

# 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

- 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 密钥建立方案概述
  - 4.1 密钥建立准备
  - 4.2 密钥协定流程
  - 4.3 密钥传输流程
- 5 密钥元素
  - 5.1 密码散列函数
  - 5.2 消息认证代码 (MAC) 算法
    - 5.2.1 密钥确认的 *MacTag* 计算
    - 5.2.2 密钥确认的 *MacTag* 验证
  - 5.3 随机位生成器
  - 5.4 Nonce
  - 5.5 用于密钥建立方案的密钥派生方法
    - 5.5.1 执行密钥派生
    - 5.5.2 *FixedInfo*
      - 5.5.2.1 一步密钥派生
        - 5.5.2.1.1 *FixedInfo* 的连结格式
        - 5.5.2.1.2 *FixedInfo* 的 ASN.1 格式
      - 5.5.2.2 两步密钥派生 (先提取后扩展)
      - 5.5.2.3 *FixedInfo* 的其他格式
  - 5.6 密钥确认
    - 5.6.1 密钥建立方案的单边密钥确认
    - 5.6.2 KAS2 方案的双边密钥确认
    - 5.6.3 挑选 MAC 和其他密钥确认参数
- 6 RSA 密钥对
  - 6.1 总体要求
  - 6.2 用于密钥建立的 RSA 密钥对准则
    - 6.2.1 密钥对定义
    - 6.2.2 格式
  - 6.3 RSA 密钥对生成器
    - 6.3.1 RSAKPG1 系列: 公钥指数固定的 RSA 密钥对生成
      - 6.3.1.1 *rsakpg1-basic*
      - 6.3.1.2 *rsakpg1-prime-factor*
      - 6.3.1.3 *rsakpg1-crt*
    - 6.3.2 RSAKPG2 系列: 公钥指数随机的 RSA 密钥对生成

- 6.3.2.1 *rsakpg1-basic*
- 6.3.2.2 *rsakpg1-prime-factor*
- 6.3.2.3 *rsakpg1-crt*
- 6.4 被要求的保证
  - 6.4.1 密钥对拥有者要求的保证
    - 6.4.1.1 拥有者获得密钥对有效性保证
    - 6.4.1.2 RSAKPV1 系列：公钥指数固定的 RSA 密钥对验证
      - 6.4.1.2.1 *rsakpv1-basic*
      - 6.4.1.2.2 *rsakpv1-prime-factor*
      - 6.4.1.2.3 *rsakpv1-crt*
    - 6.4.1.3 RSAKPV2 系列：公钥指数随机的 RSA 密钥对验证
      - 6.4.1.3.1 *rsakpv2-basic*
      - 6.4.1.3.2 *rsakpv2-prime-factor*
      - 6.4.1.3.3 *rsakpv2-crt*
    - 6.4.1.4 RSA 密钥对验证（指数创建方法未知）
      - 6.4.1.4.1 *basic-pkv*
      - 6.4.1.4.2 *prime-factor-pkv*
      - 6.4.1.4.3 *crt-pkv*
    - 6.4.1.5 拥有者要求的私钥拥有保证
  - 6.4.2 公钥接收者要求的保证
    - 6.4.2.1 为收到的公钥获得公钥有效性保证
    - 6.4.2.2 RSA 的部分公钥验证
    - 6.4.2.3 接收者要求的拥有者拥有私钥的保证
      - 6.4.2.3.1 接收者从一个可信第三方得到保证
      - 6.4.2.3.2 接收者直接从宣称的拥有者（即另一方）处得到保证
- 7 基元和运算
  - 7.1 加密和解密基元
    - 7.1.1 RSAEP
    - 7.1.2 RSADP
      - 7.1.2.1 用基本格式私钥解密
      - 7.1.2.2 用素因子格式私钥解密
      - 7.1.2.3 用 CRT 格式私钥解密
  - 7.2 加密和解密运算
    - 7.2.1 RSA 秘密值封装（RSASVE）
      - 7.2.1.1 RSASVE 的成分
      - 7.2.1.2 RSASVE 生成运算（RSASVE.Generate）
      - 7.2.1.3 RSASVE 恢复运算（RSASVE.Revocer）
    - 7.2.2 含最优非对称加密填充的 RSA（RSA-OAEP）
      - 7.2.2.1 RSA-OAEP 的成分
      - 7.2.2.2 掩码生成函数（MGF）
      - 7.2.2.3 RSA-OAEP 加密运算（RSA-OAEP.Encrypt）
      - 7.2.2.4 RSA-OAEP 解密运算（RSA-OAEP.Decrypt）
- 8 密钥协定方案

- 8.1 密钥协定的常见成分
- 8.2 KAS1 密钥协定
  - 8.2.1 KAS1 的假设
  - 8.2.2 KAS1-basic
  - 8.2.3 KAS1 的密钥确认
    - 8.2.3.1 KAS1 的密钥确认成分
    - 8.2.3.2 KAS1-Party\_V-confirmation
- 8.3 KAS2 密钥协定
  - 8.3.1 KAS2 的假设
  - 8.3.2 KAS2-basic
  - 8.3.3 KAS2 的密钥确认
    - 8.3.3.1 KAS2 的密钥确认成分
    - 8.3.3.2 KAS2-Party\_V-confirmation
    - 8.3.3.3 KAS2-Party\_U-confirmation
    - 8.3.3.4 KAS2-bilateral-confirmation
- 9 密钥传输方案**
  - 9.1 附加输入
  - 9.2 KTS-OAEP: 使用 RSA-OAEP 的密钥传输
    - 9.2.1 KTS-OAEP 的假设
    - 9.2.2 共通成分
    - 9.2.3 KTS-OAEP-basic
    - 9.2.4 KTS-OAEP 的密钥确认
      - 9.2.4.1 KTS-OAEP 用于密钥确认的共通成分
      - 9.2.4.2 KTS-OAEP-Party\_V-confirmation
  - 9.3 混合型密钥传输方法
- 10 挑选具体方案的理由阐述**
  - 10.1 选择 KAS1 密钥协定方案的理由阐述
  - 10.2 选择 KAS2 密钥协定方案的理由阐述
  - 10.3 选择 KTS-OAEP 密钥传输方案的理由阐述
  - 10.4 与密钥建立方案相关的保证归纳
- 11 密钥恢复**
- 12. 执行方案验证**
- 附录 A 参考文献**
  - A.1 标准类参考文献
  - A.2 资料类参考文献
- 附录 B 数据转换（标准类信息）**
  - B.1 整数向字节串（I2BS）的转换
  - B.2 字节串向整数（BS2I）的转换
- 附录 C 素因子恢复（标准类信息）**
  - C.1 概率性素因子恢复
  - C.2 确定性素因子恢复
- 附录 D IFC 模长的最大安全强度估值**
- 附录 E 修订历史（资料类信息）（略）**