：128-bit 长度 AES 或 Camellia。两种算法均用于 MMTP 封包和 MPEG-2 TS 封包。

在 MPEG-2 TS 情况下，加扰装置为一个 MPEG-2 TS 封包，但不包括其封包字头。由于 MPEG-2 TS 封包是一个固定长度封包，综合使用了加密块链接（CBC）和输出反馈（OFB），作为加密算法的工作模式。通过加扰描述符中的 Scramble_system_id 识别加密算法，它是业务信息的一部分。

在 MMT 情况下，加扰装置为一个 MMTP 封包，但不包括其封包字头。由于 MMTP 封包长度变化且相对较大，采用计数器（CTR）模式作为加密算法的工作模式。通过加扰描述符中的 Scramble_system_id 识别加密算法，它是业务信息的一部分。加扰控制信息放置在 MMTP 封包字头的扩展字段中，以识别以下三种加扰状态：无加扰载荷、偶数密钥加扰的载荷以及奇数密钥加扰的载荷。

3.4 相关信息子系统

有两种接收控制：一种是CAS，另一种是内容保护系统。每种系统具有自己的相关信息。

第二代CAS包含一个称为“权限管理和保护（RMP）”系统的内容保护系统，用于接收控制以外的免费广播业务。RMP系统可使广播机构向每个接收机分发用于解密内容的加扰密钥。

RMP系统与上述CAS-R系统基本相同，但它可适用于MMT和MPEG-2 TS两种情况。

3.5 三层架构和ECM/EMM

第二代CAS采用参考模型中包含ECM/EMM的三层架构。

在MPEG-2 TS 情况下，ECM为所有接收机提供通用信息。加扰密钥由ECM携载。ECM中加扰密钥的访问通过授权或EMM提供的权限方式进行控制。ECM提供单个接收机信息。工作密钥在EMM中携载。加扰密钥由EMM携载。

在MMT情况下，ECM为所有接收机提供通用信息。加扰密钥由ECM携载。ECM中加扰密钥的访问通过授权或EMM提供的权限方式进行控制。ECM提供单个接收机信息。工作密钥在EMM中携载。ECM和EMM由一条ITU-R BT.2074建议书规定的M2节消息携载。讯息认证码（MAC）可增加到每个MMTP封包中，以便接收机可核实该封包的完整性和真实性。

3.6 可下载CAS

第二代 CAS 包含一个可下载的 CAS，以不断维持接收控制系统的安全性并支持新的广播业务。接收机可安全地通过广播和/或宽带下载更新的 CAS 节目。

采用三层密钥架构和加扰通过广播频道下载 CAS 节目。广播频道中的 CAS 节目用传输频道保护密钥（Kt)）进行加密，该密钥通过采用下载控制讯息（DCM）和下载管理讯息（DMM）分发到每个接收机。

除为 CAS 节目加密外，其提供商也对其进行了签名，以维持其完整性和真实性。

4 “DVB系统IEC 62455”的描述

IEC 62455规定了用于控制接收基于MPEG2传输流的广播服务的标准化系统。IEC 62455也规定了同一系统如何用于控制接收基于互联网协议（IP）的广播服务。由此，规范广泛适用于不同类型的广播系统，包括不能在MPEG2传输流封包上实现保护的系统（如在非MPEG2网络中传输的IP业务）。

对于有条件接收系统，IEC 62455在发送和接收端之间提供了规定全面的接口。通过采用该规定全面的接口，服务器和接收机销售商都可独立实施保护系统的支持，而不是被强迫依赖于单一的安全销售商协助在服务器和接收机上实施。由此，系统内置避免了只绑定一个安全销售商，使得在不改变其他要素或其他销售商的情况下，变更任何有条件接收系统的销售商成为可能。

IEC 62455规范涵盖了系统的以下所有层，但在可能时尽量参引现有规范：

- 注册层
- 版权管理层
- 密钥流层
- 传输层。

授权管理层基于由开放移动联盟（OMA）制定、广为接受、在商业上大量采用的数字版权管理标准OMA DRM 2.0。取决于在订购还是按节目购买的基础上给予授权，该层负责传送权限和相关限制以及长期密钥，即服务加密密钥（SEK）或节目加密密钥（PEK）至接收机。

在互动模式中，即在接收机和业务提供商之间存在双向通信信道时，OMA DRM 2.0如此使用。对于缺少互动信道的单向广播操作，通过OMA DRM 2.0权限对象的带宽节省二进制版本（称为二进制编码权限对象，或BCRO）以及当通过广播信道传输时保护这些BCRO的方法来改进系统。选择BCRO包括各种寻址模式，后者进一步减少分配这些权限对象所需的带宽。保护方法基于零讯息广播加密，确保单个接收机的安全机制被破坏也不会获得传送给任何其他接收机的密钥和权限。广播带宽的使用非常优化。

对于广播信道的服务，广播模式操作所需的密钥在注册中传送给接收机。为注册某一项服务，用户只需将接收机唯一的设备号码（UDN）传送给服务提供商，后者可从证书数据库中查看接收机的证书。证书包括接收机的公共密钥，后者用于保护过渡期间的密钥集。

为保护MPEG-2传输流，服务实际内容的加密（加扰）采用IEC 62455所规定的DVB-CSA或AES-128等流行加密方法。IEC 62455还规定了IPsec、SRTP和ISMAcryp等其他加密标准的支持，以便有助于非MPEG2传输流封包的保护。

为协助经常更换用来保护服务内容的业务加密密钥（TEK），IEC 62455规定了在权限管理层和业务层之间工作的密钥流层。系统通过服务和节目权限对象支持接收同一流。在节目也可通过订购获得的情况下，如果业务提供商希望实现按节目的接收，除用PEK加密的TEK以外，密钥流讯息将携载一个用SEK加密的PEK。密钥流也可能携载一些与密钥流讯息适用的流的特定片段有关的其他信息，如接收条件或可用来在不同服务权限对象的不同权限之间进行选择的permissions_category值。这使得即使接收基于订购包含多个连续节目的服务，不同节目具有不同权限也成为可能。

附件2后附资料1

参考资料

– ITU-R BT.810建议书 – 有条件接收广播系统
– ARIB STD-B25：数字广播有条件接收系统规范
– ARIB STD-B61： 数字广播有条件接收系统（第二代）和CAS节目下载系统规范
– IEC 62455：基于互联网协议（IP）和传输流（TS）的业务接收