第34卷 第13期 计 算 机 工 程 2008年7月
Vol.34 No.13 Computer Engineering July 2008
·安全技术· 文章编号：1000—3428(2008)13—0144—03 文献标识码：A 中图分类号：TP309

密钥管理系统在数字电影播放中的实现

朱振华[1,2]，王曦爽[1,2]，王国晖[1,2]，王贞松[1]
(1. 中国科学院计算技术研究所，北京 100080；2. 中国科学院研究生院，北京 100080)

摘 要：高级内容访问系统(AACS)是蓝光光盘和HD DVD采用的安全标准。该文通过剖析AACS，提出使用软件解密的多处漏洞，给出以AES算法为核心的密钥管理系统(SMS)。该解密系统采用硬件实时解密，已经在数字电影服务器中使用，可以有效避免软件解密的多种问题。密钥管理系统还采取了额外的措施保护固化的密钥。

关键词：高级内容访问系统；AES算法；密钥管理系统

Implementation of Security Management System in Digital Cinema System

ZHU Zhen-hua[1,2], WANG Xi-shuang[1,2], WANG Guo-hui[1,2], WANG Zhen-song[1]
(1. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080;
2. Graduate University of Chinese Academy of Sciences, Beijing 100080)

【Abstract】 Blu-ray disc and HD DVD use Advanced Access Content System(AACS) to protect the media content. This paper analyzes the AACS, and finds the software decryption has many problems. It proposes Security Management System(SMS) which uses the Advanced Encryption Standard(AES) algorithm for decryption and encryption. It is implemented by hardware. It can avoid many problems which implement in software. The SMS takes some special measures to protect the AES keys which are deposited in the device.

【Key words】 Advanced Access Content System(AACS); Advanced Encryption Standard(AES); Security Management System(SMS)

2007年1月，高级内容访问系统(Advanced Access Content System, AACS)在投入使用仅仅几个月之后就被破解。由于通用计算机系统的高度开放性、高度灵活性和资源的丰富性，通过计算机软件解密极易被破解。本文在此基础上提出了数字电影密钥管理系统(Security Management System, SMS)，该系统已应用于数字电影服务器中。

1 高级内容访问系统

AACS的前一代CSS(Content Scramble System)是DVD所采用的安全技术。在其被完全破解之后，由内容供应商共同成立的AACSLA (Advanced Access Content System Licensing Authority)推出了一个新标准——AACS。它是蓝光光盘和HD DVD新一代光盘采用的版权保护技术。

AACS是一个密钥管理系统，而不是加密算法[1]。它采用的是AES算法，AACS被破解并不是AES算法被破解，而是整个密钥管理机制中在某方面出现了漏洞。这个漏洞导致了AACS系统的崩溃。

1.1 AACS整体结构

AACS的整体结构如图1所示。

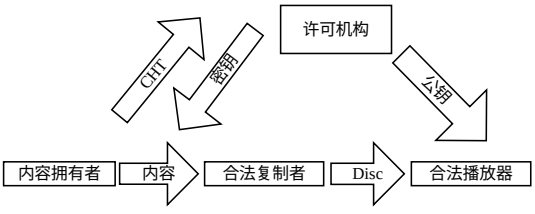

图1 AACS整体结构

在图1中，内容拥有者是音像制品的版权拥有者，合法复制者是光盘生产商，许可机构是整个系统的维护者，内容拥有者将内容交给合法复制者，合法复制者使用许可机构的密钥将其加密，并提取出内容散列表(CHT)在许可机构备案，制作出的光盘可由合法播放器播放[2]。

AACS系统实现了内容的保护。由于合法的播放器内有固化的密钥，因此合法的播放器不能放盗版光盘。光盘上的密钥如果不能和播放器内的密钥匹配(该匹配过程相当复杂)，光盘上的一些数据就会遭到破坏。因此，光盘上的内容不能被非法复制。

整个AACS系统保护的是内容拥有者、合法复制者、合法的播放器生产商的利益，那么这些生产商一定不会攻击协议，因此，最容易被攻击的是播放器播放环节，本文抽取整个协议的播放器环节进行分析[3]。

1.2 基于PC结构的播放器及其漏洞

播放器中有很大一部分是基于PC结构的播放器。PC机由多个不同的部件组成，包括CPU、主板、内存、显卡和一些其他的外设(外部设备简称外设)，蓝光或者HD DVD的光驱也是其中一个外设。基于PC结构的播放器，在经过密钥

基金项目：国家自然科学基金资助项目(60303017)；中科院计算所知识创新科研基金资助项目(20056210)

作者简介：朱振华(1982－)，男，硕士研究生，主研方向：图像处理，安全芯片设计；王曦爽，博士研究生；王国晖，硕士研究生；王贞松，研究员、博士生导师

收稿日期：2007-08-06 **E-mail：**zhuzhenhua@ict.ac.cn

验证之后需要从蓝光光盘或者 HD DVD 光盘中取出加密内容和密钥，再交给 PC 机软件解密。但是 PC 机软件解密是一个很大的漏洞。基于 PC 结构的软件解密过程见图 2。

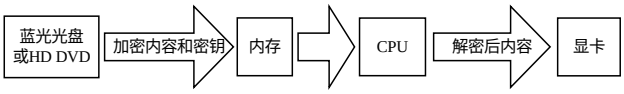

图 2　基于 PC 结构的软件解密过程

播放器软件解密的过程为：经过多步正确验证后，蓝光光盘或 HD DVD 将加密内容和密钥交给内存，由内存再交给 CPU 进行解密。解密后的内容由 CPU 交给显卡再由显卡输出给显示器。本文指出软件解密的 4 点漏洞如下：

(1)蓝光光盘或 HD DVD 光盘把加密密钥和加密内容交给内存，由于计算机本身各个部件之间的连接都是线直连，没有保密措施，这一过程很有可能被攻击者利用，密钥会被窃取。

(2)如果操作系统或者应用软件安全性上有欠缺，那么内存的内容就可能被窃取。

(3)解密后的内容传送给显卡，显卡与主机板的连接没有保密措施，这一过程也可能被攻击，内容可能被窃取。

(4)显卡到显示器之间的连接没有加密也可能被攻击。

到现在为止 AACS 被攻击都是因为第(2)点，就是操作系统或者应用软件不够安全。播放软件将 Title key(就是内容密钥)未经保护就放在了内存中，而取得这些内存中的数据就可以绕过 AACS 系统复制数据。微软作为 AACS 的创始成员，坚持认为在 XP 系统下由于很多原因，是无法开发出安全的播放软件的。在不安全的操作系统上开发安全的播放软件是不可能的。

虽然 AACS 到现在为止被攻击都是因为软件或者操作系统的漏洞，但并不代表本文列举出的其他漏洞不会被攻击，这几个漏洞也都是隐患。可以看出，由于普通计算机的开放性，计算机各部件之间连接没有保密性，因此使用 PC 机软件解密安全性得不到有效保证。

2　数字电影密钥管理系统

2.1　数字电影服务器和外部接口

整个数字电影服务器和外部的接口都采取了加密措施，保证数据不被窃取。发片商将加了密的内容和密钥交给服务器，这些密钥不能直接解密，需要先使用服务器内的设备密钥做一些处理。服务器把这些内容解密，作图像处理后再加密交给投影设备。服务器与外部的接口都是加密的，只要加密算法 AES 不被破解就可以保证内容不被窃取。

2.2　数字电影服务器内部的结构

本文设计的数字电影服务器的处理过程如图 3 所示，分为 4 个部分：

(1)服务器收到加了密的内容和密钥。

(2)加了密的密钥交给 AES 解密模块 1，AES 解密模块 1 取出设备密钥，通过设备密钥将加了密的密钥解密为内容密钥。

(3)将加了密的内容和第(2)步所得的内容密钥交给 AES 解密模块 2，AES 解密模块 2 进行内容解密，交给图像处理单元处理。完成图像解压缩及其他一些图像处理过程。

(4)图像处理单元处理后的结果通过 AES 加密模块加密后输出给投影仪，由投影设备解密。AES 加密模块的加密密钥需要和投影仪对应。

这些处理过程都是在一块电路板上完成的。这块电路板由 fpga virtex2p30, virtex2p50、3 片图像处理芯片和一些外围电路组成。整个解密、图像处理、加密过程在一块电路板上完成，可以很好地保证内容的安全性。

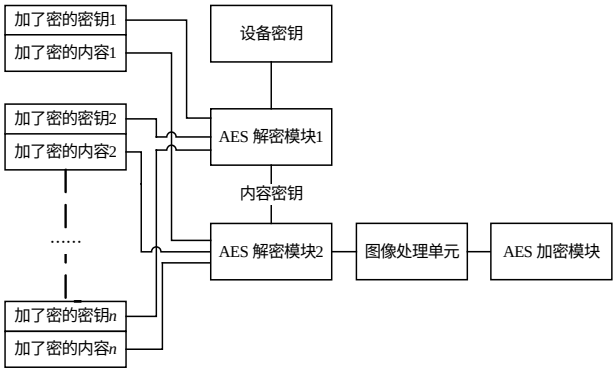

图 3　数字电影服务器的处理过程

2.3　数字电影服务器的安全性

由上文可知，整个服务器的核心是一块视频板，这块视频板完成解密、图像处理、加密等功能，服务器内容处理的功能都是由视频板来完成，而服务器和其他部件相连都有保密措施，也就是视频卡与其他部件(发片商、投影设备)都有保密措施。可以有效保证系统的安全性。AES 是整个密钥管理系统采用的算法，对固化设备密钥的保护也是密钥管理系统的一个特点。

3　加密数据格式及数据的解密过程

AES 加解密算法是美国国家标准和技术研究所发布的新加密算法。该算法实现简单、不易破解，是密钥管理系统的核心算法。

3.1　AES 数据解密过程

在AES数据解密过程之前，首先要进行密钥的扩展。解密算法接收 128 bit的密钥，并对密钥进行扩展，生成 10 组扩展密钥。在接下来的解密过程中，解密算法接收 128 bit的加密数据，并循环 11 轮数据解密过程，第 1 轮使用原始密钥对加密数据进行与扩展密钥异或步骤的处理，接下来的 9 轮，每轮都对加密数据依次完成s盒变换、行变换、列变换、与扩展密钥异或 4 个步骤，最后 1 轮对加密数据进行s盒变换、行变换、与扩展密钥异或 3 个步骤的处理，之后输出 128 bit的解密数据[4]。

由此可知，AES 解密的输入输出接口均为 128 bit。AES 数据解密过程如图 4 所示。

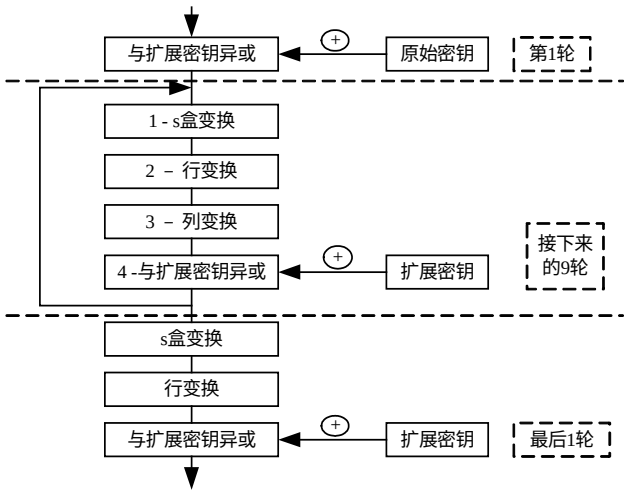

图 4　AES 数据解密过程

3.2 数字电影 AES 解密系统的硬件设计

AES解密IP模块用来接收 128 bit的解密密钥和加密数据，对加密数据进行处理并输出解密数据[4]。在数字电影AES解密系统中使用了AES解密软IP，实现了 128 bit加密数据的解密过程。由于没有实现流水机制，该IP具有资源占用率小的优点。

如图 5 所示，AES 解密 IP 的系统结构可分为控制部分、密钥扩展部分与数据解密部分。控制部分用来接收输入外设提供的数据有效信号：kld 信号与 ld 信号。

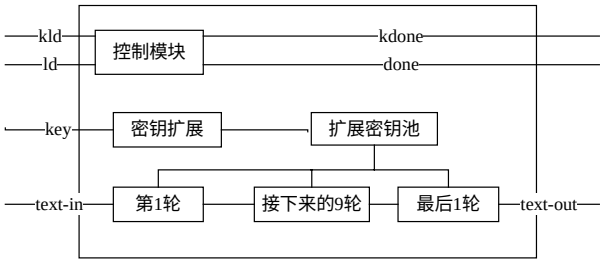

图 5　AES 解密 IP 的系统结构

当kld信号有效时，说明外设提供的密钥已经在key数据总线上准备好；当ld信号有效时，说明加密数据已经在text_in数据总线上准备好。AES解密IP向外设输出的控制信号为kdone与done信号，当kdone信号有效时，说明AES解密IP已经完成了密钥扩展工作；当done信号有效时，说明AES解密IP已经完成数据解密，可以向外设输出 128 bit的解密数据[5]。当ld信号有效时，AES解密IP从text_in数据总线上读取 128 bit的加密数据，经过 11 个时钟周期，AES解密IP在第 12 个时钟周期将done信号置为有效，指示外设可以从AES解密IP的text_out数据总线上读取有效的 128 bit解密数据。

3.3 实验结果

笔者编写的逻辑电路通过了 modelsim 仿真验证和 fpga 验证，芯片稳定工作在 66 MHz 时钟下，AES 解密系统的数据输出带宽达到了 514 Mb/s，这个数据输出带宽远大于数字电影规范规定 250 Mb/s 的数据输出带宽。

4　设备密钥的保护

一般的密钥管理系统对固化的设备密钥并不进行保护，本文的密钥管理系统为了达到更高的安全性，对设备密钥也进行了保护，采用安全芯片加 sram 加电池的方法来保证设备密钥的绝对安全。

如图 6 所示，在 sram 中存放着设备密钥，sram 由 stm1403 供电，sram 的控制线和地址线、数据线与 fpga 相连，fpga 可以对 sram 读写。由于 sram 的掉电易失性，因此需要在板上加上电池，在服务器关闭的时候给 sram 供电。stm1403 是一枚集成了多种功能的安全芯片，在电路板上电的时候通过 stm1403 给 sram 供电，当电影服务器断电的时候，电池通过 stm1403 给 sram 供电，stm1403 有 4 个安全引脚，它们分别和物理设备连接，这些物理设备是一些感知设备，一旦感知到异常情况(密钥信息有可能被窃取)就不再给 sram 供电，sram 具有掉电易失性，这样设备密钥就被销毁。在电影服务器出厂时就在 sram 中写入设备密钥，需要解密的时候 fpga 从 sram 内提取设备密钥进行解密。

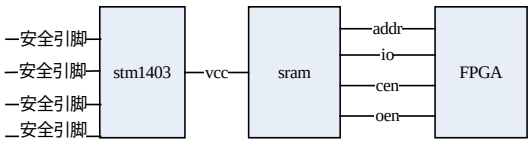

图 6　设备密钥的存放和保护

5　结束语

本文提出了使用硬件解密的密钥管理系统，该系统已经在数字电影服务器中得以实现，电影服务器视频卡上包含了图像处理单元和密钥管理单元。整个数字电影系统能够实时地播放分辨率为 2 048×1 080 的视频。该密钥管理系统还可应用于军事卫星图像处理，可以有效地保证军事机密、电影信息等重要信息不被窃取，在视频及图像处理中有着广阔的应用前景。

参考文献

[1] Advanced Access Content System(AACS) HD DVD Recordable Book[Z]. Intel Inc., Microsoft Inc., Sony Inc., et al. 2006-07-25.

[2] AACS Introduction and Common Cryptographic Elements book[Z]. Intel Inc., Microsoft Inc., Sony Inc., et al. 2006-02-17.

[3] 尹超辉. 向盗版说 No 光盘锁卷土重来——AACS 技术全解析[J]. 微型计算机, 2006, (15): 155-156.

[4] Usselmann R. Advanced Encryption Standard Rijndael IP Core[Z]. (2002-05-01). http://www.opencores.org/projects.cgi/web/aes_core/overview.

[5] 金永明, 戎蒙恬, 朱甫臣, 等. 2.56 Gbps 对称密码芯片的设计与实现[J]. 计算机工程, 2006, 32(14): 238-240.

（上接第 143 页）

然与原始平均值具有至少绝对值为 0.001 的差值，因此可通过其值的正负得到比特“ 1 ”或“ 0 ”，进而得到指纹序列，可以将两名合谋者全部确定。当两个以上合谋者进行拷贝平均时，可能出现某帧统计平均值与原始平均值相等的情况，此时可以取其值为“ 1 ”，其余判断与前面两人合谋的情况相同，结合具体指纹码字的特征以及汉明距离，仍然可以确定至少一名叛逆者。但随着用户的增加，确定的成功率会有所下降。

5　结束语

本文结合混沌和小波系数统计特性，提出了一种具有良好鲁棒性、不可感知性的音频指纹方案，可以抵御常见的音频攻击和处理方法，且对同步攻击不敏感，在非大量用户前提下，对常见的合谋攻击能以较高的概率确定至少一名合谋者。对于如何抵御大量用户条件下的合谋攻击，是下一步研究的内容。

参考文献

[1] Cox I J, Miller M L, Bloom J A. Digital Watermarking[M]. [S. l.]: Morgan Kaufman Publishers, 2002.

[2] Wu Min, Trappe W. Collusion-resistant Fingerprinting for Multimedia[J]. IEEE Signal Processing Magazine, 2004, 21(2): 15-27.

[3] 纪　震, 肖微微, 张基宏. 基于噪声分析的混沌数字图像水印算法[J]. 信号处理, 2003, 19(3): 252-255.

[4] Tzanetakis G, Essl G, Cook P. Audio Analysis Using the Discrete Wavelet Transform[C]//Proc. of Int'l Conf. on Acoustics and Music: Theory and Applications. Skiathos, Greece: [s. n.], 2001.

[5] 李　伟. 鲁棒性数字音频水印算法研究[D]. 上海: 复旦大学, 2004.