



# 中华人民共和国国家标准

GB/T 17901.3—2021

---

## 信息技术 安全技术 密钥管理 第3部分：采用非对称技术的机制

Information technology—Security techniques—Key management—  
Part 3: Mechanisms using asymmetric techniques

(ISO/IEC 11770-3:2015, MOD)

2021-03-09 发布

2021-10-01 实施

---

国家市场监督管理总局 发布  
国家标准化管理委员会

## 目 次

前言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 符号和缩略语 .....	2
5 要求 .....	3
6 密钥派生函数 .....	4
7 余子式乘法 .....	4
8 密钥承诺 .....	4
9 密钥确认 .....	5
10 密钥管理框架 .....	6
10.1 概要 .....	6
10.2 双方密钥协商 .....	6
10.3 三方密钥协商 .....	6
10.4 秘密密钥传送 .....	7
10.5 公钥传送 .....	7
11 密钥协商 .....	7
11.1 密钥协商机制 1 .....	7
11.2 密钥协商机制 2 .....	8
11.3 密钥协商机制 3 .....	9
11.4 密钥协商机制 4 .....	10
11.5 密钥协商机制 5 .....	11
11.6 密钥协商机制 6 .....	11
11.7 密钥协商机制 7 .....	12
11.8 密钥协商机制 8 .....	14
11.9 密钥协商机制 9 .....	14
11.10 密钥协商机制 10 .....	15
11.11 密钥协商机制 11 .....	16
11.12 密钥协商机制 12 .....	16
12 密钥传递 .....	17
12.1 密钥传递机制 1 .....	17
12.2 密钥传递机制 2 .....	18
12.3 密钥传递机制 3 .....	19
12.4 密钥传递机制 4 .....	20
12.5 密钥传递机制 5 .....	21
12.6 密钥传递机制 6 .....	23

13 公钥传递 .....	24
13.1 公钥传递机制 1 .....	24
13.2 公钥传递机制 2 .....	25
13.3 公钥传递机制 3 .....	26
附录 A (规范性附录) 对象标识符 .....	27
附录 B (资料性附录) 密钥建立机制特性 .....	32
附录 C (资料性附录) 密钥派生函数实例 .....	34
附录 D (资料性附录) 函数 F、集合 $S_1$ 和 $S_2$ 实例 .....	35
附录 E (资料性附录) 基于椭圆曲线的密钥建立机制实例 .....	36
附录 F (资料性附录) 所采用国际标准涉及的专利信息 .....	37
参考文献 .....	41

## 前 言

GB/T 17901《信息技术 安全技术 密钥管理》拟分为 6 个部分：

- 第 1 部分：框架；
- 第 2 部分：采用对称技术的机制；
- 第 3 部分：采用非对称技术的机制；
- 第 4 部分：基于弱秘密的机制；
- 第 5 部分：群组密钥管理；
- 第 6 部分：密钥派生。

本部分为 GB/T 17901 的第 3 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用重新起草法修改采用 ISO/IEC 11770-3:2015《信息技术 安全技术 密钥管理 第 3 部分：采用非对称技术的机制》。

本部分与 ISO/IEC 11770-3:2015 的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

- 删除了对 ISO/IEC 10118、ISO/IEC 11770-1 以及 ISO/IEC 15946-1 的引用；
- 增加了对 GB/T 15843.3—2016、GB/T 17901.1—2020、GB/T 25069、GB/T 32905 以及 GB/T 32918 系列标准的引用(见第 2 章)。

——删除了 ISO/IEC 11770-3:2015 中 3.1~3.18 和 3.20~3.43 的术语和定义，增加了 3.1、3.2 和 3.4 的术语和定义(见第 3 章)。

——增加了“本部分涉及使用椭圆曲线签名验证、公钥加解密的算法见 GB/T 32918.2 和 GB/T 32918.4。”(见第 5 章)。

——修改了对附录 C、附录 D、附录 E 和附录 F 的引用关系(见第 11 章、第 12 章和第 13 章)。

——修改或删除了 ISO/IEC 11770-3:2015 中的附录 C、附录 D 和附录 E 中与密钥管理具体实例相关的内容，并在附录 C 中增加对 GB/T 32918.3—2016 中规范的密钥派生函数的引用，在附录 E 中增加对 GB/T 32918.3—2016 规范的 SM2 密钥协商机制的引用。

——删除了 ISO/IEC 11770-3:2015 中的附录 F 和附录 G。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：西安西电捷通无线网络通信股份有限公司、无线网络安全技术国家工程实验室、中关村无线网络安全产业联盟、北京大学深圳研究生院、国家密码管理局商用密码检测中心、国家无线电监测中心检测中心、中国电子技术标准化研究院、中国通用技术研究院、天津市无线电监测站、北京计算机技术及应用研究所、天津市电子机电产品检测中心、重庆邮电大学。

本部分主要起草人：杜志强、王月辉、朱跃生、周国良、陶洪波、李琴、铁满霞、张变玲、井经涛、李志勇、李冰、彭潇、刘科伟、黄振海、许玉娜、于光明、郎元、郑骊、颜湘、张国强、刘景莉、李冬、朱正美、商钧、王莹、赵慧、高德龙、方华、熊克琦、李玉娇、龙昭华、吴冬宇。

# 信息技术 安全技术 密钥管理

## 第3部分：采用非对称技术的机制

### 1 范围

GB/T 17901 的本部分定义了基于非对称密码技术的密钥管理机制的要求、密钥派生函数、余子式乘法、密钥承诺、密钥确认、密钥管理框架、密钥协商、密钥传递、公钥传递。

本部分拟达到如下目的：

- a) 通过密钥协商建立一个共享密钥,用于实体 A 和实体 B 间的对称加密。在密钥协商机制中,密钥通过实体 A 和实体 B 交换的数据计算得到,任何实体一方不能预先确定共享密钥值。
- b) 通过密钥传递建立一个共享密钥,用于实体 A 和实体 B 间的对称加密。在密钥传递机制中,密钥由实体 A 选择,采用非对称密码保护技术,传给实体 B。
- c) 通过密钥传递将实体 A 的公钥传给其他实体。在公钥传递机制中,实体 A 的公钥经鉴别后传给其他实体,但不需保密。

本部分定义的一些机制基于 GB/T 15843.3—2016 相对应的鉴别机制。

本部分不包含以下密钥管理内容：

- a) 密钥生存期管理；
- b) 产生或确定非对称密钥对的机制；
- c) 密钥的存储、存档、删除等机制。

本部分适用于采用非对称技术实现密钥管理的系统的研制,也可指导该类系统的检测。

注：本部分定义的机制不涉及实体私钥的分发,由公钥签名系统对密钥交换消息进行签名进行操作。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 15843.3—2016 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

GB/T 17901.1—2020 信息技术 安全技术 密钥管理 第1部分：框架

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32918.1 信息安全技术 SM2 椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2 信息安全技术 SM2 椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.3—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第3部分：密钥交换协议

GB/T 32918.4 信息安全技术 SM2 椭圆曲线公钥密码算法 第4部分：公钥加密算法

### 3 术语和定义

GB/T 17901.1—2020 和 GB/T 25069 界定的以及下列术语和定义适用于本文件。