HDCP – 技术概述

目录

背景 2

HDCP 1.x 协议和工作方式 2

HDCP 2.0 4

总结 5

附录 – HDCP 1.x 授权认证和
内容加密详情 5

摘要

HDCP - 高带宽数字内容保护是一项加密协议，用于受版权保护的视频内容，如蓝光光盘和高清电影的下载。此文章详细地描述了 HDCP，介绍了 HDCP 系统的组件 – 信号源、中继器和接收器，以及 HDCP 协议的三个阶段 – 授权认证、内容加密和密钥更新。

白皮书

背景

视音频内容的数字化传输可完美重现原始素材。这种方式适合在追求最高质量时使用，但对于知识产权所有者来说却是一个令人担心的问题。高带宽数字内容保护 (HDCP) 是一项集成到数字视频连接接口的加密协议，以阻止未经授权的内容传输和复制。随着数字信号传输在市场上的激增，视音频专业人员将更加频繁地碰到 HDCP 问题。

HDCP 是一项应用于视频信号源和显示设备之间数字接口上的加密协议，可防止未经授权地访问受保护内容。HDCP 1.0 版最初应用于 DVI 接口。HDCP 1.1 版增加了 HDMI 接口，而 HDCP 1.3 版中增加了 DisplayPort 接口。随着 2008 年 10 月 2.0 版的发布，HDCP 不受接口约束，适用于信号源和显示设备之间任意的双向数字传输，无论是有线传输方式还是无线传输方式，压缩数据还是未压缩的数据。

数字内容保护有限责任公司是 Intel 的子公司，管理设备制造商的 HDCP 许可，并负责向持证许可人分配加密密钥。 每一个 HDCP 设备都必须有一组独有的加密密钥，包括一个公共密钥，也称作 KSV，以及 40 个私密密钥。HDCP 授权的制造商需要支付配置到他们产品中的加密密钥集模块的费用。

带 HDCP 的专业数字视音频系统

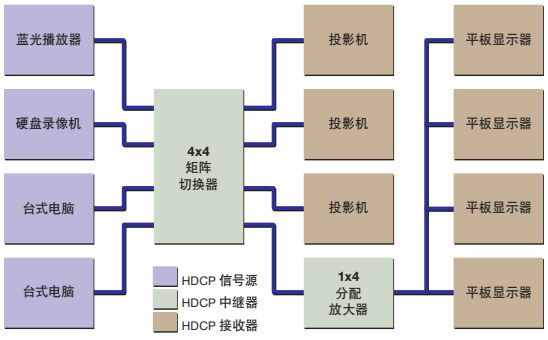

图 1： 专业视音频应用环境内的 HDCP 1.x 系统

HDCP 1.x 协议和工作方式

直至 HDCP 2.0 的推出，基本的 HDCP 协议才发生重大的改变。HDCP 1.0 至 1.3 版之间唯一主要的不同是视音频系统各个组件之间的物理连接类型。在 HDCP 系统中，这些组件被定义为信号源 - 例如 PC、蓝光播放器 - 可生成受保护的视频信号，接收器 - 例如监视器、投影机 - 用于显示内容，以及中继器 - 例如切换器、分配放大器 - 放置在信号源和接收器之间来分配视音频信号。HDCP 中继器包括输入端的一台接收器 - 或上游设备 - 连接，以及输出端的一台或多台发送器 - 或下游设备 - 连接。HDCP 1.x 系统内的组件通过双向端口进行通信，每个端口由一台发送器驱动，在接收器端终止。图 1 所示的是专业视音频环境下的典型 HDCP 1.x 系统。

从工作方式上来讲，HDCP 1.x 协议包括三个阶段：授权认证、内容加密和密钥更新。在授权认证阶段，加密信息和公共密钥在 HDCP 发送器和接收器之间交换，以确定接收器的身份、接受受保护内容的资格以及确认接收器是否是中继器的一部分。 如果接收器是中继器的一部分，那么中继器所包含的发送器将激活下游接收器的验证协议，以确定其资格。中继器也需要向信号源发送器报告所有下游设备的身份 - 公共密钥以及连接拓扑结构。信号源发送器主要是根据以下几个方面决定授权认证是否成功：

- 接收器直接的下游设备能在少于 100 ms 的时间内证实其资格。
- 所有下游设备的身份和连接拓扑都能在 5 秒内进行报告。
- 所有下游设备都有资格接收 HDCP 内容并且其资格未被废除。
- 连接的下游设备总计不超过 128 个。
- 下游中继器不超过 7 级。

如果以上条件都满足，那么授权认证即被认为是成功的，发送器可以进入到内容加密的阶段了。它使用一个 56 位的密钥来加密受保护的视音频内容，而接收器也会使用此密钥进行解密，并最终显示受保护的视音频素材。该密钥由每个 HDCP 设备进行独立计算，从不通过数字接口进行传输。所有下游中继器均会对视音频内容进行解密，并使用不同的密钥重新加密，以进一步向下游传输。出于额外的安全考虑，所有密钥都会在垂直同步期间定期地刷新。

第三个阶段，密钥更新，HDCP 许可方通过在和受保护内容一起传播的文件中罗列被盗用或破解的设备的公钥，从而废除这些设备的 HDCP 资格。受 HDCP 保护的内容如蓝光光盘，包含了系统更新信息 (SRMs)，以及黑名单中设备的失效公共密钥列表。新蓝光光盘发行时，其中一块数据罗列了失效的密钥。蓝光播放器会读取此数据，将其存储在非易失性存储器中，并将下游设备的公共密钥与此失效列表做比较。如果有任何下游设备匹配的话，则无视频传输。HDCP 设备负责检查 SRMs，当有新的失效列表公布时更新自己的内部存储器。失效列表在 HDCP 授权认证阶段查看黑名单中公共密钥的过程中使用。

参见附录进一步了解有关 HDCP 1.x 授权认证和加密的详情。

HDCP 2.0

2008 年 10 月发布的最新版 HDCP 中有许多重大变化。2.0 版中，HDCP 将不再仅仅应用于 DVI、HDMI、DisplayPort 等特定的接口，而是独立于这些接口标准，所以任何双向的通信机制都会受 HDCP 保护，包括无线通信和压缩格式。对于无线连接，HDCP 2.0 在授权认证协议中增加了一项位置核查功能，以确保只有附近的显示设备能够接收受保护内容。此外，HDCP 2.0 使用来自数据安全行业的两个标准算法代替了特定的 56 位 HDCP 1.x 加密体系：包含 1024 和 3072 位密钥的 RSA 系统用于授权认证；一个 128 位的 AES 系统用于内容加密。另外，最多可连接的数量减少到 32 个，中继器的级数减少到 4 层。所有这些改变都意味着 HDCP 2.0 不能直接反向兼容 HDCP 1.x。然而，新的规范可在 HDCP 1.x 和 HDCP 2.0 设备之间提供转换器，以支持混合了两个版本 HDCP 标准设备的视音频系统。这些转换器是非常重要的，因为 HDCP 许可协议要求被许可方在发布的 18 个月内支持新的规范标准。也就是说市场上的所有 HDCP 设备都将会支持 HDCP 2.0 版。如果最新的 HDCP 2.0 设备被增加到系统中，那么采用 HDCP 1.3 的已有视音频系统将需要转换器。图表 1 列出了 HDCP 2.0 的主要变化。

	HDCP 1.x	HDCP 2.0
加密方式	用于授权认证和视频加密的专用 56 位对称系统	授权认证： 数据安全行业标准 RSA 1024 和 3072 位非对称系统
		视频加密： 数据安全行业标准 AES 128 位对称系统
可应用的接口	DVI, HDMI, DisplayPort	任意双向数字接口
可用于每个发送器的最高下游接收器数量	< 128	< 32
可用于每个发送器的最高中继器级数	< 7	< 4
向下兼容性	是，无需电子组件	是，使用专用的 HDCP-1.x 至 2.0 和 HDCP-2.0 至 1.x 电子转换器
无线支持	由数字内容保护有限责任公司特别批准	明确能够支持，并增加了位置确认的需求

图表 1： HDCP 2.0 的 主要变化

总结

用于传输、处理或显示商业版权保护的高清内容，如蓝光光盘和 Apple® iTunes® 视频下载的所有数字视频设备，均需要支持 HDCP。HDCP 可加密数字视频，并确保只有授权的设备能够解密及显示受保护内容。 而且，根据系统中的设备数量和中继器级数，HDCP 对视音频系统分配及同时显示内容的功能也有所限制。随着 HDCP 规范的修改，这些限制也有所改变。了解 HDCP 的操作和限制，以便用于正确的系统设计和调试，这对视音频专业人员来说是至关重要的。

HDCP 标准的实施依据制造商而有所不同。 例如，即使 HDCP 1.x 协议规定来自视频信号源的下游接收器设备的最高数量不超过 128，这并不一定意味着所有 HDCP 1.x 视频信号源会允许这么多台设备与其连接。事实上，任何特定 HDCP 信号源所允许的下游接收器数量都根据型号有所不同，一定要根据具体情况决定。

附录 – HDCP 1.x 授权认证和加密详情

HDCP 1.x 授权认证

每一个 HDCP 1.x 设备都有一组独有的私钥和一个公钥。为了确定连接的接收器是经授权认证的设备并能够接收加密内容，HDCP 发送器向接收器发送一个包含公共密钥 Aksv 的信息，并期待接收器回传它的公钥 Bksv 用于交换，如果接收器回传了公共密钥，那么发送器会检验接收器的公共密钥以确定它是有效的，并根据接收器的公共密钥和它自己的私密密钥来计算密钥 Km。与此同时，接收器也会根据发送器的公共密钥和它内部的私密密钥来计算密钥 Km'。由发送器和接收器计算的密钥 Km 和 Km' 不通过通信端口发送，但如果双方都是授权的 HDCP 设备，那么密钥将能够匹配。为了表明它有一个匹配的密钥，接收器预计在发送器首次触发的 100 ms 内向发送器发送加密信息 R0'。如果上述情况没有发生，那么授权认证失败。由于 R0' 是使用密钥 Km' 生成的，发送器可以使用 R0' 与它自己内部的、使用 Km 生成的 R0 比较，所以如果 R0=R0'，则意味着 Km=Km'，从而接收器通过了初始的授权认证。请注意，密钥和私密密钥从不通过 HDCP 端口发送，所以任何的端口接收者都只能看到公共密钥 Aksv 或 Bksv，或加密的数据通信 R0'。图 2 演示了一个成功的 HDCP 初始授权认证的过程。

HDCP 发送器和接收器间初始授权认证信息的交换也是通过接收器的状态位，确定接收器是否是中继器。如果接收设备是中继器，则需要额外的步骤。HDCP 1.x 规范将连接至信号源的接收器总数量限制在 128 个之内，信号源和接收器之间中继器的总级数少于 7 层。因此，如果 HDCP 信号源遇到中继器，就必须确定是否违反了最高连接限制规定。此外，HDCP 信号源在发送受保护内容之前，必须对所有已连接的设备进行验证。为了满足这些需求，HDCP 协议规定信号源需要等待中继器

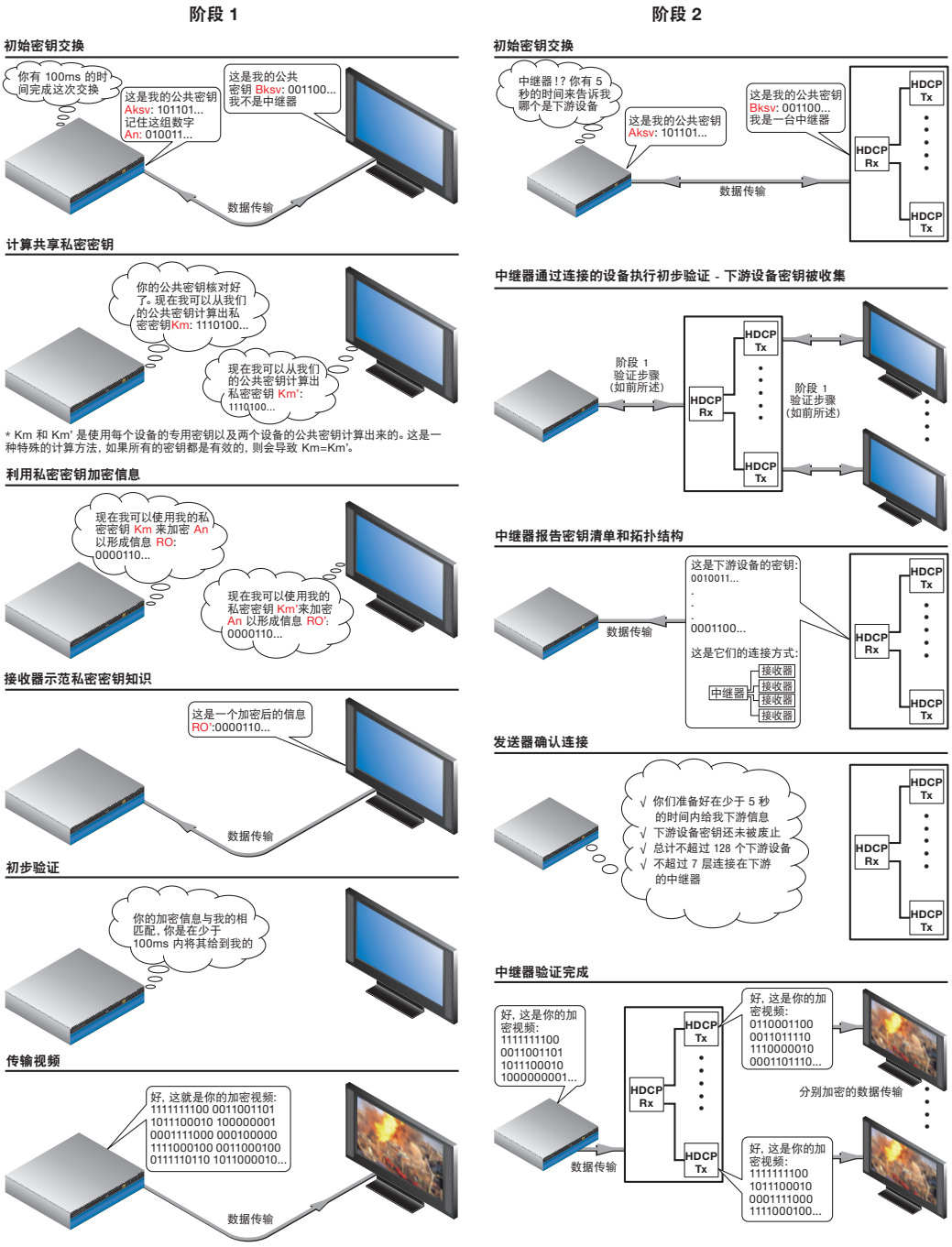

图 2： HDCP 验证

发送下游 HDCP 设备的公钥列表以及它们的连接方式。这些信息必须在初始通信后的 5 秒内发送至信号源。HDCP 中继器对于上游设备来说是一个接收器，对于下游设备来说又充当了发送器的角色。

HDCP 1.x 加密

初始授权认证完成之后，信号源开始发送数字视音频信息，信息的加密以早期描述的共享密钥 Km 为基础。任意经授权的接收器都有一个匹配的密钥 Km'，会使用 Km' 来解密视音频内容。实际的加密密钥会在垂直消隐间隔期间定期地变化，因此 HDCP 接收器必须与发送器保持同步。否则就不能继续解密视音频内容。HDCP 中继器对接收自上游信号源的视频进行解密，并重新加密视频以传送至下游接收器。由于每个发送器和它临近的下游接收器均使用相同的共享密钥进行加密和解密，所以 HDCP 1.x 加密机制被归类为对称的方式。