NXP Semiconductors
Application Notes

Document Number: AN12527
Rev. 3, 05/2021

LPC55Sxx的PRINCE实时数据加密

原文链接：https://www.nxp.com/docs/en/applicationnote/AN12527.pdf

1. PRINCE简介

PRINCE 算法用于对 LPC55Sxx 的片上闪存的内容进行实时加密/解密操作。与 AES 相比， PRINCE 的速度更快，因为它无需增加额外延迟即可进行解密和加密。PRINCE 在数据读取或写入闪存时操作，而无需先将数据存储在 RAM 中，然后再加密或解密到另一个内存空间。PRINCE 以 64 位的块进行操作，采用 128 位的密钥。

目录

此功能对于资产保护非常有用，例如加密应用程序代码、加密数据和启用安全闪存更新。

片上闪存分为三个区域进行加密/解密。这些区域被称为保密区域。LPC55Sxx 支持三个区域的加密和解密，即为保密区域。每个保密区域位于闪存内的 256 kB 地址边界处。对于 LPC55Sxx 中 640 kB 的闪存，前两个保密区域的大小为 256 kB，第三个为 128 kB。对于其他大小的闪存，可以通过配置寄存器 BASE_ADDRn 的 [19:18] 位来设置区域范围。如果 BASE_ADDR1 中的 [19:18] 位为 0x0，则区域 1 将覆盖 0x0 到 0x3FFFF 闪存地址。在本应用笔记中，以 640 kB 闪存大小为例，每个区域覆盖不同的闪存地址范围。

每个保密区域可细分为 8 kB 的子区域。可以为每个子区域启用或禁用 PRINCE 加密/解密。启用的子区域不需要是连续的。

每个保密区域都有一个专用密钥和一个初始化向量（IV）。这允许多个镜像驻留在具有独立加密基础的闪存中。密钥通过内部硬件接口从片上 SRAM PUF 获取，不会将密钥暴露在系统总线上。

图 1 显示了一个示例，其中为不同的 PRINCE 区域分配了不同的内存区域。标有“c”的子区域为“保密（crypto）”已启用，即加密和解密都启用。灰色子区域代表未使用。

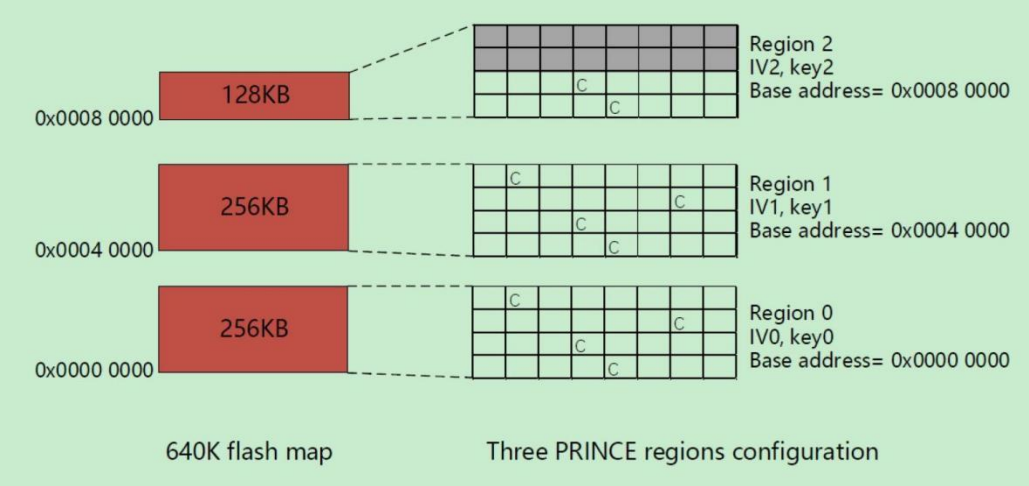

图 1. PRINCE 对于 512KB 内存映射的配置

图 2 显示了一个示例，其中区域 0 和区域 1 覆盖相同的 256 KB 内存区域。这样，客户可以在具有 256 KB 闪存的芯片中，使用不同的密钥来加密二级引导加载程序和应用程序代码。

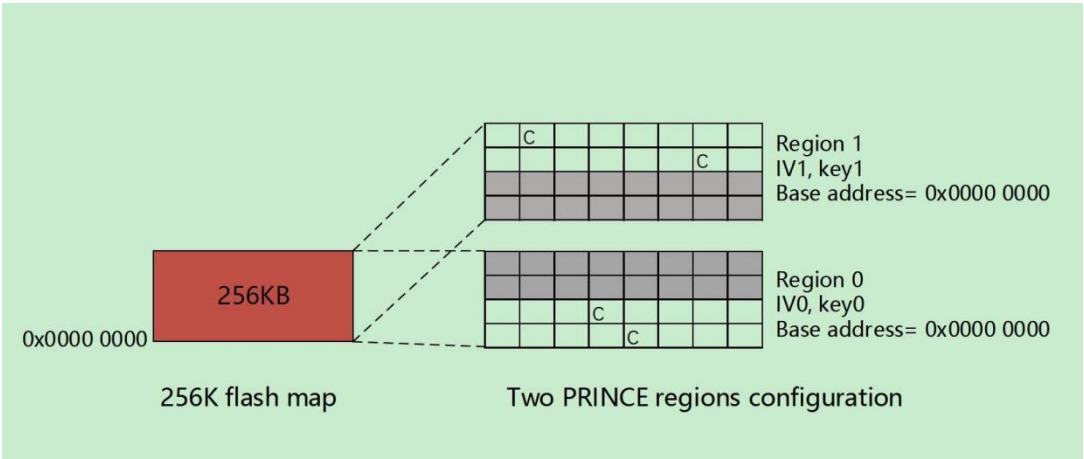

图 2. PRINCE 对于 256KB 内存映射的配置

2. PRINCE 按步骤演示

用于 PRINCE 加密/解密的密钥需从片上 SRAM PUF 获取。密钥存储库存储在闪存的 FFR 区域中，地址为 0x9E600，其中包含设备的激活码和各个 PRINCE 区域的 PRINCE 密钥的密钥码。PRINCE 密钥通过内部硬件接口分发，不可通过软件访问。每次复位时，引导 ROM 读取密钥库并将 PRINCE 密钥重建到 PRINCE 引擎中。

BLHOST 实用程序可用于向 LPC55Sxx 设备授发密钥。授发过程中，激活码和密钥码最初存储在设备的内部 SRAM 中，随后存储到 PFR 区域。

让设备进入 UART ISP 模式并打开 BLHOST。

2.1. PRINCE相关的PUF密钥存储设置

在以下示例中，您可以看到在 ISP 模式下从 PC blhost 应用程序向设备发出的命令序列，用以生成正确的 PRINCE 启用的密钥存储。密钥存储保存到设备的 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授发注册操作。理想情况下， set_key/write_key_nonvolatile 操作最好在芯片的整个生命周期内执行一次。换句话说，在完成密钥授发后不需要再次执行这些命令。PRINCE 配置和闪存擦除/编程可以在以后重复进行。

注意

本应用笔记中的实验使用 1B 修订版芯片。

警告

执行 *key-provisioning write_key_nonvolatile* 步骤后，芯片必须通过复位脚或上电复位，这样新的 密钥才能成功发送到 PRINCE 引擎。

1 打开 blhost PC 工具，使用 UART 连接到处理器（本例中UART 为 COM108）。在复位阶段按下 ISP 引脚，使处理器进入 ISP 模式。

2 获取 bootROM 的版本并检查通信的可用性。

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

3 生成设备激活码并将其存储到密钥存储结构中。

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

4 生成随机 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 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 PRINCE 区域 2。（PRINCE 区域 2 密钥类型=9）

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

7. 将钥匙存储保存到闪存的 PFR 页

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

8 按下复位引脚或重新上电以重置设备。

2.2. PRINCE 区域设置

对于 PRINCE 加密和解密，保密操作的区域和子区域是要配置的。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

将结构加载到 RAM 存储区中并使用以下序列调用“configure-memory”命令：

警告

加密区域的长度必须等于之后要擦除的范围和要编程的范围。因此，必须在您创建的二进制文件的末尾填充某些内容以使长度相符。

1 使用 UART 再次连接到处理器（在本例中，UART 为 COM108）。在复位阶段按下 ISP 引脚，使处理器进入 ISP 模式。

2 获取 bootROM 的版本并检查通信的可用性。

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

3 区域选择（本例中为区域 0）。

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

4 加密区域的起始地址（本例中为地址 0x0）。

```
blhost.exe  -p  COM108 -- fill-memory  0x20034004 40
```

5 加密区域的长度（本例中为 0x10000）。

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

6 采用 RAM 中准备好数据结构，调用配置内存命令。

```
blhost.exe  -p  COM108 -- configure-memory  00x20034000
```

警告

完成上述配置命令后，不要复位电路板、继续执行命令来擦除闪存以及加载镜像。

根据此命令，PRINCE 被配置为闪存加密。

注意

PFR 区域应该被排除在 PRINCE 加密区域之外。也就是说，配置数据结构中的起始地址和长度设置必须避免与 PFR 区域重叠。

2.3. 擦除闪存并上传镜像

“PRINCE 擦除检查器”已放置在引导 ROM 中，它可以立即检查由一个或多个子区域组成的整个 PRINCE 启用区域是否被擦除。类似地，“PRINCE 闪存写入检查器”也放置在 ROM 代码中，用以立即检查由一个或多个子区域组成的整个启用区域是否被编程。要加载 PRINCE 即时加密的镜像，请使用 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。二进制文件大小也必须为 0x10000。

[准备]：

注意

本应用的相关软件项目以 LPC5569 芯片为核心。对于其他型号的芯片，用户应创建相应的 SDK 项目和二进制文件。

打开并编译一个 LPC55Sxx 项目，创建二进制文件。将内容（即 0x55）填充到二进制文件中，使其大小为 0x10000 字节。本例使用一个名为 hello_world_0x10000_size. bin 的文件，该文件来自SDK，已被扩充到 0x10000 字节。

禁用一个 PRINCE 子区域并读取该子区域闪存中的值，可以接收到真实的闪存内容。这意味着可以验证 PRINCE 功能。有关详细信息，请参见图 4。

```
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. APP 代码

1 擦除闪存（本例中为 0x10000）。

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

2 将镜像加载到闪存中。

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

3 完成这些步骤后，加载到闪存中的镜像将被加密。

注意

在特定条件下，当部分擦除和编程命令与检查命令一起被发送后，可能会收到成功的常规响应。此结果不代表允许部分擦除和编程，并可能导致无法控制的状态。因此，整个 PRINCE 启用区域必须一次全部执行。

注意

擦除和编程范围不得超过一个区域大小（256 K 字节）。如果 PRINCE 启用了多个区域，则擦除和编程应按区域逐个进行。

2.4. 运行代码

1 使用 UART 再次连接处理器并打开 CommAssistant。

2 按下复位引脚或重新上电以重置设备。

字符串打印在图 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 window

注意

禁用 PRINCE 后地址 0xF000 的值并不永远是 0x530d8cfb，它基于每个实验中的特定条件。

3 修订历史

表 1 总结了对本文件的更改。

表 1. 修订历史

Rev.	日期	描述
0	25/10/2019	初始版本
1	26/05/2020	PRINCE 简介更新
2	28/10/2020	替换 LPC55S6x/LPC55S2x/LPC552x 的 LPC55Sxx
3	2021 年 5 月 11 日	在擦除闪存和镜像上传中添加了一个注释

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

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: 11 May, 2021
Document identifier: AN12527