密码行业标准化技术委员会

密标委〔2018〕5号

密码行业标准修改通知单

GM/T 0044.5—2016《SM9 标识密码算法 第5部分：参数定义》第2号修改单

经国家密码管理局批准，GM/T 0044.5—2016《SM9 标识密码算法 第5部分：参数定义》修改内容如下。

序号	章节	原内容	修改后内容
1	D.1 一般要求	在此示例中，分组长度为128比特，填充方式遵循PKCS#5，工作模式为ECB	在此示例中，分组长度为128比特，填充方式遵循PKCS#7，工作模式为CBC，初始向量IV＝00000000 00000000 00000000 00000000
2	D.2 公钥加解密		C_2、C_3、C值，以及u值要经重新计算后修改，修改后的完整附录D见附件

本修改单自即日起生效。

密码行业标准化技术委员会

2018年3月9日