A71CL

面向阿里云的即插可信安全元件

第 3.0 版 — 2018 年 11 月 28 日
485030

产品缩略版数据手册
公司公开文件

1. 简介

A71CL 是一款开箱即用型解决方案，可提供 IC 级信任根以及从芯片到云的可靠安全功能。产品配置中提供预配置凭证以支持阿里云应用。它是一个能够安全地存储和预配凭证、将物联网设备安全连接到云服务并执行加密节点验证的平台。

A71CL 解决方案提供各种安全措施，防止 IC 遭受物理和逻辑攻击。利用该解决方案，能够与主机平台实现集成并运行操作系统，为一系列的广泛应用增加信任链。该产品附带使用手册和一系列文档，指导用户在整个系统内集成本产品；利用即插即用的主机应用代码、开发套件、参考设计可简化设计导入。

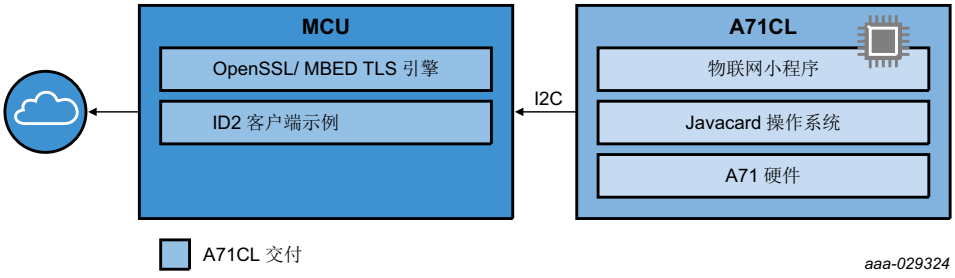


图 1. A71CL 框图

2. 概述

2.1 A71CL 命名约定

下表解释了 A71CL 产品的商品名命名约定。每款 A71CL 产品都会被分配一个这样的商品名，其中包括客户和特定应用数据。

A71CL 基本类型名称格式如下。

A71CLxagpp(p)

“A71CL”是常量，所有其他字母都是变量，表 1 对这些字母进行了解释。

表 1. A71CL 商业名称格式

变量	含义	值	说明
x	IC 硬件规范代码	1	标准工作环境温度：–25 °C 至 +85 °C 支持 I²C 接口
		2	标准工作环境温度：–40 °C 至 +90 °C 支持 I²C 接口
a	嵌入式操作系统代码	C	Javacard 操作系统
g	嵌入式应用固件（小应用程序）代码	L	L 为固定值 = 预安装了物联网安全小程序
pp(p)	封装类型代码 dd(d)= 交付类型， TK2= HVSON8 (4x4)		

2.2 I²C 接口

A71CL 带有 I²C 接口 （从模式），在快速模式 (FM) 下工作支持最高 400 KB/ 秒的数据速率。 I²C 接口使用在参考文献 3 中定义的基于 SMBus 的智能卡 I²C 协议。

具体取决于启动时的接口引脚状态，更多详细信息请参阅第 7 节 “引脚配置信息”；上电复位后的默认 I²C 地址：写入地址 0x90，读取地址 0x91。

2.3 安全许可

恩智浦半导体公司已获得 Cryptography Research Incorporated (CRI) 授予的 SPA 和 DPA 反制措施专利许可。该许可涵盖硬件和软件反制措施。与 CRI 的这个许可协议中也包含操作系统内部的反制措施，这一点对客户非常重要。根据客户要求，还可提供更多详细信息。

3. 特性和优势

3.1 主要优势

- 安全的零接触连接
- 端到端安全，从芯片到边缘到云
- 输入安全凭证，提供 IC 级信任根
- 利用完整的产品支持包，快速完成设计导入
- 易于与不同 MCU 平台集成

3.2 安全特性

A71CL 安全概念包括很多旨在保护芯片的安全措施。

A71CL 完全基于集成的 Javacard 操作系统和小程序自动运行。只有通过小程序的固定功能，才能实现直接存储器访问。因此，存储器的内容与主机系统是完全隔离的。

由芯片布局、逻辑和功能模块中的集成设计措施提供攻击保护。

3.3 加密功能

- 利用 SHA1、 SHA224、 SHA256 生成消息摘要
- 随机数生成器
- 非对称密钥存储类型：RSA 标准或 RSA CRT
- 自动 RSA 密钥生成器，密钥长度范围：512 位至 2048 位。 RSA 标准或 RSA CRT。
- 利用DES_CBC_NOPADDING、DES_ECB_NOPADDING、AES_CBC_NOPADDING、AES_ECB_NOPADDING 进行对称加密 / 解密。
- 利用 DES_CBC_ISO9797_M1、DES_CBC_ISO9797_M2、AES_CBC_ISO9797_M1、AES_CBC_ISO9797_M2 进行对称签名 / 验证。
- 利用 RSA_NOPADDING、 RSA_ PKCS1 进行非对称加密 / 解密。
- 利用 RSA_SHA1(PKCS1)、 RSA_SHA256 进行非对称签名 / 验证。
- 服务数据存储：存储数据读取和写入受 SCP 保护。
- SCP 02 服务包括选项 “i” = ‘55’。

3.4 功能特性

- 400 KB/ 秒的 I^2C 快速模式接口
- 工作环境温度为 −40 °C 至 +90 °C (A7102)
- 片上 Javacard 操作系统
- 典型睡眠模式电流为 40 µA， I^2C 引脚处于三态模式下
- 深度睡眠模式电流为 10 µA， I^2C 引脚处于三态模式下
- 高性能公共密钥基础设施 (PKI)
- EEPROM 的耐受能力至少达到 500,000 个周期，数据保持时间最少 25 年
- HVSON8 封装

4. 应用

4.1 使用案例与目标应用

- A710xCL 用例示例
  - 安全连接到公有 / 私有云、边缘计算平台、基础设施
  - 安全调试
  - 设备间认证
  - 来源证明 / 防伪
  - 密钥存储和数据保护
- A710xCL 目标应用
  - 互连工业设备
  - 传感器网络
  - IP 摄像头
  - 家庭网关
  - 家用电器

5. 订购信息

5.1 订购选项

表 2. 订购信息

型号 [1]	封装		
	名称	说明	版本
A7101agTK2/...	HVSON-8	塑料散热增强型超薄小型封装；无引脚； 8 个端子；主体尺寸 4 × 4 × 0.85 mm	SOT909-1
A7102agTK2/...			

[1] 根据 A71CL 类型分类， a = A 或 C， g = G、 C 或 A，请参阅第 2.1 节 “A71CL 命名约定”

表 3 概略列出了可用的 A71CL 产品类型。

表 3. A71CL 特性表

可订购类型	产品型号 [1]	12NC	工作环境温度	商业名称
A7101CLTK2/T0BC2WJ	A7101CLTK2/T0BC2WE	935368739118	–25 °C 至 +85 °C	A71CL，经过预配可随时用于阿里云
A7102CLTK2/T0BC2XJ	A7102CLTK2/T0BC2XR	935379152118	–40 °C 至 +90 °C	

[1] HN1，根据 A71CL 类型分类，请参见第 2.1 节 “A71CL 命名约定”

5.1.1 订购 A71CL 样品

您可从恩智浦半导体电子商务网站订购样品。

请注意，恩智浦半导体可免费提供 5 件。大量样品必须单独订购。

6. 功能说明

6.1 功能框图

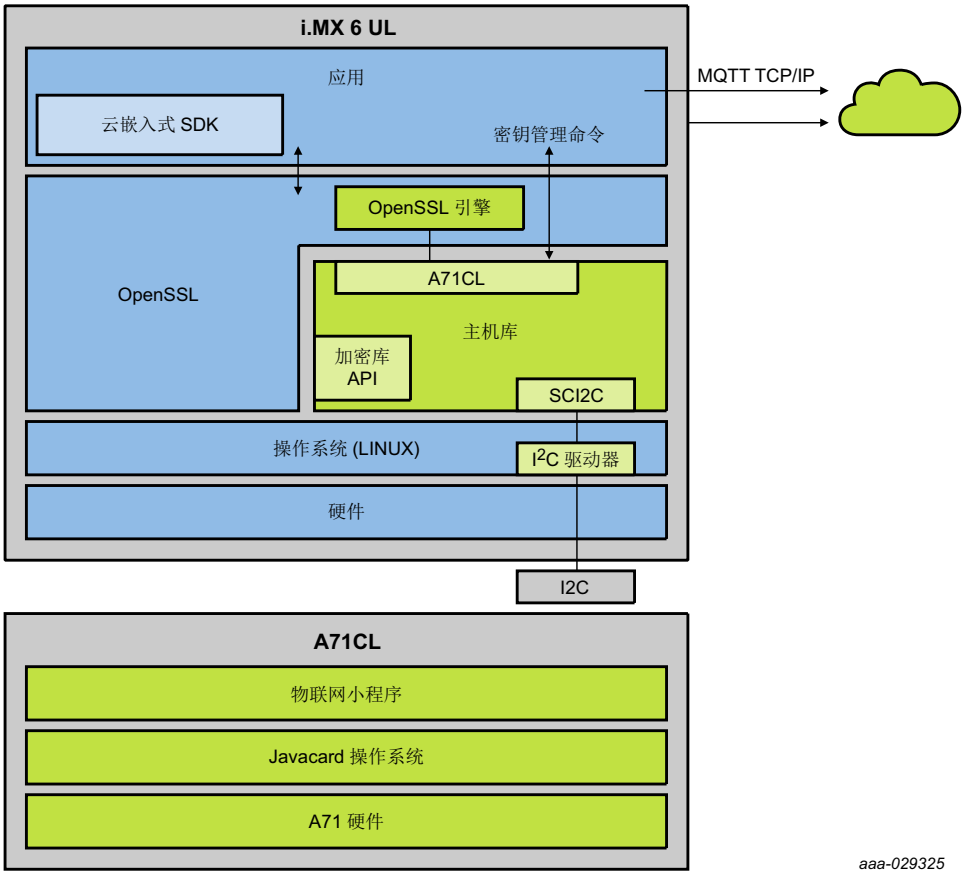


图 2. A71CL 功能框图 - 开放式 SSL 实例

A71CL 使用 I²C 作为通信接口，如下节所述。A71CL 命令使用使用智能卡 I² 协议 (SCI2C) 打包。有关 A71CL 命令 [参考 APDU 规范] 和 SCI2C 协议封装 （参考文献 3）的详细文档，请在 NXP DocStore 中查阅。

为了简化产品使用，恩智浦创建了主机库，用于管理 A71CL 命令和 SCI2C 协议封装。该主机库在 A71CL 网站上提供。 A71CL 网站还提供完整 APDU 规范以供下载。

6.2 I²C 接口

A71CL 带有 I²C 接口 （从模式），在快速模式 (FM) 下工作支持最高 400 KB/ 秒的数据速率。 I²C 接口使用在参考文献 3 中定义的基于 SMBus 的智能卡 I²C 协议。具体取决于启动时的接口引脚状态，更多详细信息请参阅第 7 节。上电复位后的默认 I²C 地址取决于启动条件，如表 4 所示。

6.3 上电时进行自动通信模式检测

IC 根据引脚状态来配置其接口，如下表所示。上电复位时，主机系统必须保持这些引脚上的电压水平稳定，至少持续 500µs。

表 4. I²C 地址

启动时的值				I²C 地址	
IF0	IF1	I2C_SCL	I2C_SDA	写入	读取
0	x	0	0	不适用	不适用
1	0	1	1	0x90	0x91
1	1	1	1	0x92	0x93

6.4 节电模式

器件提供两种节电工作模式：睡眠模式和深度睡眠模式。这些模式通过 RST_N 引脚激活（深度睡眠模式）或由器件激活。

6.4.1 睡眠模式

睡眠模式具备以下特性：

- 所有内部时钟冻结
- CPU 进入节电模式，程序执行被中止，
- CPU 寄存器保留其内容，
- RAM 保留其内容，

A71CL 自动进入睡眠模式，也自动从睡眠模式唤醒。在睡眠模式时，所有内部时钟停止。IO 保持其在空闲时被激活的逻辑状态。在睡眠模式期间，安全传感器 HVS、 LVS、 LTS、 HTS、光传感器、 Glitch 传感器和有源屏蔽处于禁用状态。

退出睡眠模式有两种方法：

- RST_N 上的复位信号
- I2C_SDA 的下降沿触发外部中断边沿

6.4.2 深度睡眠模式

A71CLx提供特殊的睡眠模式，实现最大程度的节能。将RST_N拉到逻辑零电平持续500µs以上，即可进入深度睡眠模式。

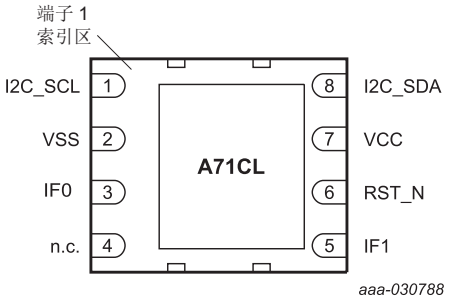
在深度睡眠模式下，内部电源完全关闭，只有 IO 引脚保持供电。所有数字引脚将保持在高电阻模式下。

要退出深度睡眠模式，必须释放 RST_N，并设置为逻辑 “1” 电平。

7. 引脚配置信息

7.1 引脚配置

7.1.1 HVSON8 的引脚配置



透明俯视图

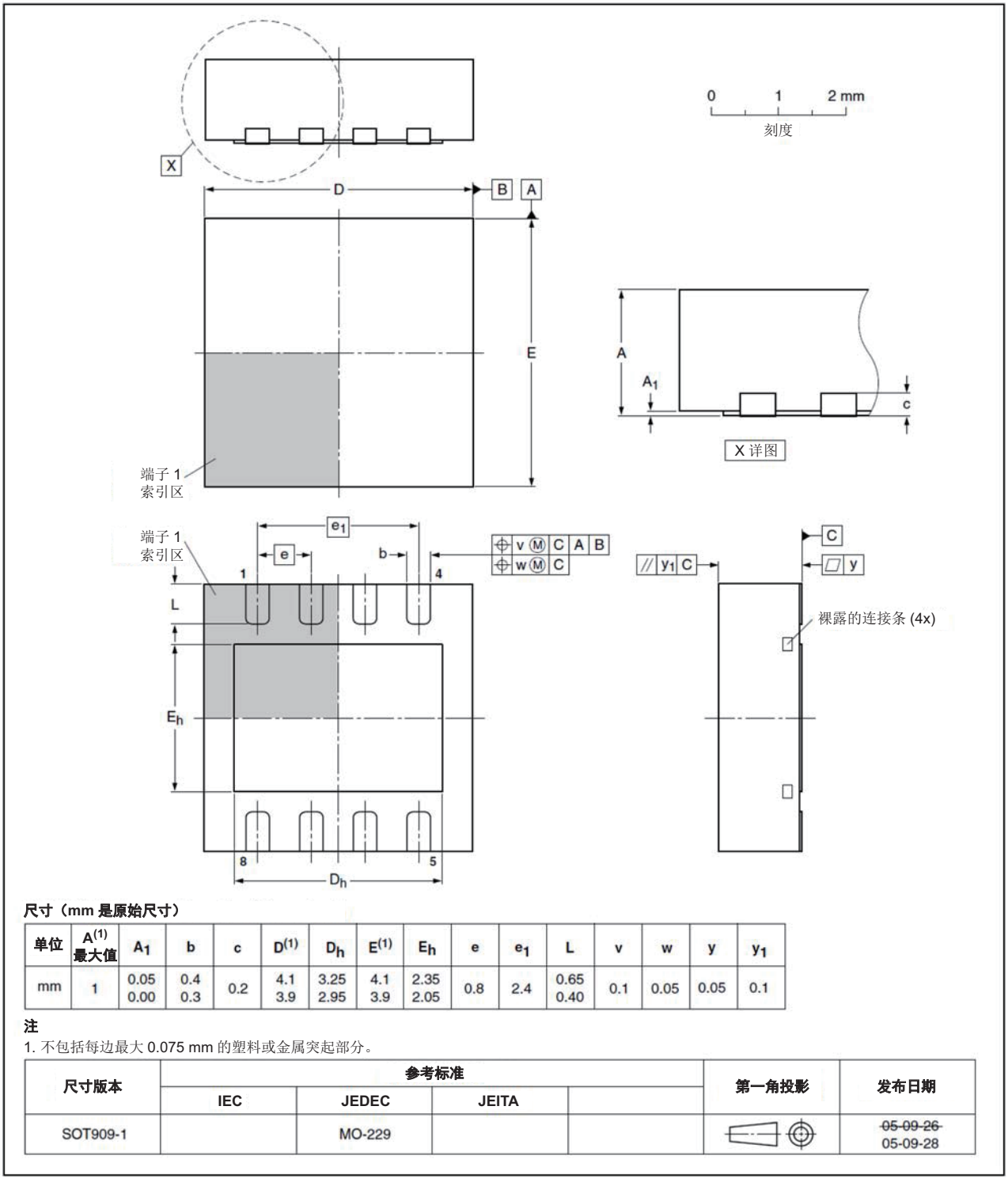
图 3. HVSON-8 的引脚配置 (SOT909-1)

表 5. HVSON8 引脚说明

符号	引脚	说明
I2C_SCL	1	I^2C 时钟
VSS	2	接地
IF0	3	接口激活，启动时为高电平
n.c.	4	未连接
IF1	5	I^2C 地址选择
RST_N	6	复位输入，低态有效
VCC	7	电源电压输入
I2C_SDA	8	I^2C 数据

8. 封装尺寸

HVSON8：塑料散热增强型超薄小型封装；无引脚；8 个端子；主体尺寸 4 x 4 x 0.85 mm **SOT909-1**



尺寸（mm 是原始尺寸）

单位	A(1) 最大值	A1	b	c	D(1)	Dh	E(1)	Eh	e	e1	L	v	w	y	y1
mm	1	0.05 0.00	0.4 0.3	0.2	4.1 3.9	3.25 2.95	4.1 3.9	2.35 2.05	0.8	2.4	0.65 0.40	0.1	0.05	0.05	0.1

注

1. 不包括每边最大 0.075 mm 的塑料或金属突起部分。

尺寸版本	参考标准				第一角投影	发布日期
	IEC	JEDEC	JEITA			
SOT909-1		MO-229				~~05-09-26~~ 05-09-28

图 4. SOT909-1 封装尺寸

9. 封装信息

9.1 卷盘封装

A71CL 产品采用 7 英寸和 13 英寸卷带封装。表 6 提供了详细信息。

表 6. 卷盘封装选项

封装类型	卷盘类型	最小封装数量
HVSON8	7 英寸卷带封装	1500
HVSON8	13 英寸卷带封装 [1]	6000

[1] 对于采用 HVSON8 封装、订购码 (12NC) 以 118 结尾的 A71 部件，有关其封装方法、产品方向、卷带尺寸和标记的详细信息，请参阅参考文献 2。

10. 电气和时序特性

用于 I^2C 的引脚和功能的静态 (DC) 和动态 (AC) 参数电气接口特性，符合恩智浦 I^2C 规范（请参见参考文献 1）。

11. 限值

表 7. 限值

依据绝对最大额定值系统 (IEC 60134)。电压以 VSS 为基准（接地 = 0 V）。

符号	参数	条件		最小值	最大值	单位
V_{DD}	电源电压			-0.3	+4.6	V
V_I	输入电压	任何信号引脚		-0.3	+4.6	V
I_I	输入电流	引脚 I2C_SDA、I2C_SCL		-	10	mA
I_O	输出电流	引脚 I2C_SDA、I2C_SCL		-	10	mA
I_{lu}	锁存电流	$V_I < 0$ V 或 $V_I > V_{DD}$		-	100	mA
V_{esd_hbm}	静电放电电压（人体模型）	引脚 VCC、VSS、RST_N、I2C_SDA、I2C_SCL	[1]		± 2.0	kV
V_{esd_cdm}	静电放电电压（充电器件模型）	引脚 VCC、VSS、RST_N、I2C_SDA、I2C_SCL	[3]		± 500	V
P_{tot}	总功耗		[2]	-	1	W
T_{stg}	存储温度			-55	+125	°C

[1] 军用标准 883-D 方法 3015；人体模型；C = 100 pF，R = 1.5 kΩ；T_{amb} = −25 °C 至 +85 °C。

[2] 取决于封装的相应热阻。

[3] JESD22-C101，JEDEC 标准电场感应充电器件模型测试方法。

12. 建议工作条件

A71CL 提供两种工作模式，即所谓的 1V8 模式和面向电池供电应用的 3V3 模式。

表 8. 建议工作条件

符号	参数	条件		最小值	典型值	最大值	单位
V_{DD}	电源电压范围	3V3 模式范围，CPU 处于自由运行模式下		2.50	3.3	3.6	V
		1V8 模式		1.62	1.8	1.98	V
V_I	数字 I/O 引脚 I2C_SCL、I2C_SDA 上的直流输入电压	3V3 模式		0		3.6	V
		1V8 模式		0		3.6	V
V_I	数字输入引脚 RST_N 上的直流输入电压	3V3 模式		0		3.6	V
		1V8 模式		0		3.6	V
T_{amb}	工作环境温度	A7101		-25		+85	°C
		A7102		-40		+90	°C

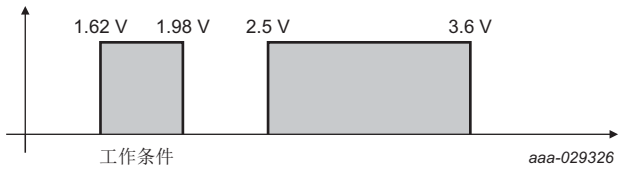


图 5. 电压范围内的建议工作条件

13. 特性

13.1 直流特性

测量约定

测试测量在受测试器件的接触垫处进行。所有电压都相对于接地接触垫 VSS 进行定义。进入器件的所有电流都视为正电流。

13.1.1 通用和 I²C I/O 接口

表 9. I2C_SCL、I2C_SDA 和 RST_N 的电气直流特性

符号	参数	条件		最小值	典型值	最大值	单位
输入 / 输出：I2C_SCL，推挽模式下的 I2C_SDA							
V_{IH}	高电平输入电压			0.7 V_{DD}		V_{Imax}[1]	V
V_{IL}	低电平输入电压			-0.5		0.3 V_{DD}	V
I_{IH}	输入模式下的高电平输入电流	$V_{IHmin} < V_I < V_{IHmax}$				± 10	µA
I_{IL}	低电平输入电流	$V_{ILmin} < V_I < V_{ILmax}$				± 10	µA
V_{OH}	高电平输出电压	I_{OH} = –3.0 mA；3V3 模式	[2]	0.7 V_{DD}			V
		I_{OH} = –3.0 mA；1V8 模式	[2]	0.7 V_{DD}			V
V_{OL}	低电平输出电压	I_{OL} = 3.0 mA 3V3 模式				0.4	V
		I_{OL} = 2.0 mA 1V8 模式				0.2 V_{DD}	V
输入 / 输出：I2C_SCL，开漏模式下的 I2C_SDA							
V_{IH}	高电平输入电压			0.7 V_{DD}		V_{Imax}[1]	V
V_{IL}	低电平输入电压			-0.5		0.3 V_{DD}	V
I_{IH}	输入模式下的高电平输入电流	$V_{IHmin} < V_I < V_{IHmax}$				± 10	µA
I_{IL}	低电平输入电流	$V_{ILmin} < V_I < V_{ILmax}$				± 10	µA
V_{OL}	低电平输出电压	I_{OL} = 3.0 mA 3V3 模式				0.4	V
		I_{OL} = 2.0 mA 1V8 模式				0.2 V_{DD}	V
输入：RST_N							
V_{IH1}	高电平输入电压			0.7 V_{DD}		V_{Imax}[1]	V
V_{IL1}	低电平输入电压			-0.3		0.3 V_{DD}	V
I_{IH1}	高电平 RST_N 输入电流	$V_{IH1min} \le V_I \le V_{DD}$	[3]			± 20	µA
I_{IL1}	低电平 RST_N 输入电流	0 V ≤ V_I ≤ V_{IL1max}；	[3]			± 20	µA

[1] 最大值依据表 8 “建议工作条件”

[2] ：外部上拉电阻 20 kΩ 至 V_{DD}。参数 V_{OH} 测试条件的最坏情况出现在 V_{DD} 为最小值的情况下。对于 A 类电源电压条件，V_{DD} = 4.5 V 是相对于固定规范限值 V_{OHmin} = 3.8 V (0.844 V_{DD}) 的最坏情况。电源电压相关限制 “0.7 V_{DD}” 比高 V_{DD}（在 V_{DD} = 5.5 V 时，0.7 V_{DD} = 3.85 V）下的 3.8 V 固定值要求更严格。因此，在 4.5 V 至 5.5 V 的 V_{DD} 范围内，V_{OHmin} 被指定为“0.7 V_{DD} 和 3.8 V 两者中相对较大的值”。

[3] 低电平有效 RST_N 输入内部具有电阻下拉器件，电压 VSS。因此，电流流入引脚，电压大于 0 V。图 6 显示了 RST_N 输入特性。

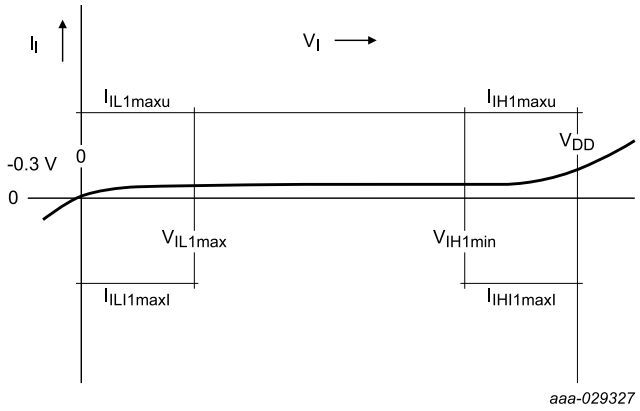


图 6. RST_N 的输入特性

13.1.2 3V3 模式下工作的 I²C 接口 [1]

表 10. IC 电源电压 V_{DD} 的电气特性； V_{SS} = 0 V ； T_{amb} = -40 至 +90 °C

符号	参数	条件		最小值	典型值	最大值	单位
电源							
V_{DD}	电源电压范围	3V3 模式范围 CPU 在自由运行模式下		2.50	3.3	3.6	V
I_{DD}	无协处理器激活	CPU 在自由运行模式下			6.3	7.0	mA
	正在进行 EPROM 编程	CPU 在自由运行模式下			7.3	8.0	mA
	AES 协处理器激活	CPU 在自由运行模式下			9.3	10.3	mA
	ECC 协处理器激活	CPU 在自由运行模式下			13.7	15.1	mA
$I_{DD(SLP)}$	电源电流睡眠模式	T_{amb} = 25 °C			45	150	µA
$I_{DD(DSLP)}$	电源电流深度睡眠模式	RST_N， 0V 条件下， T_{amb} = 25 °C				10	µA
		RST_N， 0V 条件下， T_{amb} = 90 °C				10	µA

[1] 所有标记值均为典型值，仅供参考。这些值可能变化，恕不另行通知。

13.1.3 1V8 模式下工作的 I²C 接口 [1]

表 11. IC 电源电压 V_{DD} 的电气特性； V_{SS} = 0 V ； T_{amb} = -40 至 +90 °C

符号	参数	条件		最小值	典型值	最大值	单位
电源							
V_{DD}	电源电压范围	1V8 模式范围		1.62	1.8	1.98	V
I_{DD}	无协处理器激活	CPU 在自由运行模式下			2.45		mA
	AES 协处理器激活	CPU 在自由运行模式下			2.7		mA
	ECC 协处理器激活	CPU 在自由运行模式下			7.5		mA
$I_{DD(SLP)}$	电源电流睡眠模式	T_{amb} = 25 °C			40	80	µA
$I_{DD(DSLP)}$	电源电流深度睡眠模式	RST_N， 0V 条件下， T_{amb} = 25 °C				10	µA
		RST_N， 0V 条件下， T_{amb} = 90 °C				10	µA

[1] 所有标记值均为典型值，仅供参考。这些值可能变化，恕不另行通知。

13.2 交流特性

表 12. 非易失性存储器时序特性； V_{DD} = 1.8 V ± 10% 或 3 V ± 10% V ； V_{SS} = 0 V ； T_{amb} = -40 至 90 °C

符号	参数	条件		最小值	典型值	最大值	单位
t_{EEP}	EEPROM 擦除和编程时间				2.7		ms
t_{EEE}	EEPROM 擦除时间				1.7		ms
t_{EEW}	EEPROM 编程时间				1.0		ms
t_{EER}	EEPROM 数据保持时间	T_{amb} = +55 °C		25			年
N_{EEC}	EEPROM 耐受能力（编程周期数）			5×10^5			周期

表 13. I2C_SDA、I2C_SCL 和 RST_N[1] 的电气交流特性； V_{DD} = 1.8 V ± 10% 或 3 V ± 10% V ； V_{SS} = 0 V ； T_{amb} = -40 至 90 °C

符号	参数	条件		最小值	典型值	最大值	单位
输入 / 输出：I2C_SDA，开漏模式下的 I2C_SCL							
tr_{IO}	I/O 输入上升时间	输入 / 接收模式	[4]			1	µs
tf_{IO}	I/O 输入下降时间	输入 / 接收模式	[4]			1	µs
tf_{OIO}	I/O 输出下降时间	输出 / 传输模式； C_L = 30 pF	[4]			0.3	µs
f_{CLK}	I²C 应用中的外部时钟频率	t_{CLKW}、 T_{amb} 和 V_{DD} 在它们的速度限值范围内		-		400	kHz
t_{CLKW}	时钟脉冲宽度 i.r.t. 时钟周期（CLK 的正脉冲占空比）		[3]	40		60	%
输入：RST_N							
t_{RW}	复位脉冲宽度 （RST_N 低电平），未进入深度睡眠模式			40		400	µs
t_{RDSLP}	复位脉冲宽度 （RST_N 低电平），进入深度睡眠模式			500			µs
t_{WKP}	从睡眠模式唤醒时间	$f_{CLKmin} < f_{CLK} < f_{CLKmax}$		-	8	10	µs
t_{WKPIO}	从睡眠模式唤醒的引脚低电平时间	内部 / 外部电平触发		-	8	10	µs
		内部 / 外部边沿触发		-	8	10	µs

表 13. I2C_SDA、 I2C_SCL 和 RST_N[1] 的电气交流特性；
V_{DD} = 1.8 V ± 10% 或 3 V ± 10% V； V_{SS} = 0 V； T_{amb} = -40 至 90 °C *（续）*

符号	参数	条件		最小值	典型值	最大值	单位
t_{WKPRST}	从睡眠模式唤醒的 RST_N 低电平时间			40		-	µs
t_{WKWT}	从睡眠模式唤醒事件到 I2C_SDA 有效的时间				50	100	ns
C_{PIN}	引脚电容 RST_N、 I2C_SDA、/I2C_SCL	测试频率 = 1 MHz； T_{amb} = 25 °C		-		10	pF

[1] 所有标记值均为典型值，仅供参考。这些值可能变化，恕不另行通知。

[2] t_r 定义为信号振幅在 20% 至 80% 之间的上升时间。
t_f 定义为信号振幅在 80% 至 20% 之间的下降时间。

[3] 在交流测试过程中，输入 RST_N、 I2C_SDA、 I2C_SCL 在 0 V 至 +0.3 V 电压下驱动，以提供低输入电平，在 V_{DD} −0.3 V 至 V_{DD} 的电压下驱动，提供高输入电平。时钟周期和信号脉冲（占空比）定时在 50% 的 V_{DD} 下测量。

[4] t_r 定义为信号振幅在 30% 至 70% 之间的上升时间。
t_f 定义为信号振幅在 70% 至 30% 之间的下降时间。

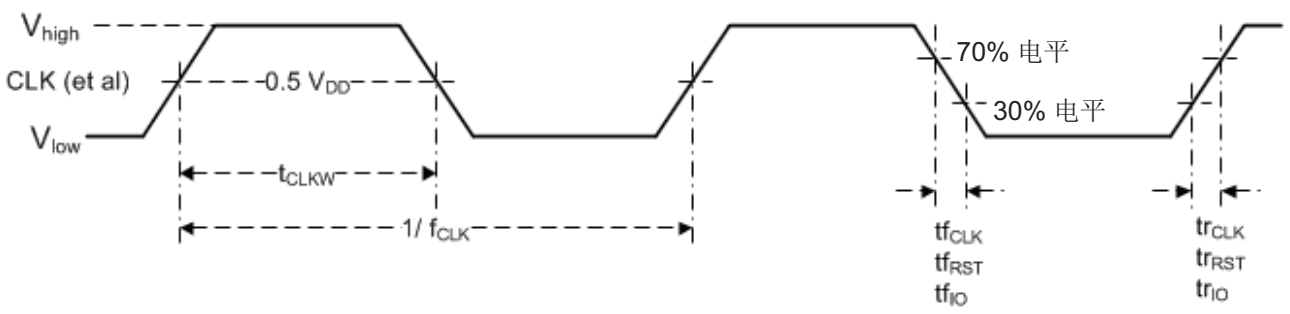


图 7. 开漏模式下， I2C_SDA、 I2C_SCL 和 RST_N 的外部时钟驱动和交流测试定时基准点（请参见表注 3 和表注 4）

13.3 EMC/EMI

符合 IEC 61967-4 的电磁兼容和抗电磁干扰要求。

14. 缩略词

表 14. 缩略词

首字母缩略词	说明
AES	高级加密标准
CRC	循环冗余检查
DES	数字加密标准
DPA	差分功耗分析
DSS	数字签名标准
ECC	椭圆曲线加密
EEPROM	电可擦可编程只读存储器
I/O	输入 / 输出
MAC	消息验证代码
OS	操作系统
PKI	公共密钥基础设施
SFI	单故障注入
SHA	安全哈希算法

15. 参考文献

[1] I^2C 总线规范和用户手册，第 3.0 版 — 2007 年 6 月 19 日，恩智浦半导体

[2] SOT909-1； HVSON8；卷盘封装；订购码 (12NC) 以 118 结尾；封装信息；第 2 版 — 2013 年 4 月 19 日

[3] 应用笔记 SCIIC 协议规范，第 Rev 1.5 版， an195015 — 2017 年 1 月 31 日

[4] 应用笔记 A71CL 安全模块，应用笔记 适用于阿里云的 APDU，第 1.1 版， AN12297

16. 修订记录

表 15. 修订记录

文档 ID	发布日期	数据手册状态	更改说明	取代版本
485030	2018/11/27	缩略版数据手册		
变更内容：	• 图 1 “A71CL 框图”更新 • 表 1 “A71CL 商业名称格式”更新 • 第 3.3 节 “加密功能”更新 • 表 3 “A71CL 特性表”更新 • 第 5 节 “订购信息”更新 • 图 2 “A71CL 功能框图 - 开放式 SSL 实例”更新 • 第 6.1 节 “功能框图”更新 • 第 15 节 “参考文献”更新 • 第 13.1.2 节 “3V3 模式下工作的 I2C 接口 [1]”更新 • 第 13.1.3 节 “1V8 模式下工作的 I2C 接口 [1]”更新 • 第 13.2 节 “交流特性”更新 • 将状态从初始缩略版数据手册更改为产品缩略版数据手册 • 标题更新 • 第 1 节 “简介”更新 • 表 3 “A71CL 特性表”更新 • 图 2 “A71CL 功能框图 - 开放式 SSL 实例”更新		
485010	2018-07-10	缩略版数据手册		
变更内容：	• 初始版本			

17. 法律信息

17.1 数据手册状态

文档状态 [1][2]	产品状态 [3]	定义
客观 [缩略版] 数据手册	开发	该文档包含产品开发客观规范的数据。
初始 [缩略版] 数据手册	验证	该文档含有初始规范的数据。
产品 [缩略版] 数据手册	生产	该文档含有产品规范。

[1] 请在开始或完成设计之前查看最新发布文件。

[2] 有关“缩略版数据手册”的说明见“定义”部分。

[3] 自本文件发布以来，文件中的器件产品状态可能已发生变化；如果存在多个器件，则可能存在差异。最新产品状态信息通过互联网发布，网址为：http://www.nxp.com

17.2 定义

初稿 — 本文仅为初稿版本。内容仍在内部审查，尚未正式批准，可能会有进一步修改或补充。恩智浦半导体对本文信息的准确性或完整性不做任何说明或保证，并对因使用此信息而导致的后果不承担任何责任。

缩略版数据手册 — 缩略版数据手册为产品型号和标题完全相同的完全版数据手册的节选。缩略版数据手册仅供快速参考使用，不包括详细和完整的信息。欲了解详细、完整的信息，请查看相关的完整版数据手册，可向当地的恩智浦半导体销售办事处索取。如完整版与缩略版存在任何不一致或冲突，请以完整版为准。

产品规格 — 产品数据手册中提供的信息和数据规定了恩智浦半导体与其客户之间约定的产品规格，恩智浦半导体及客户另行书面说明时除外。在任何情况下，若协议认为恩智浦半导体产品需要具有超出产品数据手册规定的功能和质量，则该协议无效。

17.3 免责声明

有限担保和责任 — 本文中的信息据信是准确和可靠的。但是，恩智浦半导体对此处所含信息的准确性或完整性不做任何明示或暗示的说明或保证，并对因使用此信息而导致的后果不承担任何责任。恩智浦半导体对此文档中超出恩智浦半导体信息源的内容不承担责任。恩智浦半导体不对本文中非源自恩智浦半导体的信息内容负责。

在任何情况下，对于任何间接、意外、惩罚性、特殊或衍生性损害（包括但不限于利润损失、积蓄损失、业务中断、因拆卸或更换任何产品而产生的开支或返工费用），无论此等损害是否基于侵权行为（包括过失）、担保、违约或任何其他法理，恩智浦半导体均不承担任何责任。

对于因任何原因给客户带来的任何损害，恩智浦半导体对本文所述产品的总计责任和累积责任仅限于*恩智浦商业销售条款和条件*所规定的范围。

修改权利 — 恩智浦半导体保留对本文所发布的信息（包括但不限于规格和产品说明）随时进行修改的权利，恕不另行通知。本文件将取代并替换之前就此提供的所有信息。

适宜使用 — 恩智浦半导体产品并非设计、授权或担保适合用于生命保障、生命关键或安全关键系统或设备，亦非设计、授权或担保适合用于在恩智浦半导体产品失效或故障时会导致人员受伤、死亡或严重财产或环境损害的应用。恩智浦半导体及其供应商对在此类设备或应用中加入和 / 或使用恩智浦半导体产品不承担任何责任，客户需自行承担因加入和 / 或使用恩智浦半导体产品而带来的风险。

应用 — 本文件所载任何产品的应用只用于例证目的。此类应用如不经进一步测试或修改用于特定用途，恩智浦半导体对其适用性不做任何说明或保证。

客户负责自行利用恩智浦半导体的产品进行设计和应用，对于应用或客户产品设计，恩智浦半导体无义务提供任何协助。客户须自行判断恩智浦半导体的产品是否适用于其应用和设计计划，以及是否适用于其第三方客户的规划应用。客户须提供适当的设计和操作安全保障措施，以最大程度降低与应用和产品相关的风险。

对于因客户应用或产品的任何缺陷或故障，或者客户的第三方客户的应用或使用导致的任何故障、损害、开支或问题，恩智浦半导体均不承担任何责任。客户负责对自己基于恩智浦半导体的产品的应用和产品进行所有必要测试，以避免这些应用和产品或者客户的第三方客户的应用或使用存在任何缺陷。恩智浦不承担与此相关的任何责任。

限值 — 超过一个或多个限值（如 IEC 60134 绝对最大额定值体系所规定）会给器件带来永久性损坏。限值仅为强度额定值，若设备工作于这些条件下或者超过“建议工作条件部分”（若有）或者本文档“特性”部分规定的条件下，则不在担保范围之内。持续或反复超过限值将对设备的质量和可靠性造成永久性、不可逆转的影响。

商业销售条款和条件 — 除非有效书面单项协议另有规定，恩智浦半导体的产品的销售遵循关于商业销售的一般条款和条件（见 http://www.nxp.com/profile/terms）。如果只达成了单项协议，则该协议的条款和条件适用。恩智浦半导体特此明确反对，应用客户就其购买恩智浦半导体的产品而制定的一般条款和条件。

出口管制 — 本文件以及此处所描述的产品可能受出口法规的管制。出口可能需要事先经相关主管部门批准。

快速参考数据 — 快速参考数据指本文件“限值”和“特性”部分所提供数据的节选，因此不完整、不详尽并且不具法律约束力。

非汽车应用产品 — 除非本数据手册明确表示，恩智浦半导体的本特定产品适用于汽车应用，否则，均不适用于汽车应用。未根据汽车测试或应用要求进行验证或测试。对于在汽车器件或应用中包括和 / 或使用非汽车应用产品的行为，恩智浦半导体不承担任何责任。

客户将产品用于设计导入以及符合汽车规范和标准的汽车应用时，客户 (a) 若使用产品，则恩智浦半导体不对产品的此等汽车应用、用途和规范作任何担保；并且 (b) 若客户使用恩智浦半导体所提供规格以外的产品用于汽车应用，须自行承担所有风险；并且 (c) 对于因客户设计以及客户超出恩智浦半导体标准担保范围和恩智浦半导体所提供规格使用非汽车应用产品而导致的任何责任、损害或产品故障索赔，客户须免除恩智浦半导体的全部责任。

翻译 — 非英文（翻译）版的文档仅供参考。如翻译版与英文版存在任何差异，以英文版为准。

17.4 许可

具有 DPA 反制功能的 IC

具有针对差分功率分析和简单功率分析反制功能的恩智浦 IC 仅在获得 Cryptography Research, Inc. 的适用许可的情况下生产和销售

17.5 商标

注意：所有引用的品牌、产品名称、服务名称以及商标均为其各自所有者的资产。

FabKey — NXP B.V. 的商标。

I²C 总线 — 该徽标是恩智浦的商标。

18. 联系信息

更多详情，请访问：**http://www.nxp.com**

欲咨询销售办事处地址，请发送电子邮件至：**salesaddresses@nxp.com**

19. 表

20. 图

21. 目录

续 >>

欲了解更多信息，请访问：http://www.nxp.com
欲咨询销售办事处地址，请发送电子邮件至：salesaddresses@nxp.com

发布日期：2018 年 11 月 28 日
485030