国密算法在数字电影中的应用探讨

李雪伟　刘知一　王木旺

（中国电影科学技术研究所，北京 100086）

【摘要】为践行《中华人民共和国密码法》中鼓励国家商用密码技术开发和推广应用的精神，对国密算法 SM1、SM2、SM3、SM4、SM7、SM9、ZUC 的主要特点进行了简要概括，并针对当前数字电影应用场景，对国密算法在数字电影中的应用方案进行了探讨。通过对不同类别国密算法的研究，在数字电影内容加密和传输环节采用国密算法完全可行。本文为数字电影领域国密算法的推广应用提供了可行性支持，有利于加速数字电影关键技术国产化进程。

【关键词】国密算法　数字电影　可行性　国产化

【中图分类号】J945

1 引言

近年来，全球数字电影产业进入新一轮技术革新期，我国个性化放映需求不断增强，电影内容版权保护日益得到关注。另一方面，国家从长远战略的高度提出推动国密算法应用实施、加强行业安全可控的要求，国家商用密码产业链不断完善。数字电影在发行包加密、传输、解密播放等主要环节，目前均通过国外专利密码技术支撑内容的版权保护，在数字电影领域推进国密算法应用，促进我国自主研发的国密算法逐步应用在数字电影关键技术环节，摆脱对国外技术和产品的过度依赖，推动相关设备国产化，势在必行。

2 国密算法介绍

2020 年 1 月 1 日，我国首部关于密码的立法《中华人民共和国密码法》[1]（以下简称：《密码法》）施行，其中对密码进行了定义：密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务，并将密码分为核心密码、普通密码和商用密码。其中核心密码、普通密码用于保护国家秘密信息，商用密码用于保护不属于国家秘密的信息。本文所说的国密算法即国家商用密码算法。

密码，根本上是按照一定的规则对信息进行重新编码，以保证信息的机密性。根据通信双方所持密钥是否相同，密码可分为 3 大类：对称密码算法、非对称密码算法、杂凑算法。其中对称密码算法是

【项目信息】本文受国家重点研发计划资助《影视媒体融合服务技术集成与应用》（项目编号：2018YFB1404000）中《电影数字水印和新型显示格式关键技术研究与示范》课题（课题编号：2018YFB1404004）。

【作者信息】李雪伟（1989－），女，硕士，中国电影科学技术研究所工程师，主要研究方向：数字电影技术；刘知一（1976－），男，硕士，中国电影科学技术研究所高级工程师，主要研究方向：数字电影技术；王木旺（1977－），男，硕士，中国电影科学技术研究所高级工程师，主要研究方向：数字电影技术。

通信双方拥有相同的密钥，即加密密钥和解密密钥相同；非对称密码算法是通信双方拥有不同的密钥，加密密钥和解密密钥不同，二者组成一个公钥、私钥的密钥对；杂凑算法能够将任意长度的消息压缩成固定长度的摘要，能够赋予每个消息唯一的“数字指纹”。

国际上通用的对称密码算法有 DES、AES 等，非对称密码算法有 DSA、RSA、ECC 等，杂凑算法有 MD5、SHA 等。我国自主研发的国密算法包括 SM1、SM2、SM3、SM4、SM7、SM9 和祖冲之密码算法（ZUC）等。其中 SM1、SM4、SM7 和祖冲之密码（ZUC）是对称密码算法，SM2 和 SM9 是非对称密码算法，SM3 是杂凑算法。国密算法与国际通用加密算法的对应关系如表 1 所示。

表 1　国密算法与国际通用加密算法的对应关系

密码算法类别	国际通用密码算法	国密算法
对称密码算法	AES、DES	SM1、SM4、SM7 和祖冲之密码（ZUC）
非对称密码算法	RSA、DSA、ECC	SM2、SM9
杂凑算法	SHA、MD5	SM3

2.1 对称密码算法

2.1.1 SM1 算法

SM1 算法是分组密码算法，分组长度和密钥长度均为 128 比特，该算法将待加密的数据以 128 比特为一组，分成 n 组，对每组数据使用 128 比特长度的密钥进行加密。该算法不公开，仅以 IP 核的形式存在于芯片中，调用该算法时，需要通过加密芯片的接口进行调用。该算法安全性与国际通用算法 AES 相当。该算法已被应用于芯片、智能 IC 卡、智能密码钥匙、加密卡/机等安全产品。

2.1.2 SM4 算法

SM4 算法，即 SM4 分组密码算法，分组长度和密钥长度均为 128 比特。该算法主要包含加密算法、解密算法和密钥的拓展算法，该算法加密时对字节数据进行 128 比特分组，然后使用轮密钥对每组数据进行加密，共进行 32 轮加密计算，最后得到密文。解密时逆序使用轮密钥对密文进行解密得到原数据。

2.1.3 SM7 算法

SM7 是分组密码算法，分组长度和密钥长度均为 128 比特。SM7 算法不公开，调用该算法时，需要通过加密芯片的接口进行调用。该算法适用于非接触式 IC 卡，该算法可应用于身份识别类应用（门禁卡、工作证、参赛证）、票务类应用（大型赛事门票、展会门票）、支付与通卡类应用（积分消费卡、校园一卡通、企业一卡通）等。

2.1.4 祖冲之序列密码算法

祖冲之算法，简称 ZUC，名字源于我国古代数学家祖冲之，由中国科学院等单位自主研究的序列密码算法，该算法初始化阶段输入的初始向量和初始种子密钥均为 128 比特，输出的密钥字为 32 比特，之后重复 32 次初始化阶段，第 33 步舍弃，第 34 步进入密钥输出阶段，输出密钥字 32 比特。该算法由三部分组成：算法描述、基于祖冲之算法的机密性算法和基于祖冲之算法的完整性算法。ZUC 算法作为序列密码，安全性本身就优于分组密码。

ZUC 算法于 2011 年 9 月被 3GPPLTE 采纳为国际加密标准（标准号为 TS35. 221），即第 4 代移动通信加密标准，是我国第一个成为国际密码标准的密码算法；2012 年 3 月成为中国商用密码标准（标准号为 GM/T 0001－2012）；2016 年 10 月成为国家密码标准（标准号为 GB/T 33133－2016）；2020 年 4 月，正式成为 ISO/IEC 国际标准，并纳入 ISO/IEC 18033－4/AMD1《加密算法第 4 部分：序列算法－补篇 1》发布。

2.2 非对称密码算法

2.2.1 SM2 算法

SM2 算法是我国在吸收国际先进成果的基础上研制的具有自主知识产权的椭圆曲线公钥密码算法（elliptic curve cryptography，ECC）。该算法推荐了一条 256 比特的曲线作为标准曲线，该算法标准主要包括：数字签名算法、密钥交换协议和公钥加密算法。其中 SM2 数字签名算法由签名者利用自己的私钥对数据签名，验证者利用签名者的公钥对签名进行验证，确保该签名真实可靠；SM2 密钥交换协议是用户双方利用自己的私钥和对方的公钥来商定

一个只有双方知道的会话密钥。SM2 公钥加密算法是发送方利用接收方的公钥对数据进行加密，接收方利用自己的私钥对收到的密文进行解密。

SM2 算法于 2012 年 3 月成为中国商用密码标准（标准号为 GM/T 0003－2012）；2016 年 8 月成为国家密码标准（标准号为 GB/T 32918－2016）；2017 年 11 月，SM2 数字签名算法被纳入 ISO/IEC 国际标准 ISO/IEC 14888－3/AMD1《带附录的数字签名第 3 部分：基于离散对数的机制－补篇 1》。

2.2.2 SM9 算法

SM9 标识密码算法是在有限域中，利用椭圆曲线上双线性对构造的基于标识的密码算法[2]。不同于传统的公钥密码算法，SM9 算法不需要通过传统公钥基础设施 PKI 体系中的证书认证中心 CA 等保证用户公钥来源的真实性，SM9 算法是基于用户的唯一标识信息（手机号码、邮箱地址等）生成公私钥对，发送方利用公钥加密数据，接收方利用自己的私钥解密数据，无需数字证书的申请、查询、验证和交换环节，极大地减少了计算和存储等资源的开销。SM9 算法主要包含数字签名算法、密钥交换算法、密钥封装机制、公钥加密算法等。

SM9 算法于 2016 年 3 月成为中国商用密码标准（标准号为 GM/T 0044－2016），2018 年 11 月，SM9 数字签名算法成为 ISO/IEC 国际标准，并纳入 ISO/IEC 14888－3：2018 正文发布。2020 年 4 月成为国家密码标准（标准号为 GB/T 38635－2020）。2021 年 2 月 SM9 标识加密算法，基于标识的非对称加密算法，作为国际标准 ISO/IEC 18033－5：2015/ADM1：2021《信息技术安全技术加密算法第 5 部分：基于标识的密码补篇 1：SM9》正式发布。

2.3 杂凑算法——SM3 算法

SM3 算法，又称杂凑算法。该算法可以对一定长度的消息，填充和迭代压缩后，生成长度为 256 比特的散列值，又称“数字指纹”，即使更改消息中的任意一个字符，对应的杂凑值也会改变。SM3 算法常用于数字签名和数据完整性保护。

SM3 算法于 2012 年 3 月成为中国商用密码标准（标准号为 GM/T 0004－2012）；2016 年 8 月成为国家密码标准（标准号为 GB/T 32905－2016）；2018 年 10 月，国际标准化组织（ISO）发布了包含我国 SM3 杂凑算法的 ISO/IEC 10118－3：2018《信息安全技术杂凑函数第 3 部分：专用杂凑函数》最新一版（第 4 版），SM3 算法正式成为国际标准。

3 数字电影中国密算法的应用

3.1 数字电影中密码技术应用

为促进数字电影规范发展，数字电影倡导组织 DCI（Digital Cinema Initiatives）发布了《数字电影系统规范》，为保护数字电影的安全，该规范规定：数字电影发行包必须在加密后才能传输。

（1）内容加密

数字电影由视频和声音组成，一部 2 小时的数字电影经过 JPEG 2000 编码后，大小为 100G 左右。由于数据量较大，DCI 规定电影内容采用加密速度快、加密效率高的高级加密标准 AES 进行加密，且使用 CBC 模式，128 比特的密钥长度。

发行方生成 AES 节目密钥，利用该密钥对节目的图像、声音和字幕进行加密，然后将 AES 节目密钥发送给接收方，接收方利用 AES 节目密钥对接收到的已加密的电影内容进行解密播放。

（2）内容传输完整

为了保证图像、声音等数据传输的完整性，发行方利用杂凑算法 SHA－1 对发送的数据计算杂凑值，并将其与数据一同发送给接收方，接收方接收到数据后，利用杂凑算法 SHA－1 算法对接收到的数据计算杂凑值，并与发行方计算的杂凑值进行对比。若两个值一样，则说明数据在传输的过程中没有被篡改。

（3）密钥传输安全

①AES 节目密钥传输安全

由于内容加密使用的是对称密码算法 AES，发行方需要把 AES 密钥发送给接收方，接收方才能正确解密。为了保证 AES 密钥分发的安全性，DCI 规定该 AES 节目密钥需要利用非对称加密算法 RSA，且密钥长度需使用 2048 比特的 RSA－2048 算法进行加密。

接收方生成RSA公私钥，私钥自己保存，RSA公钥发送给发行方，发行方利用接收方的RSA公钥对AES节目密钥进行加密，接收方利用自己的RSA私钥进行解密，获得AES节目密钥。

②RSA公钥传输安全

发行方需要使用接收方的RSA公钥对AES节目密钥进行加密，如何保证接收方的RSA公钥传输的安全性和完整性？DCI利用X509数字证书保证RSA公钥传输的安全性及完整性。

数字证书将个人信息与公钥进行绑定，并由权威机构证明其合法性。接收方将RSA公钥和个人信息发送给权威机构，权威机构利用RSA－2048算法对公钥和个人信息进行加密，并利用RSA－SHA256算法对其进行数字签名，生成数字证书，发送给接收方。接收方将权威机构生成的数字证书发送给发行方，发行方收到数字证书后，首先验证数字证书的签名是否正确，若正确，则从中提取公钥信息，得到接收方的RSA公钥。

（4）KDM正确

DCI规定AES节目密钥需要通过非对称加密算法RSA加密后保存在密钥传送消息（Key Delivery Message，KDM）文件中，传送给已授权的影院。KDM文件是一种基于影院外部消息（ETM，Extra-Theater Message）定义的XML文件。KDM在结构上分为三部分，即公开部分（Public）、私有部分（Private）和签名部分（Signature）。为了提高处理速度，发行方利用SHA-256算法分别对KDM的公开部分和私有部分计算杂凑值，然后利用自己的RSA私钥对公开部分和私有部分的杂凑值进行加密得到KDM文件的签名值，接收方利用从发行方X509数字证书中提取的发行方的RSA公钥验证KDM文件的数字签名是否正确，以确保接收到的KDM是正确的。

综上所述，为保障数字电影安全，DCI采用了加密效率高的对称加密算法AES-128-CBC算法加密数据量大的数字电影节目信息，之后采用加密强度大的非对称加密算法RSA-2048算法加密AES节目密钥，并通过X509数字证书和密钥传送消息KDM文件进行传输，以提高AES节目密钥的安全性，整个处理流程既高效且可靠。

3.2 数字电影中国密算法应用方案

根据相关学者的研究，国密算法的安全性与国际通用密码算法的安全性相当。汪朝晖等人[3]对比了ECC算法与RSA算法，得出ECC-210与RSA-2048安全水平相当，ECC-160与RSA-l024安全强度相当。由于SM2算法是在已有的ECC算法基础上研制的，SM2算法相当于ECC-256的安全强度，因此SM2算法可以取代RSA算法，满足各种应用在安全性上的要求，且在相同的安全强度下，SM2算法的密钥长度比RSA算法的密钥长度更短。姚键[4]，王小云等人[5]的研究表明SM3杂凑算法安全性较高。SM3杂凑算法与国际通用杂凑算法SHA-256实现效率相当。吕述望等人[6]的研究表明，与国际通用分组密码算法AES算法相比，SM4算法安全性较强。

国密算法自发布之日起，就被陆续应用在互联网通信[7][8]、银行信息系统[9]、电子政务[10]、物联网[11]、大数据安全[12]、卫生健康[13]、广播电视[14][15][16]等领域，利用国密算法实现数据加密、数据防篡改和身份认证等安全需求，保障人民个人隐私与数据安全。

表2 数字电影中国产密码应用方案

密码应用模块	现应用技术	拟改造方案
内容加密	AES-128	SM4
内容传输完整	SHA-1	SM3
密钥传输安全	RSA-2048、SHA－256、X509数字证书	SM2、SM3、国密数字证书
KDM正确	RSA-2048、SHA-256、X509数字证书	SM2、SM3、国密数字证书

综上所述，国密算法替代国际通用加密算法成为数字电影中的加密技术，为数字电影保驾护航是可行的。为满足国际通用加密算法和国密算法并行运行、实现平滑过渡的需求，本文拟采用以下方案：使用SM4算法代替AES-128算法加密节目内容，使用SM3算法代替SHA-1和SHA-256算法计算数据的杂凑值，利用SM2算法代替RSA-2048算法加

密节目密钥，使用国密数字证书代替国际 X509 数字证书保证公钥传输安全性和 KDM 签名正确性，具体如表 2 所示。

4 结束语

本文对国家商用密码算法在数字电影中的应用进行了探讨，主要对国密算法 SM1、SM2、SM3、SM4、SM7、SM9、ZUC 算法进行了介绍，并结合数字电影中密码技术的应用，提出了数字电影中国密算法应用方案，为电影行业技术人员正确有效使用国密算法提供思路，为推进电影领域国密算法的应用部署提供技术支持，让国产密码为电影行业的发展保驾护航，筑牢电影行业安全防线。❖

参考文献

[1] 全国人民代表大会．中华人民共和国密码法［EB/OL］．http：//www. npc. gov. cn/.

[2] 殷明．基于标识的密码算法 SM9 研究综述［J］．信息技术与信息化，2020（05）：88－93.

[3] 汪朝晖，张振峰．SM2 椭圆曲线公钥密码算法综述［J］．信息安全研究，2016，2（11）：972－982.

[4] 姚键．国产商用密码算法研究及性能分析［J］．计算机应用与软件，2019，36（06）：327－333.

[5] 王小云，于红波．密码杂凑算法综述［J］．信息安全研究，2015，1（01）：19－30.

[6] 吕述望，苏波展，王鹏，等．SM4 分组密码算法综述［J］．信息安全研究，2016，2（11）：995－1007.

[7] 林子康．基于国密算法的通讯加密系统研究及应用［D］．广东工业大学，2018.

[8] 周文辉，朱玉倩，宋宇飞．卫星互联网商用密码应用研究［J］．信息安全研究，2021，7（03）：263－267.

[9] 杨春雷．国密算法在国库信息系统中的应用研究［J］．金融科技时代，2021，29（07）：53－57.

[10] 黎水林，陈广勇，柳盈，等．商用密码在政府网站中的应用研究［C］//公安部第三研究所，江苏省公安厅，无锡市公安局．2019 中国网络安全等级保护和关键信息基础设施保护大会论文集．《信息网络安全》北京编辑部，2019：4.

[11] 苏彬庭，陈明志，许力，等．国密算法在工业互联网安全中的应用研究［J］．信息技术与网络安全，2021，40（03）：28－31.

[12] 王良田．数据存储及码流数据传输中的国密算法安全应用［J］．电子世界，2019（02）：160，163.

[13] 傅罡，赵梓辰，郭青．商用密码在卫生健康领域的应用与发展［J］．中国数字医学，2021，16（06）：9－13.

[14] 刘梦雨，尚文倩，林卫国．基于国密的多媒体版权保护与监管体系研究［J］．广播电视信息，2018（S1）：10－13.

[15] 黄大池，刘海章．国密算法在应急广播村村响系统中的应用［J］．西部广播电视，2020（02）：180－181，223.

[16] 吴钟乐，宫良，聂明杰．广电金卡支付系统国密算法应用研究［J］．广播与电视技术，2019，46（03）：62－65.

作者贡献声明：

李雪伟：设计论文框架，撰写和修订论文，全文文字贡献率 85%；

刘知一：指导论文框架设计，参与修订论文，全文文字贡献率 10%；

王木旺：参与修订论文，全文文字贡献率 5%。

A discussion on the application of Chinese national cryptographic algorithms in digital film

◎Li Xuewei, Liu Zhiyi, Wang Muwang (China Research Institute of Film Science and Technology)

Abstract: In order to practice the spirit of *Cryptography Law of the People's Republic of China*, which refers to encouraging development and popularising application towards national commercial cryptography, this paper briefly summarises the main features of Chinese national cryptographic algorithms such as SM1, SM2, SM3, SM4, SM7, SM9 and ZUC, then discusses solutions of Chinese national cryptographic algorithms that are used in digital film for application scenarios now. Through researches towards different categories of Chinese national cryptographic algorithms, the results show that it is completely feasible to use Chinese national cryptographic algorithms in the encryption and transmission of digital film content. This paper provides feasible support for the popularisation and application of Chinese national cryptographic algorithms used in digital film, while it may effectively accelerate the timetable for localising key technologies in this field.

Key words: Chinese national cryptographic algorithms; Digital film; Feasibility; Localisation