国密算法在国库信息系统中的应用研究

■ 中国人民银行西宁中心支行 杨春雷

摘 要：密码技术对于实现信息系统安全自主可控具有重要意义，特别是在金融信息系统领域。本文从算法、效率、安全性等方面简要阐述了商用密码在国内外的基本情况，结合国产密码SM2/3/4等在国库信息系统中的实际应用案例，讨论了在建立以国产商业密码为主要支撑的国库信息安全保障体系、实现底层密码算法自主可控等方面，国密改造所取得的成效。

关键词：国产密码；国产密码算法；国库信息系统

密码算法是用来加密和解密信息的数学表达，是数据安全交换的基础，对于信息安全的重要性不言而喻。随着科技的发展和社会的进步，世界各国都高度重视对密码算法的研究。1977年，美国国家标准和技术局NIST采用由IBM公司研发的对称加密算法DES，但该算法被现代计算机暴力破解，因此，美国政府采用高级加密标准AES来替代DES。到2006年，AES已经是对称密钥算法中最为流行的算法之一。1983年，麻省理工学院为RSA公钥密码算法申请了专利，这是一种非对称加密体制，从1978年提出到目前已超过40年，是业界公认的最优秀的公钥方案之一。1992年，美国科学家Ronald Linn Rivest设计并公开消息摘要算法MD5，该算法在RFC 1321标准中被加以规范，但1996年被证实可被破解，2004年被证实无法防止碰撞，因此，目前数字签名普遍采用美国国家安全局研发的安全散列函数SHA-2。

近年来，国家有关部门出于国家安全和长远战略的考虑，提出了研究国密算法、加强信息安全可控的要求，以彻底摆脱对国外密码算法和产品的依赖，取得了显著成绩。根据国家密码管理局最新消息，我国国密算法SM9正式成为ISO/IEC国际标准，标志着我国商用密码科技水平和国际标准化能力不断提升，进一步增强了我国商用密码产业的国际竞争力。根据《中华人民共和国密码法》第六条，密码分为核心密码、普通密码和商用密码，本文所述国密算法均指国产商用密码算法。

一、基于密钥的密码算法分类

（一）对称密码算法

对称密码算法是指加密和解密过程使用同一密

作者简介：杨春雷（1989-），男，青海化隆人，工程师，供职于中国人民银行西宁中心支行，研究方向：金融科技。
收稿日期：2021-04-21

钥的密码算法，该算法技术成熟，属于应用较早的密码算法。在对称密码算法中，消息发送方和接收方在进行安全通信之前，协商密钥和加密算法，发送方将明文和密钥经过加密算法加工后生成密文；消息接收方收到密文后，使用同一密钥和解密算法进行解密处理，还原出原始消息明文，如图1所示。

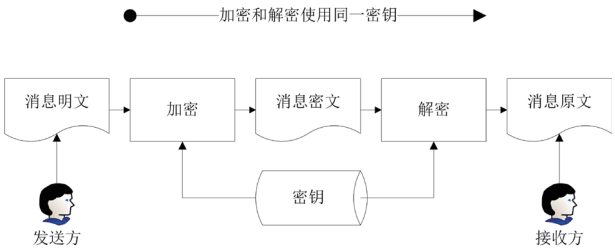

图1 对称加密过程

（二）非对称密码算法

非对称密码算法又叫公钥密码算法，通常需要两个成对的密钥，即公开密钥和私有密钥。在非对称密码算法中，消息发送方生成一对密钥并将公钥公开，然后用公钥和加密算法将消息明文加工后生成密文；接收方收到密文后，使用私钥和解密算法处理密文，还原出原始消息明文，如图2所示。

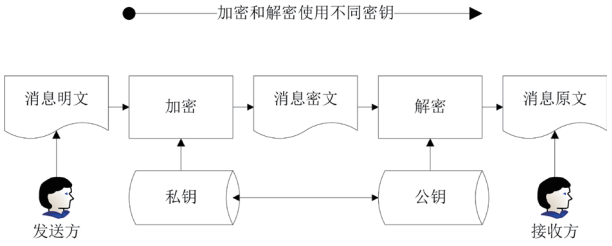

图2 非对称加密过程

（三）密码杂凑算法

密码杂凑算法也被称作哈希算法、散列算法，将任意长的消息经过一定的规则进行运算后输出定长消息，其运算过程不可逆，常用于实现数字签名服务。消息发送方用一个哈希函数对消息进行加工，得到消息摘要，再用自己的私钥对摘要进行加密，并附在消息原文后一同发送给接收方；接收方收到后对摘要部分后用公钥进行解密，再用相同的哈希算法处理消息原文得到消息摘要，最后比对两个摘要是否相同来判断消息原文是否被篡改，以及确定消息发送方的身份，如图3所示。

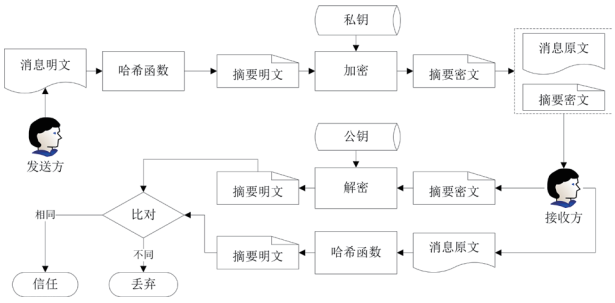

图3 数字签名过程

二、国产商用密码算法举例

（一）祖冲之（ZUC）序列密码算法

祖冲之（ZUC）密码算法属于对称密码算法，由我国自主设计完成。2011年，祖冲之（ZUC）密码算法被采纳为新一代宽带无线移动通信系统（LTE）国际标准，用于实现无线信道加密和完整性保护。这是我国商用密码算法首次在世界舞台亮相。ZUC算法输出的序列随机性较好、周期足够大，能够有效抵御弱密分析和序列密码分析，相关标准见表1所列。

表1 ZUC算法标准

标准编号	标准名称
GB/T33133.1-2016	信息安全技术 祖冲之序列密码算法 第一部分：算法描述
GM/T0001-2012	祖冲之序列密码算法

（二）国密算法SM2

SM2属于椭圆曲线密码算法（EllipticCurves Cryptography，ECC），属于非对称密码算法或公开密钥算法。2010年，国家密码管理局发布了第21号公号《SM2椭圆曲线公钥密码算法》，相关标准见表2所列。

表2 SM2算法标准

标准编号	标准名称
GB/T32918.1-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则
GB/T32918.2-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法
GB/T32918.3-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议
GB/T32918.4-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法
GB/T32918.5-2017	信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义
GM/T0003-2012	SM2椭圆曲线公钥密码算法
GM/T0009-2012	SM2密码算法使用规范
GM/T0010-2012	SM2密码算法加密签名消息语法规范
GM/T0015-2012	基于SM2密码算法的数字证书格式规范

SM2算法同样产生一对密码，使用公钥进行加密，私钥进行解密，并且在已知公钥的条件下求私钥在计算上不可行，从而保证了私钥的绝对安全。另外，相较于RSA等其他非对称密码算法而言，SM2使用更短的密钥串就能实现比较牢固的加密强度，同时由于其良好的数学设计结构，加密速度也比RSA算法快。

（三）国密算法SM3

SM3属于密码杂凑算法，国家密码管理局公布的中国商用密码杂凑算法标准见表3所列。

表3 SM3算法标准

标准编号	标准名称
GB/T32905-2016	信息安全技术 SM3密码杂凑算法
GM/T0004-2012	SM3密码杂凑算法

消息分组长度为512比特，输出摘要值长度为256比特，结构为Merkle-Damgard。SM3密码算法的压缩函数与SHA-256的压缩函数结构相似，但是设计更加复杂，效率和安全方面与SHA-256算法相当，主要用于数字签名以及生成消息认证码和随机数等。碰撞稳固性、原根稳固性和第二原根稳固性是摘要函数需满足的3个基本特性。2004年和2005年，我国密码学家王小云教授团队成功提出了高效的碰撞攻击算法破解MD5和SHA-1，因此这两种算法不再是安全的，而现今为止，SM3算法的安全性较高，未出现有效的碰撞攻击。

三、国密算法在国库信息系统中的应用

（一）国库信息系统业务架构

2018年，人民银行正式投产运行二代国库信息处理系统（TIPS），切实改善了财税民生服务，有效支撑了地方经济的健康发展。业务的不断发展，给人民银行网络安全建设和业务保障能力提出了更高要求。作为财税库关银横向联网系统的信息中枢，二代TIPS连接着国库、财政、税务、海关以及银行等机构，建立了国库收支的“大动脉”，在提高国库资金运行效率、服务财税体制改革、改善纳税主体服务体验等方面发挥了积极作用，是我国重要的财税金融基础设施，其架构如图4所示。

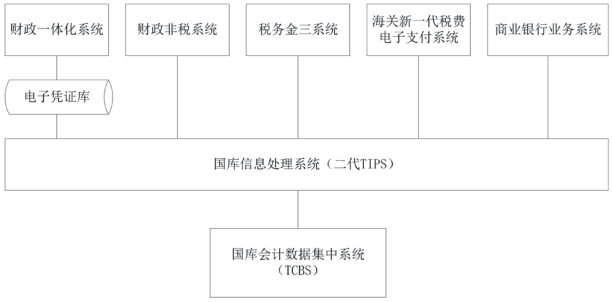

图4 财税库关银横向联网系统业务架构

目前，SM2/3/4等国产密码算法已经顺利成为ISO/IEC国际标准，此时推进二代TIPS外联机构国密改造具有重要意义。

（二）国密算法应用方案

2020年9月，人民银行总行国库局主持召开会议，对二代TIPS外联机构国产密码改造推广工作进行了安排部署。考虑到参与SM密码改造的银行机构和财政税务等非银行机构数量较多，特分批分时段有序推进部署工作，计划到2021年年中，所有外联机构全部完成切换上线。整个SM密码改造方案共分为3个阶段。

1. 准备工作

人民银行总行科技部门和分支机构科技部门分别对接一点接入机构和地方接入机构，制定详细的联调测试计划。外联机构准备支持SM密码的数字签名硬件设备，所选设备应在国家密码管理局支持的SM2/3/4商用密码产品目录中，同时向对接部门申请SM密码测试根证书和服务器证书。TIPS和外联机构均使用新签名服务接口替换原有的签名服务接口，实现应用程序升级。为满足新旧系统并行运行、实现平滑过渡的需要，改造后的系统应同时支持SM密码和RSA密码。可通过参数配置在两者之间进行切换，最后将SM密码测试根证书和服务器证书导入签名服务器，外联机构开展充分的内部测试和离线报文验签名测试后，再申请加入TIPS测试环境开展联调测试，如图5所示。

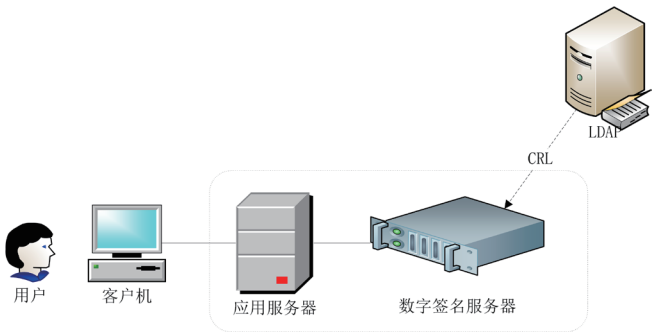

图5 签名服务改造示例

2. 联调测试

联调测试采用多轮迭代的方式进行，每一轮测试均安排SM密码场景和RSA密码场景。如迭代输出发现有程序缺陷，应尽快升级程序再进行回归测试，回归测试通过后更新测试用例进行下一轮迭代测试。从业务的角度看，功能测试应涵盖三方协议验证与撤销、实时扣税、批量扣税、银行端查询缴税、集中支付、实拨、明细对账等，以保证测试用例的有效覆盖面。从系统的角度看，性能测试应包括SM密码场景下接口响应时间、RSA密码场景下接口响应时间、SM密码场景与RSA密码场景下切换时间窗口等，除此之外，还应进行并发、容错等测试，以确定系统的吞吐量和鲁棒性等。

3. 验收和上线

验收标准为每条测试用例连续5笔测试通过。联调测试结束后，地方接入外联机构向人民银行分支机构科技部门提交功能测试报告、性能测试报告和问题反馈表。审核未达标的机构将组织进行二次测试，测试通过的外联机构统一提交至人民银行总行，由人民银行总行统筹安排上线工作。

（三）效果评价

1. 系统运行平稳未出现性能瓶颈

根据某地方性商业银行验收测试数据来看，SM密码算法改造后，业务逻辑未受影响，系统运行平稳，通过参数配置实现SM密码和RSA密码的快速切换，整个切换过程不到5分钟。从表4的性能测试数据来看，SM数字签名接口响应速度与RSA相差无几，不存在性能问题，因此可以断定，税收征缴入库、税费退库、财政支出等与国民经济生活息息相关的业务均不会因为国密算法改造而受到影响。

2. 消除国库信息系统安全隐患

国密算法SM在财税库关银横向联网系统中的成功实践，有效提升了系统安全等级，切实保障了数据传输的可靠性。目前，业界尚没有破解SM系列国产密

表4 某地方性商业银行验收测试数据

单位：毫秒

指标	RSA算法场景	SM算法场景
最大响应时间	2387	2132
最小响应时间	96	425
平均响应时间	1146	1295
错误率	0	0
并发数	100	100

码算法的案例，现阶段通过穷举攻击等方式暴力破解并不可行。SM3密码算法在对抗碰撞方面的优异表现，使得数字签名和验签服务更加高效安全，切实守牢国库资金安全和系统运行安全“两条底线”。

3. 落实密码算法自主可控国家战略

密码算法是支撑国家信息安全战略的核心技术，全方位应用具有自主知识产权的国密算法是保障信息安全的重要举措。国家推出SM系列密码算法从根本上摆脱了我国对国外密码技术的过度依赖，实现了从密码算法层面掌控核心信息安全技术。SM系列国产密码算法在国库信息系统及其外联机构信息系统中的成功实践，真正让自主可控的国家信息安全战略落到了实处，对推动国密算法在金融领域乃至全国各行各业的全面应用具有重要的借鉴意义。

四、未来展望

在国密算法日趋成熟的今天，在央行国库信息系统安全领域全面推广应用国密算法正合时宜。目前，财税库关银横向联网系统中以商业银行为主的外联机构已全部完成SM国密算法改造联调测试工作，将于2021年年中全面投产运行。下一阶段，为实现国密算法在国库信息系统中的全面覆盖，建议从以下3个方面持续推进国密算法改造工作。

一是将国密算法改造工程纳入国家“金库工程”。目前，国库会计数据集中系统（TCBS）作为国库信息系统的核心系统，仍然存在部分签名逻辑使用非国密算法的情况，比如户身份认证使用的是以USBKey专用产品为载体的CA证书，内置的密码算法为国际加密标准RSA算法，应将其逐步替换为国产SM系列密码算法，在提升国库履职水平的同时，筑牢系统安全防线。

二是积极推进财政支出无纸化项目实现国密算法全覆盖。财政实行国库集中支付改革以来，在人民银行、财政、代理银行三端同步部署的电子凭证库衔接着财库银各方业务系统，实现对各类电子单据的电子签章和数字签名。但目前全国大多数省份使用的仍然是国际加密标准RSA算法，出于系统安全和自主可控的考虑，应采购符合国家密码管理局相关规定的签名服务设备进行接口替换。

三是协调推进税务、海关等直连二代TIPS的外联机构进行国密改造。二代TIPS通过连接财税库关银等机构的核心系统组建起国库收支的一张“金融大网”。要提升如此庞大的金融网络的安全性，就势必要求这张“大网”中的每个参与者同步实施以国密改造为主的安全工程。因此，必须牢牢把握国家“金税工程”“金关工程”等契机，全面推动税务、海关等国密算法改造进程，实现财税库关银横向联网这张“大网”密码算法的完全国产化，确保财政预算和国库收支安全高效运转。FTT

参考文献：

[1]文学. 国密算法在央行应用的实践分析[J]. 金融科技时代，2017(2):58-60.

[2]谢宗晓，董坤祥，甄杰. 国产商用密码算法及其相关标准介绍[J]. 中国质量与标准导报，2020(6):12-14.

[3]祁凌. 基于PKI技术下的电子商务信息安全研究[J]. 网络安全技术与应用，2020(12):127-129.

[4]董贞良. 密码算法应用及国际标准化情况[J]. 金融电子化，2018(10):54-55.

[5]秦志光. 密码算法的现状和发展研究[J]. 计算机应用，2004(2):1-4.