

密码密钥生成建议

内部资料

翻译：高卓

Elaine Barker

Allen Roginsky

信息技术实验室计算机安全部

Richard Davis

国家安全局

本出版物英文版可从以下网址免费获得：

<http://dx.doi.org/10.6028/NIST.SP.800-133r2>

2020 年 6 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

目录

- 1 介绍
 - 2 定义、缩略语和符号
 - 2.1 定义
 - 2.2 缩略语
 - 2.3 符号和术语
 - 3 总论
 - 3.1 密钥的生成
 - 3.2 何处生成密钥
 - 3.3 支持特定安全强度
 - 4 随机位生成器输出的使用
 - 5 非对称密钥算法的密钥对生成
 - 5.1 用于数字签名方案的密钥对
 - 5.2 用于密钥建立的密钥对
 - 5.3 密钥对的分发
 - 5.4 密钥对的更换
 - 6 对称密钥算法的密钥生成
 - 6.1 对称密钥的“直接生成”
 - 6.2 对称密钥的派生
 - 6.2.1 通过密钥协定方案生成的对称密钥
 - 6.2.2 从预先存在的密钥派生的对称密钥
 - 6.2.3 从口令派生的对称密钥
 - 6.3 （多个）密钥与其他数据组合生成的对称密钥
 - 6.4 对称密钥分发
 - 6.5 对称密钥更换
- 参考文献