

有关密钥建立方案所用 密钥派生方法的建议

内部资料
翻译：高卓

Elaine Barker
Lily Chen
Richard Davis

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.800-56Cr2-draft>

2020 年 3 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

- 1 介绍
- 2 范围和目的
- 3 定义、符号和缩略语
 - 3.1 定义
 - 3.2 符号和缩略语
- 4 一步密钥派生
 - 4.1 有关密钥派生函数的规定
 - 4.2 辅助函数 $H(x)$ 和相关参数
- 5 两步密钥派生
 - 5.1 有关密钥派生规程的规定
 - 5.2 辅助 MAC 算法和相关参数
 - 5.3 先随机提取，然后多密钥扩展
- 6 应用特有的密钥派生方法
- 7 挑选散列函数和 MAC 算法
- 8 进一步的讨论
 - 8.1 使用截断版散列函数
 - 8.2 挑选盐值
 - 8.3 用于提取和扩展的 MAC 算法
 - 8.4 销毁本地保存的敏感数据
- 附录 A 参考文献

