doi:10.1631/FITEE.1700005

题目：再议防二重认证签名：新定义和基于变色龙哈希的构造

概要：防二重认证签名（DAPS）是在 ESORICS 2014 会议上提出的一种新型电子签名。防二重认证性质指同一主题上两个不同消息的签名可以用来摧毁整个签名体系。其提出者已指出防二重认证签名的几个潜在应用场景，比如，在数字证书领域，可以提供针对证书颁发机构（CA）的自我约束体制，使其不敢违规提供假冒证书。本文主要考虑防二重认证签名的基础性质。提出一种适度弱化条件的新定义，同时为刻画防二重认证性质而保持足够性质强度。提出带密钥泄露的可逆变色龙哈希函数的新密码原型。提出防二重认证签名方案的通用构造，同时基于带密钥泄露的可逆变色龙哈希函数性质给出安全性证明。在此通用型防二重认证签名方案框架下，分别基于整数分解、不对称密码算法（RSA）和狄菲-赫尔曼计算（CDH）假设构造了 3 个具体的防二重认证签名方案。这些方案比现有的防二重认证签名方案效率更高。相比现有方案，分别基于 RSA 和 CDH 的两个新方案不再依赖可信系统建立模型。

关键词：防二重认证签名；变色龙哈希函数；数字签名；可证明安全；权威信任层次