# YC31xx ROM BOOT

v1.4

Yichip Microelectronics

## Revision History

| Version | Date | Author | Description |
|---|---|---|---|
| V1.0 | 2018-7-19 | Kiven | Initial version |
| V1.1 | 2018-12-19 | Kiven | 修改通讯协议 |
| V1.2 | 2019-12-19 | Kiven | 优化描述 |
| V1.3 | 2020-03-16 | Kiven | 完善生命周期描述 |
| V1.4 | 2020-04-15 | Kiven | 添加签名文件说明 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Confidentiality Level:

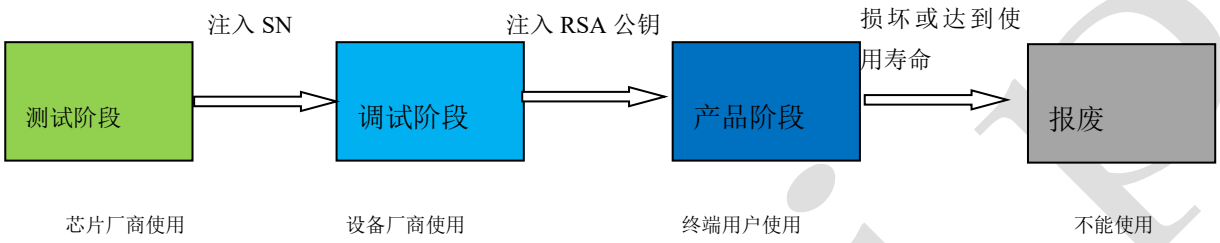
## Confidential

# 第1章 ROM BOOT 说明

ROM BOOT 提供用户应用程序的下载、验签及启动等功能，具有安全机制来确保用户的应用程序不被窥视和篡改。

# 第2章 芯片生命周期划分

芯片的生命周期划分为 4 个阶段，每一个阶段只能向下一个阶段升级，不可回退。此安全不可逆生命周期依靠分阶段向 OTP 写入特定信息来实现。




## 2.1 测试阶段：

用于芯片厂商对芯片进行测试，此阶段不设保护，芯片厂商可以下载测试程序对芯片外围接口及模块进行测试，电路和性能测试 OK 之后，在 OTP 中打入质检测试标记、注入 SN（芯片唯一序号），芯片进入调试阶段。

## 2.2 调试阶段：

设备厂商进行软硬件调试用，此阶段只对芯片基本身份信息（SN 号及测试标记）做保护，设备厂商可下载调试固件进行调试，当调试完成后，设备厂商向 OTP 中注入用于验签应用的 RSA 公钥之后，芯片调试接口将被永久禁用，芯片进入产品阶段；出厂的设备必须注入公钥升级到产品阶段。

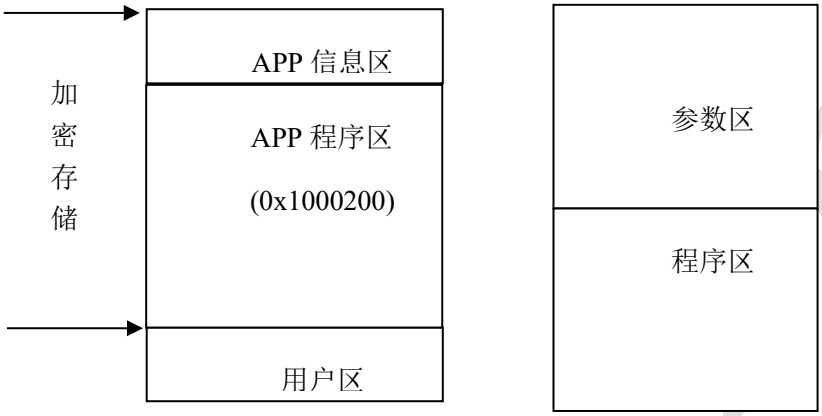
## 2.3 产品阶段：

以终端产品形式提供给用户使用，此阶段芯片工作于实际产品环境中，所以该阶段芯片信息及用户固件都将受到保护。在该阶段，调试功能将被禁用，且应用固件更新及启动都需要验证签名。

## 2.4 报废：

芯片损坏或达到使用寿命时进入到报废阶段，芯片将不能再使用。

# 第3章 安全存储说明




## 3.1 app 信息区（512B[0x1000000-0x10001ff]）

app info

| |
|---|
| App Valid（1byte） |
| sha type（1byte） |
| App version（2byte） |
| App start addr(4byte) |
| App len（4byte） |
| En_hash（256byte） |
| App info CRC32（4byte） |

**App Valid（1byte）**：app 程序有效性，每次下载或升级时由 ROM BOOT 程序根据对 app 程序的验证结

果填写，0x55 为可用，其余为不可用，当标记为不可用时将不会启动 app 程序。

sha type（1byte）：hash 算法选择，1：sha256，2：sha512，其他值错误

App version（2byte）：app 程序版本号

App start addr(4byte)：下载程序的起始地址。

App len（4byte）：app 程序长度

En_hash（256byte）：app 程序 hash 值

App info CRC32（4byte）：由 APP_Valid 域到 hash 域（含）的 Crc32 校验值

## 3.2 app 程序区[0x1000200-0x1xxxxxx]

用户 app 程序存储区起始地址 0x1000200

## 3.3 用户区（固件之后的区域）

用户自由使用

## 3.4 OTP 参数区（1kbyte）

参数区用于存放芯片质检标记、CSN、boot 信息

质检标记：芯片通过检测后写入

CSN：记录芯片序列号，通过检测后按规则写入

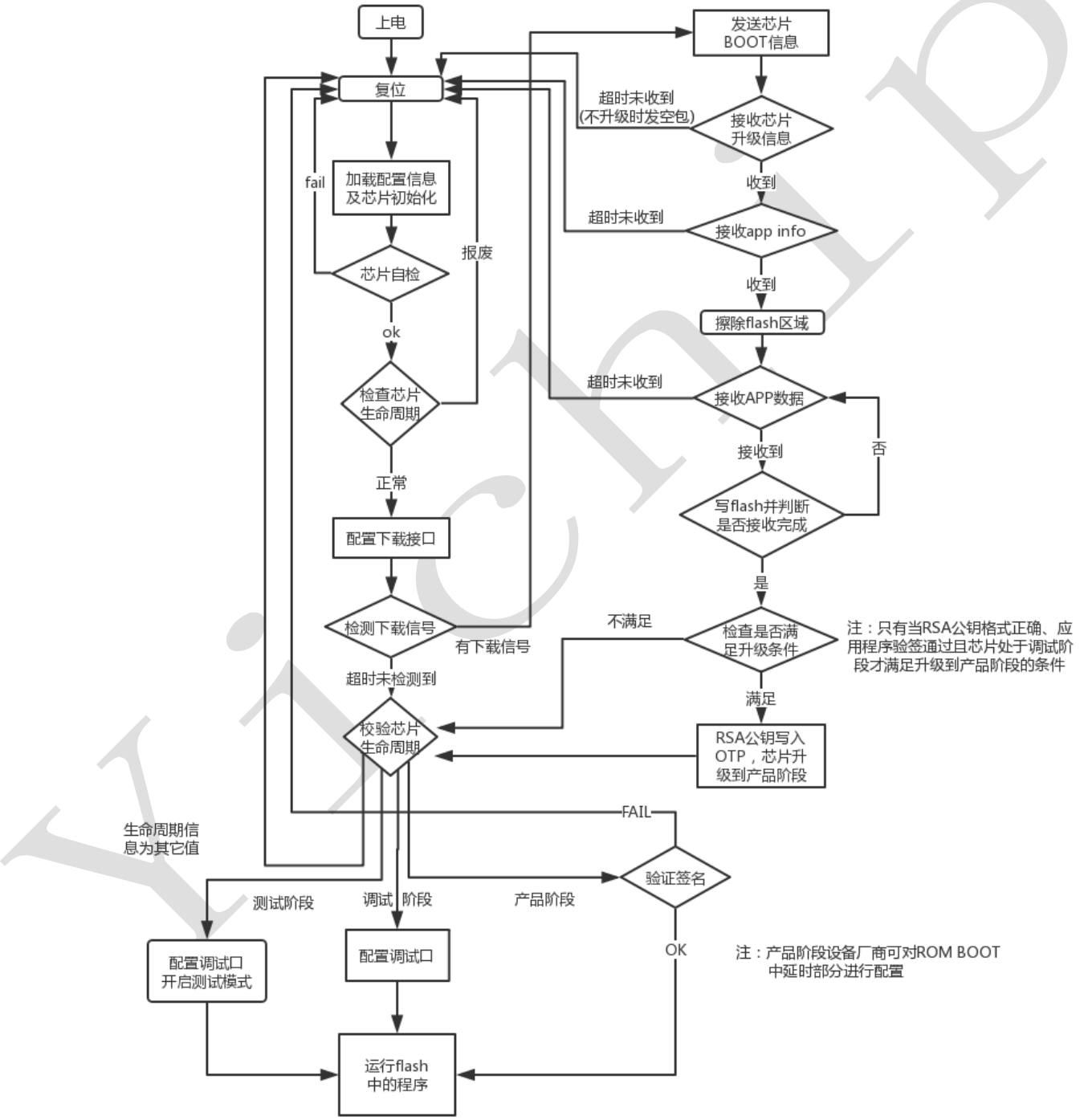
boot 信息：boot 配置信息

## 3.5 OTP 用户区（7Kbyte）

用户自由使用

# 第4章 ROM BOOT 下载流程

## 4.1 ROM BOOT 安全启动流程




ROM BOOT 安全流程图

## 4.2 ROM BOOT 安全启动流程说明

### 4.2.1 上电自检及初始化

芯片上电后首先进行算法模块、安全报警模块自检，自检 OK，后加载配置信息检查芯片生命周期，生命周期处于可用周期则初始化芯片。

### 4.2.2 应用程序下载

提供用户应用程序下载及升级功能，详细下载流程见后面的“rom boot 下载流程”。

### 4.2.3 签名认证

当芯片生命周期处于产品阶段时，必须通过签名认证才能启动应用程序，签名认证机制如下：

A、 计算 flash 中应用程序的哈希值（sha512）；

B、 使用 OTP 中的 RSA 公钥对 flash 中的经过私钥加密（签名）过的哈希值进行解密（验签）

C、 对比计算出的哈希值与解密出的哈希值，相同则签名认证通过，启动应用程序，否则复位芯片

## 4.3 ROM BOOT 下载流程

ROM BOOT 下载流程分为以下 5 个步骤：

### 4.3.1 STEP1：握手及获取 boot 信息

PC（泛指下载程序者）连续发送 0x99，芯片接收到连续 10 个 0x99 后回复 boot 信息，格式如下：

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0xAA |
| Step | 1 | 0x01 下（载交互步骤编号） |

| | | |
|---|---|---|
| Length | 2 | 36（Stage 到 CRC16 字段长度） |
| Stage | 2 | 表示芯片当前所处阶段（调试阶段为 0x1111、产品阶段为 0x7777） |
| CSN | 6 | 表示芯片唯一序列号 |
| CTime | 2 | 调试阶段下载等待时间（芯片 ROMBOOT 运行，完成通讯口初始化后等待下载信号的时间，单位为毫秒）：<br>低字节为下载信号 sync 超时时间<br>高字节*低字节为中间通讯超时时间 |
| CInfo | 2 | 质检信息 |
| ESN | 16 | 表示设备唯一序列号 |
| ETime | 2 | 设备阶段（即产品阶段）下载等待时间（芯片 ROMBOOT 运行，完成通讯口初始化后等待下载信号的时间，单位为毫秒）：<br>低字节为下载信号 sync 超时时间<br>高字节*低字节为中间通讯超时时间 |
| EInfo | 2 | 用户自定义，可用于 RSA 密钥号等 |
| App version | 2 | 当前芯片中的 App 版本号 |
| CRC16 | 2 | 校验范围为 Type 到 Ever 字段 |

### 4.3.2 STEP2：密钥下载（芯片升级）

PC 接收到芯片上传的 step1 boot 信息后，根据需要下发芯片升级信息，格式如下：

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0x55 |
| Step | 1 | 0x02 下（载交互步骤编号） |
| Length | 2 | 289（Stage 到 CRC16 字段长度） |

| | | |
|---|---|---|
| Stage | 2 | 表示芯片当前所处阶段（调试阶段为 0x1111、产品阶段为 0x7777） |
| upgrade | 1 | 是否升级到产品阶段（即是否要将公钥信息写入 OTP），如果芯片已处于产品阶段则忽略,0x55 表示写入，其他之为不写入 |
| ESN | 16 | 表示要写入的设备唯一序列号 |
| ETime | 2 | 设备阶段（产品阶段）等待时间（芯片 ROMBOOT 运行，完成通讯口初始化后等待下载信号的时间，单位为毫秒）：<br>低字节为下载信号 sync 超时时间<br>高字节*低字节为中间通讯超时时间 |
| EInfo | 2 | 设备阶段参数的信息（可用于 RSA 密钥号等） |
| RSAKEY | 264 | RSA 公钥（N:256byte,E:8 byte） |
| CRC16 | 2 | 校验范围为 Type 到 RSAKEY 字段 |

芯片成功接收到升级信息后回复

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0xAA |
| Step | 1 | 0x02 下（载交互步骤编号） |
| Length | 2 | 03（Status 到 CRC16 字段长度） |
| Status | 1 | Status，00：成功；01：CRC 校验失败；02：长度错误； 03：校验错误； 04：重传 |
| CRC16 | 2 | 校验范围为 Type 到 Status 字段 |

### 4.3.3 STEP3：下发 app 信息头

PC 接收到芯片上传的 step2 成功 ACK 信息后，下发 app 程序信息头信息，格式如下：

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0x55 |
| Step | 1 | 0x03 下（载交互步骤编号） |
| Length | 2 | 274（App Valid 到 CRC16 字段长度） |
| App Valid | 1 | 表示 app 信息头是否有效，芯片的 ROM BOOT 验证程序之后，会根据实际验证结果修改此值 |
| sha type | 1 | hash 算法选择，1：sha256，2：sha512，其他值错误 |
| App version | 2 | App 程序版本号 |
| App start addr | 4 | App 程序开始地址(固定为 0x1000200) |
| App len | 4 | App 程序文件长度 |
| En_hash | 256 | App 程序文件的 hash 值密文<br>1.计算 app 程序文件的 hash 值.<br>2.私钥加密上一步 hash 值,得到结果为该处需要填写的数据 |
| CRC32 | 4 | 校验范围为 App Valid 到 hash 字段 |
| CRC16 | 2 | 校验范围为 Type 到 CRC32 字段 |

芯片成功接收到 app 信息头后回复

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0xAA |
| Step | 1 | 0x03 下（载交互步骤编号） |

| | | |
|---|---|---|
| Length | 2 | 03（Status 到 CRC16 字段长度） |
| Status | 1 | Status，00：成功；01：CRC 校验失败；02：长度错误； 03：校验错误； 04：重传 |
| CRC16 | 2 | 校验范围为 Type 到 Status 字段 |

### 4.3.4 STEP4：下发 app 程序

PC 接收到芯片上传的 step3 成功 ACK 信息后，下发 app 程序数据，格式如下：

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0x55 |
| Step | 1 | 0x04 下（载交互步骤编号） |
| Length | 2 | 0xYY 0x YY（App Data 到 CRC16 字段长度）（App Data 长度大于 1k 时分包下发） |
| App Data | XX | App 程序数据 |
| CRC16 | 2 | 校验范围为 Type 到 App Data 字段 |

注：下载程序数据时用总长度计算是否有后续数据

芯片成功接收到 app 程序数据后回复

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0xAA |
| Step | 1 | 0x04 下（载交互步骤编号） |
| Length | 2 | 03（Status 到 CRC16 字段长度） |

| | | |
|---|---|---|
| Status | 1 | Status，00：成功；01：CRC 校验失败；02：长度错误； 03：校验错误； 04：重传 |
| CRC16 | 2 | 校验范围为 Type 到 Status 字段 |

### 4.3.5 STEP5：上传验证结果

芯片成功接收完 app 程序数据后进行验证并回复结果

| 字段 | 长度(byte) | 说明 |
|---|---|---|
| Type | 1 | 值为 0xAA |
| Step | 1 | 0x05 下（载交互步骤编号） |
| Length | 2 | 03（Status 到 CRC16 字段长度） |
| Status | 1 | Status，00：成功；03：验证失败； |
| CRC16 | 2 | 校验范围为 Type 到 Status 字段 |

# 第5章 签名文件格式说明

签名文件采用以下格式存放:

| Type(1byte) | Cmd(1byte) | Len(4byte) | Data |
|---|---|---|---|
| 0xaa | | Data 长度 | |

签名文件中存有 公钥信息、应用信息及应用数据三部分，见下图及注释

```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: AA 01 1D 01 00 00 55 00 00 00 00 00 00 00 00 00 ;
00000010h: 00 00 00 00 00 00 00 64 02 01 00 C8 69 DC 20 0E ;
00000020h: F6 60 72 7B E8 4B 20 A6 8D 64 3D CF 61 23 34 A0 ;
00000030h: A6 06 86 81 9D 0B 42 A3 75 1F 5F 8B BC 04 7D 64 ;
00000040h: C4 27 DA 69 4A 29 CB 7D 4A 13 A2 48 F7 14 EB 5B ;
00000050h: 30 1D 39 8C DF CE 43 FC B0 B5 B4 EE 9A 99 F1 FF ;
00000060h: 28 FB 00 16 4E D4 65 EA A9 15 1E 84 78 96 56 85 ;
00000070h: 1C 9F C0 DC 27 AB F5 8F F5 D0 77 5D D8 26 8B 37 ;
00000080h: D4 F7 29 19 CF 30 11 2F 67 72 C1 11 1E 39 78 2A ;
00000090h: B0 8E 0C F6 9A ED B4 CA 3F FC DA 0E BB 69 8E D8 ;
000000a0h: FC 2A E6 4B D7 6F 76 D9 C7 F8 B7 AF 90 57 4D 28 ;
000000b0h: A3 BF 8F 1D 7A D8 2B 55 BB A7 64 BA 36 3C E0 53 ;
000000c0h: 9F 90 DE 6D 9F 8A 3E 58 E3 C0 E3 0F 4A 5D C9 FB ;
000000d0h: AD AC CE 26 15 46 D2 BB 9A D2 8D A2 31 23 16 5D ;
000000e0h: B9 A8 CB A5 48 F8 FC C4 16 B1 DA 78 B2 64 7B FF ;
000000f0h: C8 0C 7E 80 2F 2A BD B6 81 40 B5 1A D3 7C 6B 34 ;
00000100h: 07 35 E4 F4 38 3D 9F F0 1A E8 6F B9 1C FD C0 FA ;
00000110h: 62 B3 82 06 FB A9 0E 52 D2 B2 91 00 01 00 01 00 ;
00000120h: 00 00 00 AA 02 10 01 00 00 55 02 FE FF 00 02 00 ;
00000130h: 01 50 51 00 00 AB 81 A6 10 C3 85 2F 59 80 CA E2 ;
00000140h: F7 8B 02 62 7A 90 0E D0 62 2C A2 68 22 42 46 F8 ;
00000150h: B2 9C 75 55 06 E7 6C 61 6B 1B 4E CA E5 4F B7 C1 ;
00000160h: CB 72 D9 64 2D 55 7B AD 1A ED 5D DE 8C 5B 95 22 ;
00000170h: 25 ED C6 3E DC AA 9C AB 57 4A 91 8D EA C2 99 4A ;
00000180h: CA D5 0C 99 2A 45 D8 24 1D 9F 16 2C D9 1F 09 2C ;
00000190h: A1 C4 35 2D 04 4E 52 0B 64 EC 32 25 D5 BC A4 1C ;
000001a0h: B2 30 54 E0 65 FC 4C 75 BA 34 63 70 97 D1 CC 7D ;
000001b0h: 93 B2 92 AF 11 66 E6 08 0E 08 67 19 F6 0C 58 17 ;
000001c0h: 5D 29 FD 57 20 24 54 8D 2B 48 81 D0 93 E4 FC C4 ;
000001d0h: 95 3F 77 D8 77 AF 1B 75 2B 0E D9 29 4B E2 D2 3F ;
000001e0h: 73 A4 59 88 42 7A 5D A4 A0 0A 82 8A 40 F1 F9 C5 ;
000001f0h: FC 45 5C 99 96 7B 5A 7A 61 5E 18 C3 38 2D 9A 95 ;
00000200h: E3 4D E8 7B 8C 40 D2 30 51 A4 0A C0 F7 2C DC 40 ;
00000210h: CF 70 CC DB 9F 5B 21 85 5D 2F 18 0F F2 31 A8 7D ;
00000220h: 97 A0 7A B3 AC 6B D7 25 FB D7 E3 95 8F 5B 93 B0 ;
00000230h: 7D 94 90 A8 3E 51 EF F9 D0 AA 03 50 51 00 00 65 ;
00000240h: 48 00 47 00 20 66 E0 00 BF 06 20 63 E0 00 BF 0C ;
```

1、 公钥信息

公钥信息头为：AA 01，紧跟后面 4 个字节(1D 01 00 00)为公钥信息长度，之后是公钥信息内容，与“4.3.2 STEP2：密钥下载（芯片升级）”章节包格中的 upgrade-- RSA_KEY 字段对应

2、 应用信息

应用信息头为：AA 02，紧跟后面 4 个字节(10 01 00 00)为应用信息长度，之后是应用信息内容，与“4.3.3 STEP3：下发 app 信息头”章节包格中的 App Valid -- CRC32 字段对应

3、 应用数据

应用数据头为：AA 03，紧跟后面 4 个字节(50 51 00 00)为应用数据长度，之后的数据就是“4.3.4 STEP4：下发 app 程序”步骤中所要下发的 app data