

# 有关使用离散对数密码的 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

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.800-56Ar3>

2018 年 4 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 基于 DLC 的密钥传输
- 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 MAC 标记计算
    - 5.2.2 密钥确认的 MAC 标记验证
  - 5.3 随机数生成
  - 5.4 Nonce
  - 5.5 域参数
    - 5.5.1 域参数的挑选/生成
      - 5.5.1.1 FFC 域参数的挑选/生成
      - 5.5.1.2 ECC 域参数的挑选
    - 5.5.2 域参数的有效性保证
    - 5.5.3 域参数管理
  - 5.6 密钥建立密钥对
    - 5.6.1 密钥对生成
      - 5.6.1.1 FFC 密钥对生成
        - 5.6.1.1.1 使用得到批准的安全素数群
        - 5.6.1.1.2 使用 FIPS 186 型 FFC 参数大小集
        - 5.6.1.1.3 通过额外随机位生成密钥对
        - 5.6.1.1.4 通过测试候选对象生成密钥对
      - 5.6.1.2 ECC 密钥对生成
        - 5.6.1.2.1 通过额外随机位生成密钥对
        - 5.6.1.2.2 通过测试候选对象生成密钥对
    - 5.6.2 被要求的保证
      - 5.6.2.1 密钥对拥有者要求的保证
        - 5.6.2.1.1 拥有者要求的正确生成保证
        - 5.6.2.1.2 拥有者要求的私钥有效性保证
        - 5.6.2.1.3 拥有者要求的公钥有效性保证
        - 5.6.2.1.4 拥有者要求的成对一致性保证
        - 5.6.2.1.5 拥有者要求的私钥拥有保证

- 5.6.2.2 公钥接收者要求的保证
  - 5.6.2.2.1 接收者要求的静态公钥有效性保证
  - 5.5.2.2.2 接收者要求的临时公钥有效性保证
  - 5.6.2.2.3 接收者要求的拥有者拥有静态私钥的保证
  - 5.6.2.2.4 接收者要求的拥有者拥有临时私钥的保证
- 5.6.2.3 公钥验证例程
  - 5.6.2.3.1 FFC 完全公钥验证例程
  - 5.6.2.3.2 FFC 部分公钥验证例程
  - 5.6.2.3.3 ECC 完全公钥验证例程
  - 5.6.2.3.4 ECC 部分公钥验证例程
- 5.6.3 密钥对管理
  - 5.6.3.1 有关静态和临时密钥对的要求
  - 5.6.3.2 有关静态密钥对的具体要求
  - 5.6.3.3 有关临时密钥对的具体要求
- 5.7 DLC 基元
  - 5.7.1 Diffie-Hellman 基元
    - 5.7.1.1 有限域密码 Diffie-Hellman (FFC DH) 基元
    - 5.7.1.2 椭圆曲线密码代数余子式 Diffie-Hellman (ECC CDH) 基元
  - 5.7.2 MQV 基元
    - 5.7.2.1 有限域密码 MQV (FFC MQV) 基元
      - 5.7.2.1.1 FFC MQV 基元的 MQV2 形式
      - 5.7.2.1.2 FFC MQV 基元的 MQV1 形式
    - 5.7.2.2 ECC MQV 的副值函数
    - 5.7.2.3 椭圆曲线密码的 MQV (ECC MQV) 基元
      - 5.7.2.3.1 ECC MQV 基元的完全 MQV 形式
      - 5.7.2.3.2 ECC MQV 基元的一次传递形式
- 5.8 密钥协定方案的密钥派生方法
  - 5.8.1 执行密钥派生
  - 5.8.2 FixedInfo
    - 5.8.2.1 一步密钥派生
      - 5.8.2.1.1 FixedInfo 的连结格式
      - 5.8.2.1.2 FixedInfo 的 ASN.1 格式
    - 5.8.2.2 两步密钥派生 (先提取后扩展)
    - 5.8.2.3 FixedInfo 的其他格式
- 5.9 密钥确认
  - 5.9.1 密钥协定方案的单边密钥确认
  - 5.9.2 密钥协定方案的双边密钥确认
  - 5.9.3 挑选 MAC 和其他密钥确认参数
- 6 密钥协定方案**
  - 6.1 使用两个临时密钥对的方案 C(2e)
    - 6.1.1 C(2e, 2s)方案
      - 6.1.1.1 dhHybrid1, C(2e, 2s, FFC DH)方案
      - 6.1.1.2 (代数余子式) 完全统一模型, C(2e, 2s, ECC CDH)方案

- 6.1.1.3 MQV2, C(2e, 2s, FFC MQV)方案
- 6.1.1.4 完全 MQV, C(2e, 2s, ECC MQV)方案
- 6.1.1.5 将密钥确认纳入 C(2e, 2s)方案
  - 6.1.1.5.1 U 方向 V 方提供单边密钥确认的 C(2e, 2s)方案
  - 6.1.1.5.2 V 方向 U 方提供单边密钥确认的 C(2e, 2s)方案
  - 6.1.1.5.3 含双边密钥确认的 C(2e, 2s)方案
- 6.1.2 C(2e, 0s)方案
  - 6.1.2.1 dhEphem, C(2e, 0s, FFC DH)方案
  - 6.1.2.2 (代数余子式) 临时统一模型, C(2e, 0s, ECC CDH)方案
  - 6.1.2.3 C(2e, 0s)方案的密钥确认
- 6.2 使用一个临时密钥对的方案 C(1e)
  - 6.2.1 C(1e, 2s)方案
    - 6.2.1.1 dhHybridOneFlow, C(1e, 2s FFC DH)方案
    - 6.2.1.2 (代数余子式) 一次传递统一模型, C(1e, 2s, ECC CDH)方案
    - 6.2.1.3 MQV1, C(1e, 2s, FFC MQV)方案
    - 6.2.1.4 一次传递 MQV, C(1e, 2s, ECC MQV)方案
    - 6.2.1.5 将密钥确认纳入 C(1e, 2s)方案
      - 6.1.1.5.1 通过 U 方提供给 V 方的单边密钥确认执行的 C(1e, 2s)方案
      - 6.1.1.5.2 通过 V 方提供给 U 方的单边密钥确认执行的 C(1e, 2s)方案
      - 6.1.1.5.3 通过双边密钥确认执行的 C(1e, 2s)方案
  - 6.2.2 C(1e, 1s)方案
    - 6.2.2.1 dhOneFlow, C(1e, 1s FFC DH)方案
    - 6.2.2.2 (代数余子式) 一次传递 Diffie-Hellman, C(1e, 1s, ECC CDH)方案
    - 6.2.2.3 将密钥确认纳入 C(1e, 1s)方案
      - 6.2.3.3.1 通过 V 方提供给 U 方的单边密钥确认执行的 C(1e, 1s)方案
- 6.3 C(0e, 2s)方案
  - 6.3.1 dhStatic, C(0e, 2s, FFC DH)方案
  - 6.3.2 (代数余子式) 静态统一模型, C(0e, 2s, ECC CDH)方案
  - 6.3.3 将密钥确认纳入 C(0e, 2s, ECC CDH)方案
    - 6.3.3.1 通过 U 方提供给 V 方的单边密钥确认执行的 C(0e, 2s)方案
    - 6.3.3.2 通过 V 方提供给 U 方的单边密钥确认执行的 C(0e, 2s)方案
    - 6.3.3.3 通过双边密钥确认执行的 C(0e, 2s)方案

## 7 挑选具体方案的理由阐述

- 7.1 选择 C(2e, 2s)方案的理由阐述
- 7.2 选择 C(2e, 0s)方案的理由阐述
- 7.3 选择 C(1e, 2s)方案的理由阐述
- 7.4 选择 C(1e, 1s)方案的理由阐述
- 7.5 选择 C(0e, 2s)方案的理由阐述
- 7.6 与密钥协定方案相关的保证归纳

## 8 密钥恢复

## 9. 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 将标识符和其他上下文特有信息收入密钥派生方法输入的理由阐述（资料类信息）**

**附录 C 数据转换（标准类信息）**

C.1 整数向字节串的转换

C.2 域元素向字节串的转换

C.3 域元素向整数的转换

C.4 位串向整数的转换

**附录 D 得到批准的 ECC 曲线和 FFC 安全素数群**

**附录 E 修订历史（资料类信息）（略）**