AN12527

LPC55Sxx 系列实时代码/数据加密引擎 PRINCE

Rev. 2 — 28 October 2020 Application Note

目录

1 PRINCE 简介

PRINCE 算法引擎用于对 LPC55Sxx 芯片上的闪存内容进行实时加密/解密操作。与 AES 相比，PRINCE 速度更快，因为它可以没有任何延迟的加密和解密。PRINCE 是在数据直接被读取或写入闪存时工作，而无需先将数据存储在 RAM 中，然后再解密或加密到另一个存储空间中。PRINCE 操作 64 位数据块，其密钥大小为 128 位。

此功能对于资产保护非常有用，例如保护应用程序代码，保护数据和启用安全的闪存更新。

芯片上的闪存可分为几个区域，用于加密/解密。LPC55Sxx 支持三个用于加密和解密的区域，称为加密区域。每个加密区域位于闪存内的一个 256KB 的地址边界处。对于 LPC55Sxx 中的大小为 640KB 的闪存，前两个加密区域的大小为 256KB，第三个加密区域的大小为 128KB。对于其它大小的闪存，可以通过配置寄存器 BASE_ADDRn 位[19:18]来设置区域范围。如果 BASE_ADDR1 中的位[19:18]为 0，则 region1 将覆盖从 0x0 到 0x3FFFF 的地址闪存。在本应用笔记中，以 640kB 的闪存大小为例，每个区域覆盖不同的闪存地址范围。

每个加密区域被细分为 8kB 子区域。可以为每个子区域启用或禁用 PRINCE 加密/解密。启用的子区域不必是连续的。

每个加密区域都有一个专用的密钥和一个初始化向量（IV）。这允许多个映像分别加密并驻留在闪存中。该密钥是通过内部专用硬件接口从芯片上的 SPAM PUF 中获取的，而没有将密钥暴露在系统总线上。

图 1 显示了一个为不同的 PRINCE 区域分配不同的存储区域的示例。标有“c”的子区域已启用“加密”，即已启用它们同时进行加密和解密。灰色子区域代表未使用。

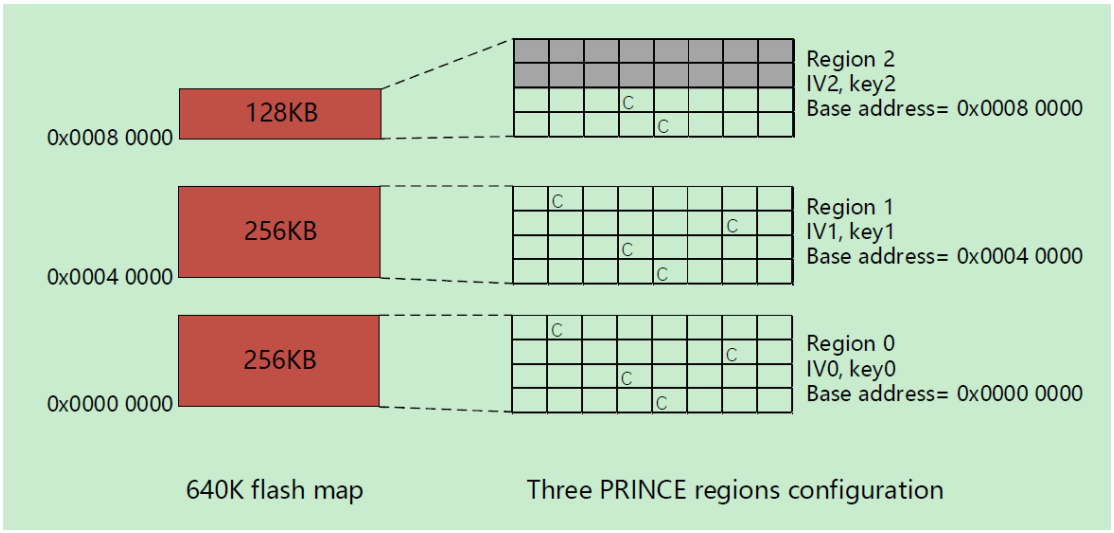

图 1. PRINCE 配置为 640KB 时内存图

图 2 显示了一个区域 0 和区域 1 覆盖了相同的 256KB 存储区域的示例。这样，客户可以在内存大小为 256KB 的芯片中使用不同的密钥来保护第二个引导程序和应用程序代码。

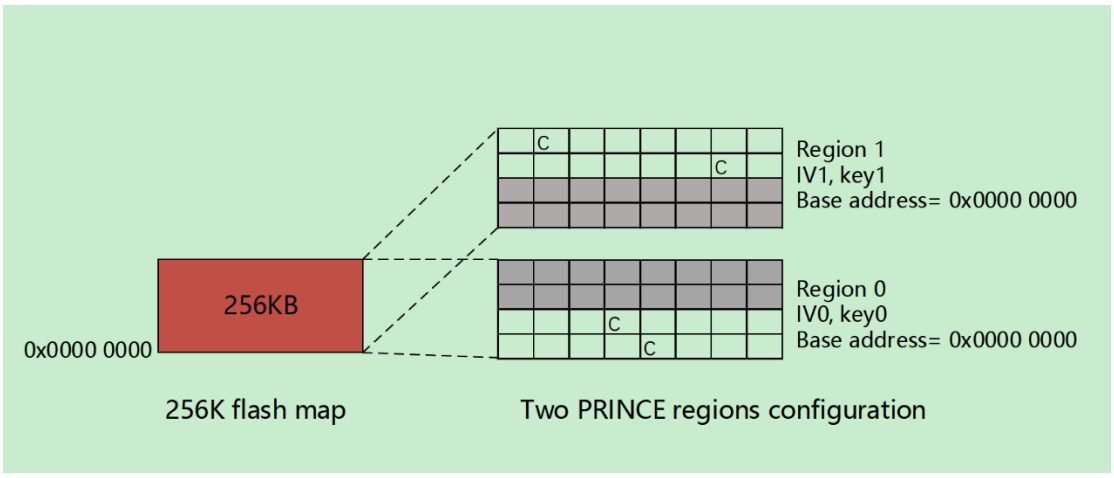

图 2. PRINCE 配置为 256KB 内存映射

2 PRINCE 的分步演示

用于 PRINCE 加密/解密的密钥来自芯片上 SPAM PUF。密钥库存储在闪存的 PFR 区域中，地址为 0x9E600，其中包含设备的激活代码和各个 PRINCE 区域的 PRINCE 密钥的键码。PRINCE 密钥通过内部硬件接口提供，不能通过软件访问。每次复位时，引导 ROM 都会读取密钥库并将 PRINCE 密钥重构到 PRINCE 引擎中。blhost 实用程序可用于将密钥设置到 LPC55Sxx 器件中。在密钥配置过程中，激活码和键码最初存储在设备的内部 SRAM 中，然后存储在 PFR 区域中。

现在使设备进入 UART ISP 模式并打开 blhost。

2.1 与 PRINCE 相关的 PUF 密钥库设置

在以下示例中，你可以看到从 PC blhost 应用程序通过 ISP 模式向设备下发命令序列，以生成正确的启用 PRINCE 的密钥库。密钥库被保存到设备 PFR 中，并在安全引导期间由引导 ROM 访问。

警告

在芯片的整个生命周期内，每个设备只执行一次密钥配置注册操作。理想状况下，最好在芯片的整个生命周期中执行一次 set_key/write_key_nonvolatile 操作。换句话说，密钥配置完成后，无需再次执行这些命令。PRINCE 的配置和闪存的擦除/编程可以在以后重复做。

注

本应用笔记中的实验使用的是 1B 修订版芯片

警告

在执行完密钥配置 write_key_nonvolatile 步骤之后，必须通过复位引脚或 POR（上电）复位芯片，以便可以将新密钥成功发送到 PRINCE 引擎。

1. 打开 blhost PC 工具，使用 UART 连接到处理器（在本示例中 UART 为 COM108）。在复位时按下 ISP 引脚，可使处理器进入 ISP 模式。
2. 获取 bootROM 的版本并检查通讯的可用性。

```
blhost.exe -p COM108 -- get-property 1
```

3. 生成设备激活码并将其存储到密钥库结构中。

```
blhost.exe -p COM108 -- key-provisioning enroll
```

4. 生成随机的 PRINCE 区域 0。（PRINCE 区域 0 密钥类型=7）

```
blhost.exe -p COM108 -- key-provisioning set_key 7 16
```

5. 生成随机的 PRINCE 区域 1.（PRINCE 区域 1 密钥类型=8）

```
blhost.exe -p COM108 -- key-provisioning set_key 8 16
```

6. 生成随机的 PRINCE 区域 2.（PRINCE 区域 2 密钥类型=9）

```
blhost.exe -p COM108 -- key-provisioning set_key 9 16
```

7. 将密钥库保存到闪存的 PFR 页中。

```
blhost.exe -p COM108 -- key-provisioning write_key_nonvolatile 0
```

8. 按复位引脚或 POR 复位设备。

2.2 PRINCE 区域配置

对于 PRINCE 加密和解密，配置了用于加密操作的区域和子区域。这可以通过 ISP 命令“configure-memory”来完成。必须使用以下数据结构调用此命令。

Offset	Size	Description
0	4	PRINCE Configuration
4	8	PRINCE Region info

Table 193. PRINCE configuration register for configure-memory command

Bit	Symbol
1:0	0x00 – PRINCE Region 0 0x01 – PRINCE Region 1 0x10 – PRINCE Region 2
25:2	Reserved
31:8	0x50 ('P') – Configure PRINCE

Table 194. PRINCE region info register for configure-memory command

Bit	Symbol
31:0	PRINCE Region X Start
63:32	PRINCE Region X size

图 3. configure-memory 命令的结构

将此结构加载到 RAM 内存中，并按照以下顺序调用“configure memory”命令：

警告

加密区域的长度必须等于以后要擦除的范围，并且等于以后要编程的范围。因此，必须在创建的二进制文件的末尾填充特定的模式数据，以便与长度对齐。

1. 使用 UART 重新连接到处理器（在本示例中，UART 为 COM108）。在复位阶段，通过按 ISP 引脚使处理器进入 ISP 模式。
2. 获取 bootROM 的版本并检查通讯的可用性。

```
blhost.exe -p COM108 -- get-property 1
```

3. 区域选择（在本示例中区域为 0）。

```
blhost.exe -p COM108 -- fill-memory 0x20034000 4 0x50000000
```

4. 加密区域的起始地址（在本示例中地址为 0x0）。

```
blhost.exe -p COM108 -- fill-memory 0x20034004 4 0
```

5. 加密区域的长度（在此示例中为 0x10000）。

```
blhost.exe -p COM108 -- fill-memory 0x20034008 4 0x10000
```

6. 用在 RAM 中使用已准备好的结构调用 configure-memory。

```
blhost.exe -p COM108 -- configure-memory 0 0x20034000
```

警告

完成上述配置命令后，请勿复位板卡，而是继续执行闪存擦除和加载映像的命令。

执行完以上命令后，PRINCE 已配置好对闪存进行加密。

注

PFR 区域应从 PRINCE 加密区域中排除掉。即必须对以上配置结构中的开始和大小进行相应设置，以避免与 PFR 区域重叠。

2.3 擦除闪存并上传程序映像

在引导 ROM 中实现了“prince erase checker”，用于检查是否立即擦除了由一个或多个子区域组成的整个 PRINCE 使能区域。类似地，在 ROM 代码中实现了“prince flash write checker”，以检查是否立即对包括一个或多个子区域的整个使能区域进行了编程。要加载由 PRINCE 即时加密的映像，使用 blhost 工具发出以下 ISP 命令序列。

警告

如果加密区域的长度为如上所述的 0x10000，则擦除和编程区域应设置为 0x10000。二进制文件大小必须为 0x10000。

【准备】

打开并编译一个 LPC55Sxx 项目，生成二进制文件。将模式 0x55 填充到二进制文件中，使其大小为 0x10000 字节。本示例使用一个来自 SDK 的名为 hello_world_0x10000_size.bin 的文件，该文件已扩大为 0x10000 字节。禁用 PRINCE 子区域并读取该子区域中的闪存值。接收到真实的闪存值。这意味着可以验证 PRINCE 功能。有关详细信息，请参见 图 4.

```c
int main(void)
{
    char ch;
    int value;

    /* Init board hardware. */
    /* attach main clock divide to FLEXCOMM0 (debug console) */
    CLOCK_AttachClk(BOARD_DEBUG_UART_CLK_ATTACH);

    BOARD_InitPins();
    BOARD_BootClockPLL150M();
    BOARD_InitDebugConsole();

    PRINTF("hello world.\r\n");

    PRINTF("the value after configure the PRINCE enable by blhost .\r\n");
    value = *(int *)0xF000;//read the value decrypted by PRINCE located at 0xF000.
    PRINTF("the value of address 0xF000 is :%x\r\n",value);
    PRINCE->SR_ENABLE0 = 0x7F;//disable prince to the rang from 0xE000 to 0xFFFF
    PRINTF("the value after PRINCE disable in the app code.\r\n");
    value = *(int *)0xF000;//read the true flash value located at 0xF000.
    PRINTF("the value of address 0xF000 is :%x\r\n",value);

    while (1)
    {
        ch = GETCHAR();
        PUTCHAR(ch);
    }
}
```

图 4. 应用代码

1. 擦除闪存（在此示例中为 0x10000）。

```
blhost.exe -p COM108 -- flash-erase-region 0x0 0x10000
```

2. 将程序映像加载到闪存中。

```
blhost.exe -p COM108 -- write-memory 0 hello_world_0x10000_size.bin
```

3. 完成这些步骤后，闪存中加载的程序将被加密。

注

在特定条件下，当发送带有校验功能的部分擦除和编程命令时，可能会收到成功的通用响应。该结果并不代表允许部分擦除和编程，并且可能导致无法控制的状态。因此，整个 PRINCE 使能区域必须执行一次。

注

擦除和编程的范围不得超过一个区域大小（256K 字节）。如果 PRINCE 启用了多个区域，则按区域分别进行擦除和编程。

2.4 运行代码

1. 使用 UART 重新连接到处理器并打开串口助手 CommAssistant。
2. 按复位引脚或 POR 复位设备。字符串显示在 图 5 中。

```
hello world.
the value after configure the PRINCE enable by blhost .
the value of address 0xF000 is :55555555
the value after PRINCE disable in the app code.
the value of address 0xF000 is :530d8cfb
```

图 5. CommAssistant 窗口

注

禁用 PRINCE 后地址 0xF000 的值不会永远是 0x530d8cfb，它取决于每个实验中的特定条件。

3 修订记录

表 1 总结了对本文档的更改。

表 1. 修订记录

版本号	日期	说明
0	25/10/2019	初始版本
1	26/05/2020	更新了“PRINCE 简介”
2	28/10/2020	“LPC55S6x/LPC55S2x/LPC552x”替换成“LPC55Sxx”

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

Limited warranty and liability — Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

Right to make changes - NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer’s applications and products. Customer’s responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer’s applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 28 October 2020
Document identifier: AN12527

arm