NIST 特别出版物 800-56B
第 2 修订版

国家标准和技术研究所
美国商务部

# 有关使用整数因子分解密码的成对密钥建立方案的建议

**内部资料**

翻译：高卓

**Elaine Barker**
**Lily Chen**
**Allen Roginsky**
**Apostol Vassilev**
**Richard Davis**
**Scott Simon**

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.800-56Br2

**2019 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