高速SPI接口在SIM卡上的应用设计

Design of High-speed SPI Interface Application on SIM Card

王海涛，衣莉莉，孙阳阳，刘　觅（联通华盛通信有限公司，北京 100032）
Wang Haitao，Yi Lili，Sun Yangyang，Liu Mi（Unicom Vsens Communications Co.，Ltd.，Beijing 100032，China）

摘　要：
通过对当前物联网的安全威胁进行深入分析，发现SIM卡安全方案在实际使用过程中存在的一些问题。鉴于此，结合安全元件（SE）的SPI接口优点，设计了SPI接口应用在SIM卡上的全新方案，详述了该方案的软硬件架构，最后阐述了该方案在实际应用中所具有的优势。

关键词：
SPI；SIM；SE；物联网安全
doi：10.12045/j.issn.1007-3043.2024.06.010
文章编号：1007-3043（2024）06-0047-04
中图分类号：TN929.5
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Through an in-depth analysis of current security threats in the Internet of Things （IoT），some issues with SIM card security solutions in practical use are discoverd. In light of this，combined with the advantages of Secure Elements （SE） with SPI interface，a novel approach integrating SPI interface into SIM cards has been devised. A comprehensive elucidation of the software and hardware architecture of this approach has been provided. Furthermore，the advantages of this approach in real-world applications have also been expounded upon.

Keywords：
SPI；SIM；SE；Internet of Things Security

引用格式：王海涛，衣莉莉，孙阳阳，等. 高速SPI接口在SIM卡上的应用设计[J]. 邮电设计技术，2024（6）：47-50.

1 概述

随着物联网设备的普及和应用范围不断扩大，物联网设备的安全问题逐渐凸显，已成为迫切需要解决的重要问题。目前解决物联网设备安全问题主要有2种解决方案：一是增加单独的SE模块（Secure Element）；二是复用运营商的SIM卡。SIM卡作为运营商蜂窝网络身份鉴权的载体，除具备基础通信能力外，天然具有安全存储和数据加解密运算能力，非常适合用来解决物联网终端风险中的数据安全风险问题。

收稿日期：2024-04-06

然而在SIM卡实际的使用过程中，存在以下2个方面的问题。

a）SIM卡传输速率较低。SIM卡仅有一个ISO7816接口，对外通信采用半双工模式，理论最大传输速率为270 kbit/s，接口性能仅能满足传输数据量小、交互频率低的设备需求。然而，物联网终端通常需要采集和传输大量数据，对数据传输接口速率要求较高。以常见的1080P（200万像素）单路摄像头为例，其传输速率可达4 Mbit/s，SIM卡的ISO7816接口性能存在瓶颈，限制了SIM卡安全能力的输出，同时也制约了SIM卡在物联网设备安全解决方案中的快速发展。

b）SIM卡接口能力受到限制。安全元件（SE）模

块可以通过SPI（Serial Peripheral Interface）接口与基带芯片或主控芯片通信。与SE模块不同，SIM卡仅通过ISO7816直接与基带芯片连接，缺乏其他接口。外部的主控芯片只能通过基带芯片提供的AT指令来调用SIM卡的功能，无法直接访问。因此，在某些情况下，主控芯片无法充分利用SIM卡的功能，从而限制了其灵活性。

为了解决SIM卡传输速率低和接口能力不足的问题，本文借鉴了SE模块的SPI接口，设计了支持SPI接口的SIM卡。这一设计在保留SIM卡原有通信功能的基础上，增加了通用的SPI接口。这一创新使SIM卡能够为各种物联网应用提供安全、稳定、快速的连接，实现远程监控、数据采集、远程控制等功能，从而提升生产效率，优化资源利用，改善服务质量。

2 SIM卡接口能力现状

2.1 国际标准现状

目前，全球通用的SIM接口标准主要是ISO/IEC 7816系列标准，它定义了SIM卡与终端设备之间的电器接口和通信协议，涵盖了SIM卡的物理尺寸、电器特性、通信协议等方面。然而，SPI接口在一些特定场景中被广泛使用，但支持SPI接口的SIM卡并未成为国际标准。

2.2 现有SIM接口现状

目前，大多数SIM卡采用ISO7816标准定义的接口。ISO7816接口规定了物理、电气和传输特性，以及命令结构和数据传输协议。然而，ISO7816接口对外通信采用半双工模式，标准速率通常在几kbit/s到几十kbit/s的范围。这种接口的主要限制为传输速率相对较低，且通信方式相对固定，无法满足某些需要高速数据传输和更灵活通信方式的应用需求。

2.3 SPI接口能力现状

SPI接口是一种串行外设接口，通常用于在微控制器和外部设备之间的通信[1]。

a）高速传输。SPI接口可以实现高速数据传输，通常速度可以达到几百kbit/s到几十Mbit/s，甚至更高，具体取决于设备的支持和设置。

b）简单灵活。SPI接口的通信方式相对简单，由主设备（通常是微控制器）发起通信，并控制通信时序。这种简单的通信方式使SPI接口在许多应用中具有较高的灵活性。

c）双向通信。SPI接口支持全双工通信，允许同时进行数据的发送和接收，这使得它适用于需要双向数据传输的应用场景。

d）硬件支持。SPI接口通常由硬件支持，可以在微控制器或其他集成电路中找到专门的SPI外设，这简化了软件的设计和开发。

总之，SPI接口在高速传输、简单灵活、双向通信和硬件支持等方面具有较高能力，从而被广泛应用。

3 支持SPI接口的SIM卡设计

3.1 硬件架构

支持高速SPI接口的SIM卡采用了更强大的处理器和更高性能的CPU。这种处理器具有更高的时钟速度和更大的能力，能够更迅速地处理通信数据，从而提高SIM卡的响应速度（见图1）。

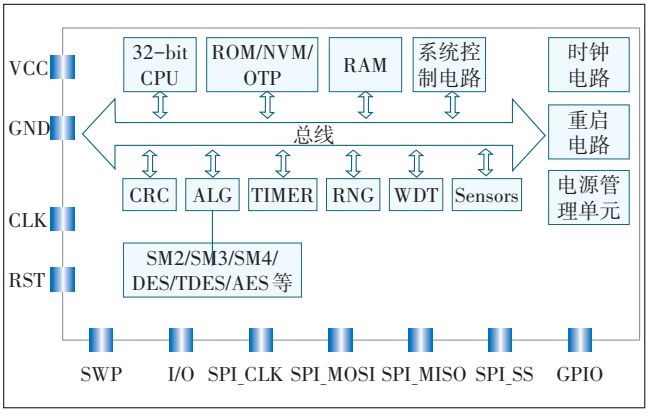

图1 支持高速SPI接口的SIM卡硬件架构

此外，支持高速SPI接口的SIM卡还采用了更大容量的RAM和ROM存储器。这意味着SIM卡能够存储更多的数据、应用程序，并进行更多的数据交换。它还支持更多的算法和应用程序，因此提供更高的安全性和灵活性。

除了ISO7816标准的VCC/GND/CLK/RST/IO引脚外，支持高速SPI接口的SIM卡还提供了更多的外部接口选项，如SWP接口、SPI接口、I2C接口、UART接口等。SPI接口速率通常可达20 Mbit/s，使得支持高速SPI接口的SIM卡能够更快地与各种设备通信，从而提高了数据传输效率。

最后，支持高速SPI接口的SIM卡支持DMA（Direct Memory Access）方式传输数据，这意味着数据可以在SIM卡和设备之间直接传输，而无需CPU的干预。这不仅提高了数据传输效率，还减轻了CPU的负担。

综上所述，与传统的SIM卡相比，支持高速SPI接

口的SIM卡具有更高的性能、更大的存储容量、支持更多的算法、更多的外部接口选项以及更高的数据传输效率。这使得支持高速SPI接口的SIM卡能够被广泛应用于各种移动设备和通信设备中。

3.2 软件架构

3.2.1 UICC框架

支持高速SPI接口的SIM卡以UICC多应用平台为基础进行构建，引入JavaCard虚拟机（JCVM）[2-3]、JavaCard运行环境（JCRE）、GlobalPlatform运行环境（OPEN）等多类应用的运行环境，实现了多个维度的“一卡多应用”功能。具体而言，此SIM卡具备在1张卡上完成接触式应用与非接触应用、电信应用（Network Access Application，NAA，如SIM、USIM）和非电信应用等多种应用，并能够满足业务的多样需求，是一种可应用于跨领域业务的电信智能卡。

如图2所示，支持高速SPI接口的SIM卡软件包括2个主要部分，即底层架构和应用层。底层架构包括UICC框架（UICC Framework）、JavaCard虚拟机（JavaCard VM）、JavaCard运行环境（JavaCard RE）、GP运行环境（OPEN and GP Trusted Framework）、非接触框架（Contactless Framework）、USIM、USAT以及API接口。应用层则包含安全域（SD/ISD）和应用（Applet）。

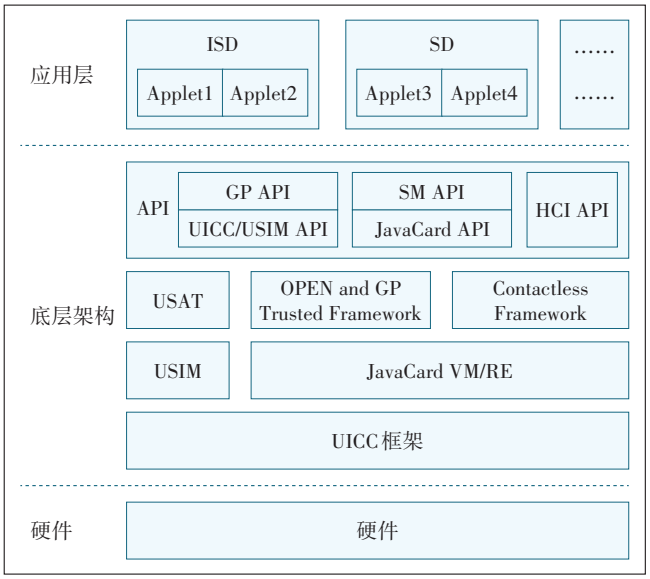

图2　支持高速SPI接口的SIM卡软件架构

3.2.2 JavaCard虚拟机

JavaCard虚拟机符合JavaCard平台相关要求，提供了一种基于Java技术的智能卡应用程序平台，是运行在智能卡芯片的虚拟机，负责解释和执行JavaCard应用程序的字节码。

JavaCard虚拟机在支持SPI接口的SIM卡上运行，需要JavaCard虚拟机支持与SPI接口通信相关的功能。具体来说，JavaCard虚拟机需要具备以下能力。

a）SPI接口访问权限。JavaCard应用需要能够访问芯片上的SPI接口，以便与外部设备进行通信。因此，JavaCard虚拟机需要提供相应的API或框架，以允许JavaCard程序通过API调用与SPI接口进行交互。

b）SPI通信协议支持。JavaCard虚拟机需要能够识别和处理SPI通信协议。这包括在JavaCard应用程序中对SPI接口进行配置（如时钟频率、数据格式等）、发送和接收数据等操作。

c）安全性支持。由于JavaCard应用程序通常处理敏感数据，因此JavaCard虚拟机需要提供安全机制来确保SPI接口通信的安全性。

3.2.3 JavaCard运行环境

JavaCard运行环境符合JavaCard平台相关要求，负责JavaCard应用程序的管理、生命周期控制、安全管理等任务。

具备JavaCard运行环境的SIM卡支持SPI接口，JavaCard运行环境需要具备以下能力。

a）SPI通信协议支持。JavaCard运行环境需要提供与SPI接口通信相关的API并能够识别和处理SPI通信协议，以允许JavaCard应用程序通过JavaCard API与SPI接口进行交互，如配置SPI接口参数，发送和接收数据等功能。

b）安全性支持。由于JavaCard应用程序通常处理敏感数据，JavaCard运行环境需要提供安全机制来确保SPI接口通信的安全性。这包括对通信数据加密、身份验证、访问控制等功能，以确保通信的机密性和完整性。

c）资源管理。JavaCard运行环境需要能够有效识别SIM卡上SPI接口所需的硬件资源，包括SPI接口与其他应用程序或系统组件之间的正确共享和管理。

3.2.4 GP运行环境

GP运行环境符合GlobalPlatform Card Specification等国际规范，提供了多种安全和管理服务，包括应用程序加载、个人化、远程管理、升级和卸载等功能[4]。

具备GP运行环境的SIM卡支持SPI接口，需要GP运行环境提供SPI接口权限控制能力。SPI接口访问控制权限主要限制SPI接口上应用的运行，只有指定的应用才允许在SPI接口上激活。

3.2.5 非接触式框架

非接触式框架遵循GlobalPlatform组织的相关国际规范，在UICC多应用平台的基础上增加了非接触式通信功能，以满足非接触式应用的需求。

3.2.6 USIM/USAT

USIM应用符合国际规范3GPP TS 31.102，它规定了GSM、UMTS、LTE、5G移动通信网络中智能卡的物理和电气特性、基础传输协议、应用和文件结构基础定义、命令结构等方面的要求，保证智能卡在移动通信网络中的互操作性、安全性和可靠性。

USAT是一种应用于SIM卡或USIM卡的应用工具集，提供了一组命令和应用，用于与移动设备通信并实现各种功能，增强移动设备的智能化和用户体验。

3.2.7 API

API（Application Programming Interface）是一组定义软件组件如何通信、如何交互的接口标准。在UICC（Universal Integrated Circuit Card）中，API接口包含GP API、USIM API、UICC API、国密API、JavaCard API、HCI API等，为开发人员提供了访问UICC中JavaCard应用程序的标准接口。

3.2.8 安全域和应用程序

安全域是一种基于智能卡的应用程序集合，由智能卡的应用程序开发人员或应用程序提供商创建和管理。一个安全域通常包含多个应用程序，这些应用程序可以相互协作，提供更为复杂的功能。每个安全域都有其独立的文件系统和应用程序管理器，可以保证安全域内的应用程序独立运行，互不干扰。

应用程序是指安装在智能卡中的程序，可以是原生的二进制代码，也可以是基于JavaCard虚拟机（JCVM）的Java应用程序。与安全域不同的是，应用程序通常只包含一个单一的功能模块，也可能是一个与其他应用程序合作完成某个功能的集合。

4 支持SPI接口的SIM卡应用

现有的物联网终端主控单元（MCU）芯片中，SPI作为其数据传输的常规接口，可以考虑通过在物联网终端的MCU与SIM卡之间建立基于SPI接口的连接，向终端输出安全能力，以便充分发挥SIM卡在物联网终端侧的数据安全作用，实现终端的全面安全保护（见图3）。

为了充分利用SIM卡在物联网终端侧的数据安全功能，除了建立支持SPI接口能力的连接外，还需提供

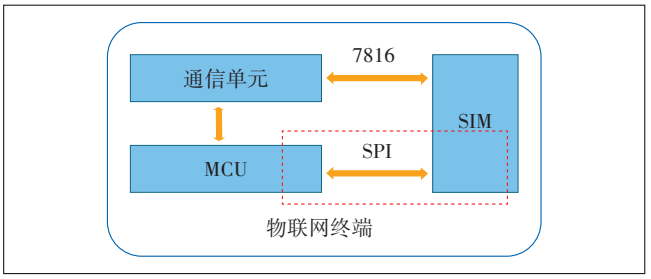

图3 支持高速SPI接口的SIM卡连接示意

标准接口的终端SDK包，以方便终端集成。SDK包可为终端开发人员提供访问SIM卡的标准接口，降低访问SIM卡的复杂性，同时有助于维护应用程序和数据的安全性。通过提供标准接口，还可以促进终端与SIM卡之间的互操作性，实现更高效、更可靠的数据传输。

5 总结

通过对现有SIM卡功能的分析，并结合SE的SPI接口优点，设计了一种支持高速SPI接口的SIM卡，提出了更为广泛的物联网终端安全解决方案。为实现这一方案，需要对现有物联网终端进行重新设计，建立物联网终端与支持高速SPI接口的SIM卡之间的电路结构。建议与产业链合作伙伴共同开展支持SPI接口规范的SIM卡数据传输方案研究，以实现SIM卡与MCU之间的数据传输能力。同时，为了推动该技术的应用和发展，应通过产业联盟或行业协会来推动制定行业标准，并与上下游合作伙伴广泛合作，共同开展物联网终端安全领域的创新和产品落地。这样可以更好地解决物联网终端上的安全问题，确保用户的数据安全。

参考文献：

[1] SPI接口协议[EB/OL].[2024-03-30].https://en.wikipedia.org/wiki/Serial_Peripheral_Interface.

[2] Java Card虚拟机[EB/OL].[2024-03-30].https://docs.oracle.com/javacard/3.1/related-docs/JCVMS/JCVMS.pdf.

[3] Java Card运行环境[EB/OL].[2024-03-30].https://docs.oracle.com/javacard/3.1/related-docs/JCCRE/JCCRE.pdf.

[4] GlobalPlatform安全框架[EB/OL].[2024-03-30].https://globalplatform.org/specs-library/.

作者简介：
王海涛，高级工程师，硕士，主要从事信息安全及智能卡相关技术工作；衣莉莉，高级工程师，硕士，主要从事智能卡技术管理工作；孙阳阳，工程师，学士，主要从智能卡研发及技术管理工作；刘觅，工程师，硕士，主要从事智能卡相关技术及应用研究工作。