HDCP 在 Displayport 上的应用及实现①

Application and Implemention of HDCP Based on Displayport Interface

王建平 (桂林电子科技大学 电子工程学院 广西 桂林 541004)
范科峰 (中国电子技术标准化研究所 电子设备与系统研究中心 北京 100007)
肖 勇 (硅谷数模半导体有限公司 系统部 北京 100086)

摘 要: 实现了 HDCP（高带宽数字内容保护）在 Displayport 接口上的应用。在深入分析 HDCP 协议和 displayport 链路结构的基础上，设计了基于 displayport 接口芯片的 HDCP 认证驱动，按照 HDCP 认证机制实现了 HDCP 的三步认证过程。最后通过实例验证了 HDCP 驱动代码，实验表明芯片驱动符合 HDCP 的认证协议，完成了 displayport 接口对 HDCP 的完整认证。

关键词: HDCP Displayport 链路结构 芯片驱动

1 引言

HDCP[1](HDCP,high bandwidth digital cont－ent protection)技术是由好莱坞与半导体界巨人 Intel 合作发开，保护未经压缩的数字音视频内容，适用于高速的数字视频接口(Displayport、HDMI、DVI)，其最新版本 HDCP V1.3 已经支持 DisplayPort 接口采用源设备和显示设备间直接认证，内容加扰实现保护。

HDCP 设计为内容消费链中的最后一个环节，从内容源设备到显示设备，HDCP 不允许完全内容拷贝行为，即拷贝控制信息 CCI 只有禁止拷贝状态。在系统更新方面，HDCP 采用吊销列表来屏蔽已经被窃取的设备私钥。

2 displayport标准

DisplayPort 接口标准[2]是由视频电子标准协会(VESA)批准的，一个开放的、可扩展的标准。其为降低 PC 平台和元件的平台成本及推动通用数字接口而开发。DisplayPort 实现了显示设备用一条电缆与数字视频信号连通的高清数字音频，并实现真正即插即用的强大的互操作性，这些使其现有的数字显示互连非常具有成本效益。而且为了提高其与现有数字接口的互通性，DisplayPort 的 1.1 标准增加了兼容支持高带宽数字内容保护(HDCP)来支持 HDMI 和 DVI 采用的 HDCP 技术。

3 displayport

3.1 displayport 接口

Displayport1.1 是由显示端口任务发展组织(displayPort Task Group)共同研制开发的。Displayport 体积小，传输结构利用了类似 PCI Express 的电气层，采用“Micro-Packet Architecture(微封包架构)”传输架构，使视频内容以封包方式传送。传输数据最高可支持 10.8Gb/S 的传输带宽。

3.2 displayport 链路

Displayport 链路由一个主链路、一个辅助通道(AUX CH)、一个热插拔检测(HPD)信号线组成。如下图 1 所示，主链路是一条单向、高带宽并且低延时的通道，用于传输未经压缩的视频和音频等同步数据流。辅助通道是一条用于链路管理和设备控制的、半双工的双向通道。HPD 信号用作终端设备的中断请求信号。

① 基金项目:国家自然科学基金项目(60672112);科技部重要技术标准项目(2007GYB167)
收稿时间:2008-09-26

图 1　Displayport 数据传输通道

4　HDCP与displayport

4.1 HDCP 在 displayport 上的应用机制

HDCP 应用于 displayport 接口的保护机制[3]包括三个元素：

(1)HDCP 发送器(Transmitter/Source)，能立即识别下游接收器的拓扑连接结构，认证协议会确保 HDCP 发送器发出的讯号是 HDCP 接收器所授权接受的。

(2)DCP LLC 会撤销授权无效之 HDCP 接收器的授权。

(3)在有 HDCP 保护的讯号下发送与接收的同时，不断对加密视频传输的完整性进行验证。

4.2 HDCP 结构以及算法实现

4.2.1 HDCP 结构

HDCP 在 displayport 接口内容保护中采用了树状的拓扑结构[4]，为了使得完成认证的时间在容许范围之内，HDCP 规定了一个拓扑结构最多允许有 7 层结点、128 个接收设备。下图显示了一个设备深度为 2、设备数为 4 的拓扑结构示例。

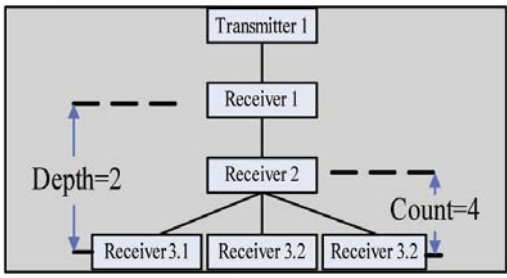

图 2　HDCP 拓扑结构图

4.2.2 Displayport 的 HDCP 认证实现

实现 HDCP 认证过程中，需要芯片内部硬件加密系统的支持，比如伪随机数的产生等。硬件加密系统结构如图 3 所示。

HDCP 由发送端(Tx)发起，Tx 系统初始化时内部首先产生伪随机数 An，并将其与自身的 KSV 一并发

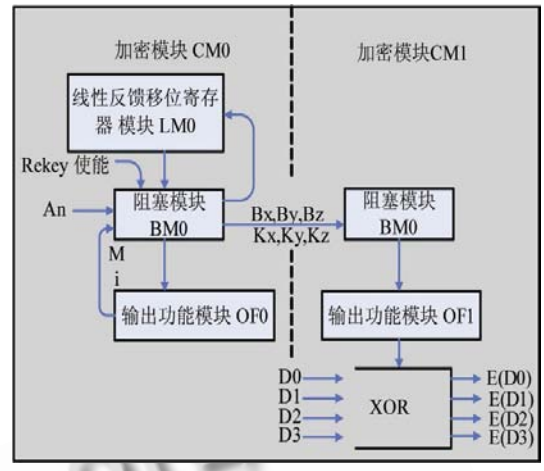

图 3　硬件加密系统结构

给接收端(Rx)，同时 Tx 读取 Rx 的 BKSV，BKSV 存储在接收端的 DPCD(DisplayPort Configuration Data)地址 0x68000 到 0x68004 内，共 40 个 bit。HDCP 采用了严密的校验方式，每一部都有必要的验证协议。当读取到 BKSV 后先对 BKSV 进行完整性验证和黑名单检测[5]。

(1)BKSV 检验

HDCP 的“撤销密钥”机制来应对密钥泄漏。每个设备的密钥集 KSV 值都是唯一的，HDCP 系统会在收到 KSV 值后在撤销列表中进行比较和查找，出现在列表中的 KSV 将被认做非法，导致认证过程的失败。这里的撤销密钥列表将包含在 HDCP 对应的多媒体数据中并将自动更新。

(2)协议第一步：R0(R0’)验证

当 KSV 检测和验证成功后，系统将进入算法认证的第一步。其认证协议结构如图 4 所示。

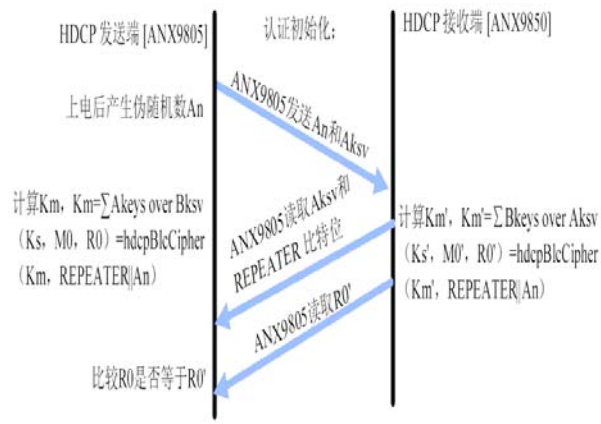

图 4　密钥交换认证协议图

其中 Km=∑Akeys over Bksv 和 Km'=∑Bkeys over Aksv 是一种密钥选择机制。接收端的 KSV 被认为合法后，发送端和接收端都会通过自己的私钥和相应的 KSV 计算出一个 56 比特的公钥 Km，这里把接收端计算出的公钥记为 Km'。制造商从 HDCP 认证组织 Digital Content Protection LLC 获得私钥和相应的 KSV 后，会在每一个支持该功能设备中存储这些数据，Km(Km')的计算就是通过对这些数据进行处理后得到的。

Km(Km')是给后续计算的准备，在 Km 和 Km' 计算完成后，HDCP 的加密系统就会根据产生的 Km(Km')和 An 以及 REPEATER 位来计算 KS(KS')、M0(M0')和 R0(R0')。KS(KS')是一个 56 比特的 HDCP 私钥，M0(M0')是 64 比特的私钥，在 HDCP 认证协议的第二步的初始化中需要该参数，R0 则是作为 HDCP 认证协议的计算结果，发送端通过读取接收端计算出的 R0' 并且与本地计算的 R0 比较，如果相同则意味着第一步认证协议的成功。

(3)协议第二步：中继器认证

在第一部分的认证过程中，transmitter 在读取 receiver 的 BKSV 同时，也读取了 DPCD 中的一个 REPEATER 位，HDCP 的第二部分是否执行取决于该位。这一位标志着该接收端是否为中继器。如果接收端没有中继功能，HDCP 会跳过该验证部分，直接执行认证的第三部分链路完整性检测。第二部分的认证协议框图如图 5。

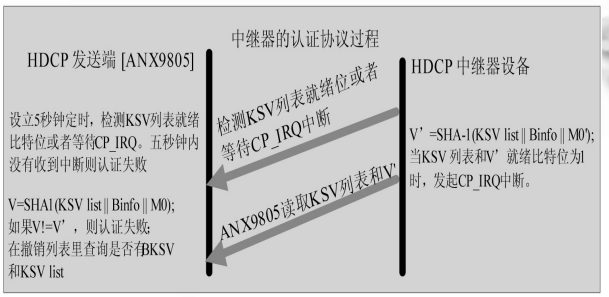

图 5　中继器认证协议图

当发送端检测到下游是中继器设备时，立即设立起五秒钟的超时定时器。源端设备可以通过抽样或者等待中断的方式来获取中继器的状态，而在这五秒钟之内，中继器就会建立自己的设备 KSV 列表并且计算 V'(哈希算法)。如果五秒钟之内没有完成这些操作，上游设备会认为该次认证失败。

安全哈希算法(Secure Hash Algorithm)是主要应用于数字签名标准(Digital Signature Standard DSS)领域定义的数字签名算法(Digital Signature Algorithm DSA)。SHA1 有如下特性[6]：不能从消息摘要中复原信息；两个不同的消息不会产生同样的消息摘要。HDCP 协议中 V(V')计算如下：

KSV list 存储于中继器 DPCD 地址 0x6802C 到 0x6803A 的 FIFO 中，FIFO 中有 15 个字节，每个设备的 KSV 是 40 个比特，也就是五个字节，所以 FIFO 中每次读取出来的是 3 个设备 KSV。Displayport 的中继器最多支持下游有 127 个设备，也就是说 FIFO 最多需要读取 127/3 次。每次读取完后硬件会自动清掉被读走的数据，同时用下一组 KSV 填满。Binfo 是存储下游设备拓扑结构的 16 比特数据，包括拓扑深度等。M0(M0')是 64 比特的私钥。也就是说计算 V(V')时，系统传输给 SHA1 的消息长度最大为 127*40+16+64=5160(0x1428H)个比特，对于长度小于 2^64（0x40000000000000H）位的消息，SHA1 会产生一个 160 位的消息摘要[7]。当接收到消息的时候，这个消息摘要可以用来验证数据的完整性。在传输的过程中，数据很可能会发生变化，这时候就会产生不同的消息摘要。

(4)协议第三步：加密完整性检测

在解密过程中，HDCP 在 HDMI 与 Displayport 中的应用所不同。在 HDMI 的解密过程中，HDCP 系统会每 2 秒中进行一次连接确认，同时每 128 帧画面进行一次发送端和接受端同步识别码，确保连接的同步，所有这些都是由发送端发起。而在 Displayport 的解密过程中， DisplayPort 的 Link Layer 负责确认两台设备之间的连结效能与正确的沟通，以其参数值(0=完整、1=不完整)作为沟通的语言，该参数是发送端通过辅助通道读取接收端的 DPCD 的某一位的值来获取，也就是说解密的完整性验证完全是由接收端来执行。

5　HDCP在Displayport接口上应用实例

ANX9805 是硅谷数模半导体公司设计的 DisplayPort 发送芯片，其完全符合 DisplayPort 1.1a 标准，也是 DisplayPort 产品业内第一个通过 VESA 认证的 DisplayPort 发送芯。其支持 HDCP1.3 标准

和 NVIDIA Upstream Protocol。

接收端使用目前市面上唯一的一款带有 Displayport 接口的 Dell 显示器 3008WFP，其 DP 接口支持 HDCP。支持 HDCP 的源端设备 ANX9805 可以通过黑屏、蓝屏或者低画质图像的方式使不支持 HDCP 或者 HDCP 不合法的设备无法播放音视频数据，这里采用降低色差使显示无法正常收看的方式防止未授权的显示终端。

图 6 和图 7 分别是在 HDCP 认证成功和失败后的输出图像，可以看到失败后的图像几乎没有观赏价值。HDCP 认证前后的视频参数如表 1 所列，加密解密的过程不会对视频参数[8,9]有影响，达到了安全认证的目的。

图 6　HDCP 认证成功的图像

图 7　HDCP 认证失败的图像

6　结论

结合芯片内部的硬件运算模块，设计了 displayport 的 HDCP 应用，实际测试表明在认证失败前后的图像参数无变化，但色差大幅度降低，无法正常观看，从而有效的实现了数字内容的保护，该驱动为日后 HDCP 在 displayport 接口上的应用奠定了基础。

表 1　HDCP 认证前后的参数比较

视频参数	认证前	认证后
Pixels clock	154.00MHz	154.20MHz
Hor freq	74.038 KHz	74.022 KHz
Ver freq	59.95 Hz	59.90 Hz
Hor total time	2080 pixels	2080 pixels
Ver total time	1235 lines	1235 lines
Hor sync	7.7% of Htotal	7.7% of Htotal
Ver sync	2.8% of Vtotal	2.8% of Vtotal
Hor blank time	160 Pixels	160 Pixels
Ver blank time	35 lines	35 lines

7　致谢

本课题研究得到国家自然科学基金和科技部重要技术标准项目的资助，特此致以诚挚的谢意！

参考文献

1 High-bandwidth Digital Content Protection System v1.3 Amendment for DisplayPort Revision 1.0. 19 December, 2006.

2 VESA DisplayPort Standard Version 1, Revision 1a. January 11, 2008.

3 宋亚平.基于 HDCP 协议的认证研究与流加密算法的实现[硕士学位论文].上海:上海交通大学, 2007:22－40.

4 王曙光.高清晰多媒体接口的研究与设计[硕士学位论文].合肥:合肥工业大学, 2007:13－21.

5 周咸春,梁维铭.HDMI 与 HDCP 技术分析及应用中国科技信息, 2007,(11) .

6 Federal Information Processing Standards Publication 180-2.2002 August 1.

7 李波,刘平,王张宜. SHA-256 输出序列的随机性研究.计算机工程与应用, 2007,(9).

8 泰克发布 DisplayPort 发射机测试自动化方案.电子与电脑, 2008,(1).

9 泰克推出 DisplayPort 测试解决方案和实现方法.世界电子元器件, 2008,(1).