NIST 特别出版物 800-186
草案

国家标准和技术研究所
美国商务部

有关基于离散对数算法的密码的建议：

椭圆曲线域参数

内部资料

翻译：高卓

Lily Chen
Dustin Moody
Andrew Regenscheid
信息技术实验室计算机安全部

Karen Randall
Randall 咨询公司

本出版物英文版可从以下网址免费获得：
https://doi.org/10.6028/NIST.SP.800-186-draft

2019 年 10 月

美国商务部
Wilbur L. Ross Jr.，部长
国家标准和技术研究所
Walter Copan，商务部副部长兼 NIST 所长

北京江南天安科技有限公司

目录