一种新型 MCU 加密方法

App. Notes

在 Xinnova 新推出的高性能 XN12L/XN62L 系列中，它支持一种与众不同的 MCU 加密方式。这种加密方式不但可以保护发布的软件免受他人窃取而失密，还可最大限度保护软件在开发过程因必要的团队工作而泄密。在如今信息高度发达，技术保密代价过高和困难的环境里，它给 MCU 用户提出一个全新嵌入式软件知识产权保护的方法。

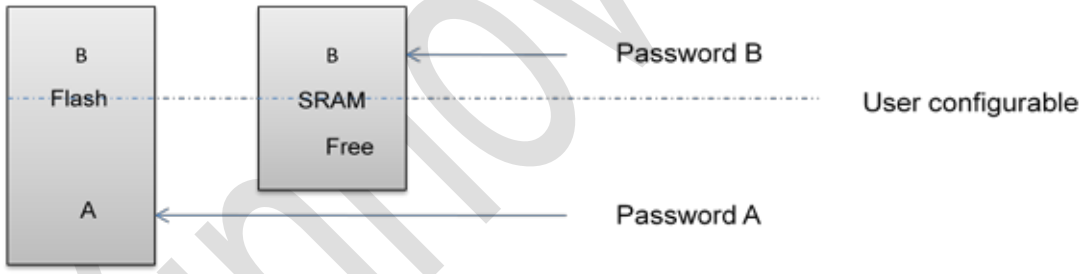
首先，Xinnova MCU 采用的是 128 位的密码加密。

使用密码加密在 MCU 中没有什么新鲜的，但用到 128 位密码，这是很少见的。128 位密码，如果采用遍历法来穷举是不可能的，因为这可能要花不知多少年才能破解。128 位的密码，这是极为牢固加密方式。

其次，Xinnova MCU 采用了两个 128 位密码可以对存储器（闪存和 SRAM）分区加密。

在当今的产品开发中，时间是一个重要因素。错过产品上市时间，再好的产品也变垃圾。因此，缩短开发时间，团队工作不可避免。而人员流动是当今社会的特点。如果不做好保密工作，你可能面临知识产权流失。Xinnova 的产品通过对存储器划分成两个区域，并使用不同的密码，可以让两个不同的开发背靠背同时进行，还可相互调用进行全系统调试。另一种情况是，设计公司掌握一些关键技术，而最终客户却想对产品再做一些定制，那么如何才能协调设计公司和最终客户呢？答案是采用 Xinnova 这种分区加密技术，设计公司可以把它的软件定义好接口并加密放在其中的一个区，而最终客户可通过接口进行调试而无法获取设计公司的代码拷贝。这样既满足了最终客户的需求，设计公司没有流失对关键技术掌握。

下图是 Xinnova MCU 加密方法一个简要概括



A 和 B 拥有各自的密码，当密码不对时，对外部都是不可读写的。但却可以按定义好接口调用程序。A/B 区域大小用户可以自行定义。

Xinnova MCU 提供针对加密功能的 ISP 和 IAP 接口。

ISP 接口命令：

命令	命令	参数个数	参数长度	数据
密码验证	#4AH	1	16	No
设置密码	#4BH	2	32	No
设置 B 区边界	#4CH	2	20	No
密码状态	#4DH	2	4	No

1. 密码验证

命令: 0x4AH

参数:

AB 区选择(32 位)	密码(128 位)

- AB 区选择。 0: A; 1: B.
- 密码: 128 位密码

返回代码: 0x4AH

参数:

AB 区选择(32 位)

2. 设置密码

命令: 0x4BH

参数:

AB 选择(32 位)	旧密码(128 位)	新密码(128 位)

- AB 选择。 0: A; 1: B.
- 旧密码: 128 位密码
- 新密码: 128 位密码

返回代码: 0x4BH

参数:

AB 选择(32 位)

3. 设置 B 区边界

命令: 0x4CH

参数:

AB 区选择(32 位)	128 位密码	Flash 边界(32 位)	SRAM 边界(32 位)

- AB 选择: 等于 1
- 密码: 128 位密码
- Flash 边界: 32 位边界地址
- SRAM 边界: 32 位边界地址

返回代码: 0x4CH

参数:

AB 选择(32 位)

4. 密码状态

命令: 0x4DH

返回代码: 0x4DH

参数:

A 区状态 (32 位)	B 区状态(32 位)	B 区 Flash 边界(32 位)	B 区 SRAM 边界(32 位)

- A 区状态。0: 已解锁; 非 0: 上锁
- B 区状态。0: 已解锁; 非 0: 上锁
- Flash 边界: 32 位边界地址
- SRAM 边界: 32 位边界地址

IAP 接口命令：

IAP 命令	寄存器 R0 指针					寄存器 R1 指针				
	命令代码	参数 1	参数 2	参数 3~6	参数 5~9	状态代码	结果 1	结果 2	结果 3	结果 4
密码效验	0x4A	A/B 选择	128 位密码		-	状态	-	-	-	-
设置密码	0x4B	A/B 选择	128 位旧密码		128 位新密码	状态	-	-	-	-
设置 B 区边界地址	0x4C	A/B 选择	128 位密码		B 边界	状态	Flash 边界设置状态	SRAM 边界设置状态	-	-
密码状态	0x4D					状态	A 密码状态	B 密码状态	B Flash 边界	B SRAM 边界

IAP 命令执行返回状态代码:

1. CMD_SUCC 0x00
2. INVALID_ADDR 0x01
3. INVALID_CMD 0x05
4. INVALID_PWD 0x06
5. IRC_NOT_POWERED 0x07

详细内容参照 Xinnova 网页的用户手册。