密码行业标准化技术委员会

密标委〔2018〕3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1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	3.2	式（3）进行三次扩张的约化多项式为：x^3-v，$v^2=u$，$v=\sqrt[3]{\sqrt{-2}}$	式（3）进行三次扩张的约化多项式为：x^3-v，$v^2=u$，$v=\sqrt{\sqrt{-2}}$
2	附录B	hid：0x02	hid：0x03， 根据hid=0x03的值对附录B示例数据进行修改，修改后的完整附录B见附件

本修改单自即日起有效。

密码行业标准化技术委员会

2018年1月29日