密码算法专题概要
Introduction to Issue of Cryptographic Algorithm

我国密码算法应用情况

□ 谢永泉

密码作为维护国家网络与信息安全的核心技术和基础支撑，在维护国家网络空间安全、信息安全、经济安全等方面发挥着重要作用。密码算法是最基础、最重要的密码技术。国家密码管理局高度重视密码算法管理工作，近 10 年来，发布了 SM2 公钥密码算法、SM3 密码杂凑算法、SM4 分组密码算法、SM9 标识密码算法等 SM 系列算法及 ZUC 序列密码算法，构成了包括对称密码算法、非对称密码算法、杂凑密码算法、标识密码算法和序列密码算法的完整、自主的国产密码算法体系。作为我国大力推广的国产密码算法，尤其是在上述算法成为密码行业标准后，SM 系列算法和 ZUC 算法的应用取得显著成绩，为促进商用密码发展、保障我国信息安全发挥了巨大作用。

目前，SM 系列算法和 ZUC 等国产密码算法在商用密码产品中得到广泛采用，经审批的产品几乎全部实现了对上述一种或几种密码算法的支持，相关产品总数逾 1600 余款，其中支持 SM2/SM3/SM4 算法的产品总数达 700 款，涵盖了密码芯片、密码板卡、密码整机、密码系统等各种产品类型，形成了完善的基于国产密码算法的产业支撑能力。随着商用密码产品应用领域不断扩大、应用程度不断加深，国产密码算法的应用呈现 3 个特点：数量大——2015 年度全国共销售含有上述算法的商用密码产品 49 355.34 万台（套），销售总额为 123.32 亿元，市场规模可观，所带来的用户数量，附加价值和社会、经济效益更为显著；范围广——国产密码算法已经大规模应用于电信网、广播电视网、互联网等基础信息网络，能源、教育、公安、社保、交通、卫生计生、金融等涉及国计民生和基础信息资源的重要信息系统，石油石化、电力系统、交通运输、城市设施等重要工业控制系统，以及党政机关和使用财政性资金的事业单位、团体组织使用的面向社会服务的政务信息系统中；认同高——自 SM 系列算法和 ZUC 算法陆续作为标准颁布以来，必须支持国产密码算法已经成为各行业、各领域在体系规划、方案设计、产品选型、系统建设和对外宣传中的共识，这既体现了用户单位自觉遵守国家密码管理政策法规意识的提升，也说明经过多年的积累和发展，国产密码算法在安全性、高效性、易用性等方面应用表现优异，完全可以取代国际算法，得到用户单位的高度认同。以下分别简介各个算法的应用情况。

SM2 算法是基于椭圆曲线的公钥密码算法，目前支持 SM2 算法的产品已达 1000 余款，广泛应用于电子政务、移动办公、电子商务、移动支付、电子证书等基础设施、云服务等领域。以《中华人民共和国电子签名法》为依据，各类应用数字签名 / 验签的旺盛需求，催生出一批支持 SM2 算法高性能产品，如中国科学院 DCS 中心研制的高性能金融数据密码机 SM2 签名速率超过 33 万次 / 秒；清华大学微电子所研制的单颗算法芯片 SM2 签名速率达 81 763.03 次 / 秒。在公钥基础设施（PKI）领

域，以基于SM2算法的数字证书应用最具有代表性，尤其是自2011年国家密码管理局发布公钥算法升级工作通知以来，全国总计有45家第三方电子认证服务机构（CA）完成了支持SM2算法的系统新建或升级改造，工行、农行、建行、交行、税务、海关、交通、教育等12家系统性电子认证服务系统也实现了对SM2算法的支持，累计证书发行量近亿张，支持SM2算法的智能密码钥匙、IC卡的芯片出货量达5亿颗，有力地促进了SM2算法在交通、能源、金融、税务、公安、卫生、社保、教育等多个领域的应用。SM2算法也已被纳入可信计算组织（TCG）发布的可信平台模块库规范（TPM2.0），由国民技术研制的支持TPM2.0的Z32H320TC系列芯片集成了SM2算法，被应用在微软于中国发售的Microsoft Surface Pro 3 pad中。

SM3算法作为标准杂凑算法使用非常广泛。目前支持SM3算法的产品已达1 100多款，包括安全芯片、终端、设备和应用系统，采用SM3算法的产品和系统运行安全稳定。如在智能电网领域，截至2016年10月，采用SM3算法的智能电表已经安装近6亿用户，均能安全稳定运行。在金融系统，目前大约有7亿多银行磁条卡更新为密码芯片卡，动态令牌累计发行7 726万支，这些卡片及令牌均使用了SM3算法。SM3算法也支持可信计算组织（TCG）发布的可信平台模块库规范（TPM2.0）。该算法业已成为我国电子签名类密码系统、计算机安全登录系统、计算机安全通信系统、数字证书、网络安全基础设施、安全云计算平台与大数据等领域信息安全的基础技术。

SM4算法最初作为无线局域网专用密码算法发布，后成为分组密码算法行业标准。目前支持SM4算法的产品已达700余款，覆盖了各种有对称加密需求的应用。由于SM4算法最初用于无线局域网芯片WAPI协议中，支持SM4算法的WAPI无线局域网芯片已超过350多个型号，全球累计出货量超过70亿颗。在金融领域，仅统计支持SM4算法的智能密码钥匙出货量已超过1.5亿支。此外，SM4算法已被纳入可信计算组织（TCG）发布的可信平台模块库规范（TPM2.0）中。国际上已有IBM公司与中国厂商合作完成了面向IBM_{z13}主机的密码中间件，可用于实现SM4算法与IBM_{z13}主机的兼容。

SM9密码算法为标识密码算法，随着基于标识的密码技术（IBC）受到越来越多的关注，标识密码算法的应用发展迅速。虽然因SM9算法标准发布较晚（2016年4月发布），目前支持SM9算法的产品数量尚少（6款），但由于IBC技术灵活易用和方便管理的特点，SM9算法的应用需求十分旺盛。自标准发布以来，已有厂商着手研制支持SM9算法的智能密码钥匙、标识密码机、密钥管理系统等系列基础产品，更多的应用单位基于SM9算法设计其系统方案。可以预见的是，SM9算法将会在更广阔的领域发挥其自身优势，作为PKI技术的有益补充，应用前景十分可观。

ZUC算法最初是面向4G LTE空口加密设计的序列密码算法，2011年被3GPP LTE采纳为国际加密标准（3GPP TS 33.401），因此ZUC算法目前主要用于通信领域。根据工信部反馈情况，4G入网检测已要求手机终端全部支持ZUC算法；中国移动针对4G LTE/VoLTE网络及窄带物联网（NB-IOT）的空口接入要求全面支持ZUC算法，并以《中国移动VoLTE试点测试规范》和《中国移动窄带物联网安全规范》形式明确。此外，中国移动研制的智能加密移动终端、三零瑞通研制的VoIP语音加密系统以及兴唐通信研制的链路密码机等密码产品中也都率先支持了ZUC算法，为ZUC算法

的进一步推广应用打下坚实基础。

国家密码管理局已经发布了 44 个密码行业标准（参见国家商用密码管理网站：www.oscca.gov.cn），对密码算法，商用密码产品，密码应用系统等的设计、检测和应用等予以规范。SM2/3/4/9 和 ZUC 密码算法已经发布为国家标准，其中 SM3 密码杂凑算法正在 ISO 面向国家成员体进行投票，有望于今年年底到 2017 年上半年发布，正式成为国际标准； SM2/4/9 密码算法的国际标准推进工作也在积极进行中。

目前，国家正在大力推进自主密码技术在金融领域以及基础信息网络、重要信息系统、重要工业控制系统和面向公众服务的政务信息系统中的全面应用，SM 系列算法和 ZUC 算法受到越来越多的关注。我们组织相关专家撰写了系列算法综述，较为系统地对这些算法的体系结构、密码学特性、抵抗密码攻击的能力等特征予以介绍，并以附录的形式给出了这些算法的 C 语言实现，以更好地满足学术机构、产业单位、应用部门等对密码算法的研究和应用需求。

» 本期专题组稿专家

谢 永 泉

谢永泉（yqxie_oscca@263.com），博士，密码行业标准化技术委员会总体组组长，全国信息安全标准化技术委员会 WG3 工作组副组长，工业与信息化部电子签名专家委员会委员。SM3 算法主要设计者之一。组织并参与《证书认证系统密码及其相关安全技术规范》等 20 多个国家标准或行业标准的制修订工作。获得国家科技进步二等奖一次、省部级科技进步一等奖三次。