国际标准

自主密码算法与协议成为ISO/IEC国际标准

主要完成人：张振峰、 张立武、刘丽敏等

联系方式（张严、13552567403、zhangyan@tca.iscas.ac.cn）

2017年11月，ISO/IEC14888-3/AMD1通过国家成员体投票，SM2/SM9数字签名算法正式成为国际标准，标志着我国商用密码算法走向国际，对于增强我国密码产业在国际上的核心竞争力具有重要的意义。SM2/SM9数字签名算法是我国国家密码管理局发布的数字签名标准。数字签名，又称电子签名，用于保证身份的真实性、数据的完整性和行为的不可否认性等，是世界各国保障网络空间安全、构建可信可控信息技术体系的密码重器。

SM2/SM9算法由我所研究员张振峰主持设计并负责国际标准化工作。

ISO/IEC 20009系列标准 “信息技术 安全技术 匿名实体鉴别”，是一类基础技术机制标准，主要解决在实体件鉴别中的隐私保护问题。ISO/IEC 20009-4 :2017为第 4 部分: 基于弱秘密的机制。

该标准于2017年8月颁布，共收录了3种机制，其中YZ机制为我所研究员张振峰主持设计，张立武负责国际标准化工作。

匿名实体鉴别可在完成实体合法性资格验证的同时保护用户具体身份，对于保护用户身份隐私具有重要意义。口令容易被暴力攻击和离线字典攻击，基于口令设计匿名实体鉴别面临双重挑战，必须进行精心设计，YZ机制巧妙地结合基于口令的安全协议实现了匿名实体鉴别。