JAVACARD SIM内存管理方法优化研究

Optimization Study on JAVACARD SIM Memory Management Method

黄健文，黄　健，蔡秋艳，杨　光（中国电信股份有限公司研究院，广州 510630）
Huang Jianwen，Huang Jian，Cai Qiuyan，Yang Guang（Research Institute of China Telecom Corporation Limited，Guangzhou 510630，China）

摘　要：
在移动通信网络中，SIM主要负责移动通信网络接入鉴权认证，并承载各种行业应用，当前SIM芯片物理内存资源有限，需提升SIM内存利用率从而加载更多行业应用。首先对SIM的内存架构进行分析，将物理内存分为固定内存和剩余待分配内存。其次明确了待分配内存中DTR和RTR内存的管理原则。最后结合应用的安装、删除等管理操作，阐述了待分配内存申请占用、释放回收、内存溢出等管理原则。通过对待分配内存优化管理可提升SIM物理内存利用率，加载并运行更多的行业应用。

关键词：
JAVACARD SIM；内存申请；内存释放；内存溢出；RTR；DTR
doi：10.12045/j.issn.1007-3043.2023.12.013
文章编号：1007-3043（2023）12-0063-04
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：
In the mobile communication network，SIM is mainly responsible for the authentication of mobile communication network access，and carrying various industrial applications. Currently，the physical memory resources of SIM chips are limited，so SIM memory utilization needs to be improved to load more industrial applications. Firstly，the memory architecture of SIM is analyzed，and the physical memory is divided into fixed memory and the remaining memory to be allocated. Secondly，the management principles of DTR and RTR memory in the pending allocated memory are defined. Finally，combined with the management operations of application installation and deletion，the management principles of memory request，release，recycle，and memory overflow are expounded. Memory allocation optimization management improves SIM physical memory utilization and can load and run more industry applications.

Keywords：
JAVACARD SIM；Memory request；Memory release；Memory overflow；RTR；DTR

引用格式：黄健文，黄健，蔡秋艳，等. JAVACARD SIM内存管理方法优化研究[J]. 邮电设计技术，2023（12）：63-66.

1 概述

随着移动通信技术从1G到5G持续演进，移动通信已渗透到人们生产生活的方方面面[1-2]。3G时代移动通信技术和互联网技术开始结合[3]，4G推动了移动互联网的高速发展[4]，出现了微信、支付宝等超级应用APP。5G通信技术带来了大带宽（eMBB）、大连接（mMTC）和低时延（uRLLC）等新应用场景，快速拉动大数据、人工智能、物联网和智能驾驶等一系列新业态[5]。6G开始进入空天一体化时代，将形成沉浸式云XR、全息通信、感官互联、数字孪生等八大业务应用。

在1G~3G时代，SIM的核心用途是移动网络接入认证，是使用NATIVE语言开发的单应用卡。在4G、5G时代，由于行业应用的快速推广和终端技术的快速进步，SIM芯片从ICC架构发展为UICC架构，采用JAVACARD与GP架构技术的多应用卡成为未来SIM的主流发展方向，SIM具备入网鉴权与应用加载双重核心用途。在5G、6G时代，电信运营商不仅向外提供移动通信数据管道服务，同时正力争成为全产业链综合服务商。电信运营商发挥SIM的天然安全属性向外

收稿日期：2023-11-28

输出安全服务能力，并借用SIM卡安全存储空间承载数字货币、数字身份、数字公交、市民卡等国家重要基础实施应用[6]。SIM RAM内存资源是行业应用开发、加载流程中不可或缺的重要元素，将决定行业应用在SIM内的运行效率及稳定性。为满足行业应用在SIM上最大程度的加载需求，本文后续将从SIM芯片、COS内存资源现状，国际规范内存资源管理要求，分析优化提升SIM内存资源利用率的方法。

2 SIM卡内存资源现状

2.1 国际标准现状

现有JAVACARD JCRE国际标准将SIM内存分为CLEAR_ON_RESET和CLEAR_ON_DESELECT 2类。CLEAR_ON_RESET简称RTR内存，用于存储应用的永久性状态，CLEAR_ON_DESELECT简称DTR内存，用于存储应用的临时性、过渡性状态。RTR内存在应用安装时候申请并占用，应用删除后释放回收为待分配的RTR，DTR在应用安装时申请，应用选择运行时候内存占用，应用去选择后释放回收为DTR内存。

2.2 芯片现状

当前国内运营商发行的JAVACARD SIM芯片主要以国产芯片为主，典型代表为华大电子CIU98M25、紫光国微THD89，芯片物理内存为40~44 KB。

2.3 现有SIM内存管理方法现状

现有SIM内存管理方法将待分配内存资源按一定比例预先固定划分为DTR和RTR内存，应用安装将在固定的DTR和RTR空间内进行申请分配，DTR和RTR内存类型不可混合使用。现有SIM内存管理方法，当应用实际DTR大于预先固定设置DTR时，应用被禁止安装，限制了应用DTR内存资源的使用。目前国内具备多应用SIM产品研发能力的主流卡商有东信和平、恒宝、华弘、握奇、天喻等，各个厂家研发的SIM商用产品可用于行业应用加载运行使用的待分配RAM剩余空间为15~18 KB。

3 JAVACARD SIM内存管理优化方法

3.1 SIM内存分配管理架构

本文遵循JAVACARD国际标准对DTR与RTR内存类型的管理原则：DTR内存在各个应用间可共享，应用去选择后进行内存释放；RTR内存类型分配即占用，不可在应用间共享，应用删除后则释放内存。

SIM卡芯片物理内存分为基础功能层内存和应用层内存。基础功能层内存是分配给基本通信能力、JAVACARD、GP管理架构使用的固定物理内存，在SIM卡开发过程中被固定分配，不可释放供后下载应用使用；应用层内存即SIM卡的剩余内存空间，只提供给应用下载使用。

应用层内存空间分为逻辑通道固定分配内存空间和当前待分配内存空间。固定分配内存空间标记为$N\times D_e$，N表示SIM支持的逻辑通道数量，D_e表示每个逻辑通道固定独立分配的DTR，每个逻辑通道间独立使用D_e字节DTR，不共享。当前待分配内存空间标记为M，可作为DTR和RTR使用，不预设置其内存类型，根据应用安装参数进行内存类型设置和内存数量分配。JAVACARD SIM内存分配管理架构如图1所示。

3.2 JAVACARD SIM内存管理原则

为便于JAVACARD SIM内存管理，根据GP国际标准，定义如下应用内存管理参数：C_7表示应用可使用最大RTR内存空间；D_7表示至少为应用固定预留的RTR内存空间；R表示应用安装实际使用的RTR空间；D表示应用安装实际使用的DTR空间。

JAVACARD SIM应用层$M+N\times D_e$内存空间，在应用安装、应用选择、应用删除等管理流程中，按如下原则进行内存申请释放管理。

a）当前待分配M字节内存空间管理原则，分配前不预设置DTR和RTR类型，根据内存分配请求进行

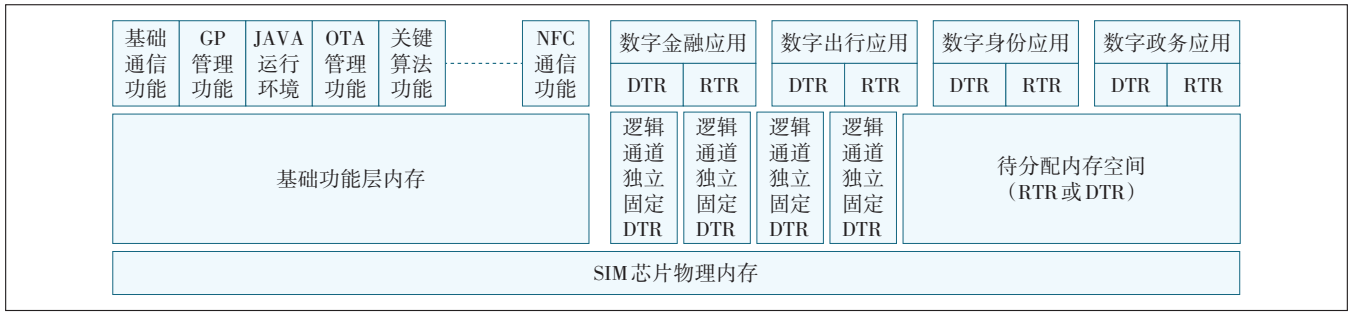

图1　JAVACARD SIM内存管理架构

DTR和RTR类型分配。RTR分配即被占用不可共享、应用删除后该应用占用的RTR释放，RTR分配后1∶1实际占用物理内存；DTR分配后可共享，应用去选择后该应用的DTR被释放，多段DTR内存可临时共享占用相同物理内存。

b）获取SIM当前剩余空间原则，SIM在应用安装前可使用GP指令获取SIM当前可使用的剩余内存空间，获取SIM当前可使用的RTR空间为M，获取当前SIM可使用DTR空间为D_c+M。

c）带C_7/D_7安装参数的应用安装内存申请管理原则，应用安装优先分配RTR内存，当($D_7\leqslant M$)&($D<M-D_7+D_c$)条件成立时，允许进行应用安装，否则应用安装失败。安装X个相同应用时，当($M\geqslant D_7\times X$)&($M+D_c-D_7\times X\geqslant D$)&($D_7\leqslant M$)，第$X$个应用允许安装成功，$X$为正整数。

d）不带C_7/D_7安装参数的应用安装内存申请管理原则，应用安装优先分配RTR内存，当($R<M$)&($D<M-R+D_c$)条件成立时，允许进行应用安装，否则应用安装失败。安装X个相同应用时，当($M\geqslant R\times X$)&($M+D_c-R\times X\geqslant D$)&($R\leqslant M$)，第$X$个应用允许安装成功，$X$为正整数。

e）应用调用API获取应用可使用的内存空间管理原则。当应用不带C_7/D_7参数时，应用可使用的内存空间为当前SIM待分配空间M，RTR为M，DTR为$M+D_c-D$。当应用带C_7/D_7参数时候，当$C_7-D_7>M$，应用可使用的RTR为M，当$C_7-D_7\leqslant M$时候，应用可使用的RTR为C_7-D_7；DTR为$M+D_c-D$。

f）带安装参数C_7/D_7的应用删除内存管理原则，删除前SIM当前待分配内存空间为M，删除后SIM当前待分配内存空间为D_7+M，删除后可使用的RTR为D_7+M，删除后可使用的DTR为D_7+M+D_c。

g）不带安装参数C_7/D_7的应用删除内存管理原则，删除前SIM当前待分配内存空间为M，删除后SIM当前待分配内存空间为$R+M$，删除后可使用的RTR为$R+M$，删除后可使用的DTR为$R+M+D_c$。

h）应用选择DTR内存溢出冲突管理原则，SIM卡支持n个逻辑通道同时打开n个应用，每次在逻辑通道选择应用应按如下规则进行内存溢出冲突判断：

（a）当SUM($D_1+D_2\cdots D_X$)>$M+X\times D_c$，$X\leqslant n$，DTR内存溢出，SIM应禁止当前在第X逻辑通道上选择D_X应用，需等待其余逻辑通道上的DTR内存释放后再进行选择。

（b）在支持X个逻辑通道的SIM上，不会产生内存溢出冲突的DTR最大平均值为$M/X+D_c$；当SIM卡全部安装只要求DTR的应用时，DTR≤$M/X+D_c$时，不会产生DTR内存溢出；当应用带RTR和DTR、且DTR≤D_c时，不会产生内存溢出冲突。

3.3 SIM内存分配管理实例

假设JAVACARD SIM应用层内存空间为16 KB，SIM支持4个逻辑通道，每个逻辑通道固定分配1 KB DTR共4×1 KB DTR，剩余12 KB为当前待分配内存空间，可根据需要作为DTR或RTR内存类型分配使用。

a）分别安装配置C_7/D_7参数的应用APP-A、APP-B后SIM内存状态如表1所示。APP-A应用：C_7=25，D_7=2，R=1，D=2。APP-B应用：C_7=10，D_7=2，R=1，D=2。API方式获取应用可用空间：C_7-D_7>M_AF，RTR_API=M_AF；$C_7-D_7\leqslant$M_AF，RTR_API=C_7-D_7。

b）分别安装不配置C_7/D_7参数的应用APP-C、APP-D、E、F后SIM内存状态如表2所示。APP-C应用：C_7=0，D_7=0，R=1，D=2。APP-D应用：C_7=0，D_7=0，R=0，D=2。

c）累计可安装APP-A的数量与内存溢出冲突实例如表3所示。应用APP-A：C_7=25，D_7=2，R=1，D=2；根据安装成功条件($M\geqslant D_7\times X$)&($M+D_c-D_7\times X\geqslant D$)&($D_7\leqslant M$)，即(12≥2$X$)&(12+1−2$X$≥2)，可得$X$最大为5，可安装5个APP-A应用，第6个应用安装失败。采用API方式获取应用可用空间：C_7-D_7>M_AF，RTR_API=M_AF；$C_7-D_7\leqslant$M_AF，RTR_API=C_7-D_7。DTR内存溢出计算：SUM($D_1+D_2+\cdots+D_X+D_X$)>$M+X\times D_c$，安装完第5个应用后当前待分配内存空间为2，2×X>2+1×X，当X>2时，产生DTR内存溢出，SIM卡只能在2个逻辑通道上同时选择2个应用，在第3个逻辑通道上打开第3个应用时DTR内存溢出，应禁止打开。

d）删除SIM卡内多个APP-A应用后，SIM内存状

表1　安装APP-A、APP-B应用后SIM剩余内存状态

应用类型	安装前SIM剩余内存空间/KB			安装后SIM剩余内存空间/KB			API方式获取的应用可用空间/KB	
	DTR=$M+D_c$	RTR=M	M	DTR_AF=$M-D_7+D_c$	RTR_AF=$M-D_7$	M_AF=$M-D_7$	DTR_API=M_AF+D_c-D	RTR_API
APP-A	13	12	12	11	10	10	9	25−2>10，RTR_API=10
APP-B	13	12	12	11	10	10	9	10−2<10，RTR_API=8

表2　安装APP-C、APP-D应用后SIM剩余内存状态

应用类型	安装前SIM剩余内存空间/KB			安装后SIM剩余内存空间/KB			API方式获取的应用可用空间/KB	
	DTR=$M+D_e$	RTR=M	M	DTR_AF=$M-R+D_e$	RTR_AF=$M-R$	M_AF=$M-R$	DTR_API=M_AF+D_e-D	RTR_API=M_AF
AAP-C	13	12	12	12	11	11	10	11
AAP-D	13	12	12	13	12	12	11	12

表3　累计安装多个APP-A应用SIM内存状态变化

应用类型	安装前SIM剩余内存空间/KB			应用安装后SIM剩余内存空间/KB			API方式获取的应用可用空间/KB	
	DTR=$M+D_e$	RTR=M	M	DTR_AF=$M-D_7+D_e$	RTR_AF=$M-D_7$	M_AF=$M-D_7$	DTR_API=M_AF+D_e-D	RTR_API
APP-A1	13	12	12	11	10	10	9	25-2>10，RTR_API=10
APP-A2	11	10	10	9	8	8	7	25-2>8，RTR_API=8
APP-A3	9	8	8	7	6	6	5	25-2>8，RTR_API=6
APP-A4	7	6	6	5	4	4	5	25-2>8，RTR_API=4
APP-A5	5	4	4	3	2	2	1	25-2>8，RTR_API=2
APP-A6	3	2	2	1<2	0	0	安装失败	APP-A1

态变化如表4所示，应用APP-A：C_7=25，D_7=2，R=1，D=2；初始条件：SIM已安装5个APP-A；当前SIM待分配内存空间为2。

表4　删除APP-A应用SIM内存状态

应用类型	应用删除前SIM待分配空间/KB			应用删除后SIM待分配空间/KB		
	DTR =$M+D_e$	RTR =M	M	DTR_AF =$M+D_7+D_e$	RTR_AF =$M+D_7$	M_AF =$M+D_7$
APP-A1	3	2	2	5	4	4
APP-A2	5	4	4	7	6	6
APP-A3	7	6	6	9	8	8
APP-A4	9	8	8	11	10	10
APP-A5	11	10	10	13	12	12

4 总结

本文在JAVACARD国际标准RTR和DTR内存类型管理原则基础上，对SIM应用层待分配内存空间进行优化管理，对待分配内存空间不预设置分配内存类型，待分配空间可作为RTR和DTR混合使用，应用删除后释放回收的内存空间可作为RTR和DTR混合使用。本文结合应用安装、应用选择、应用删除等流程，定义了SIM应用层内存空间管理原则、RTR和DTR内存类型管理原则、应用安装内存申请管理规则、应用删除内存回收管理原则、应用选择内存溢出冲突管理原则和应用开发安装内存类型推荐原则。本文定义的内存管理方法具有如下优点：可指导SIM卡外实体在应用开发阶段尽可能使用DTR内存类型，少使用或者不使用RTR内存类型，当全部安装只使用DTR内存类型应用时，DTR≤M/N+D_e时，可安装无数个应用，且不产生内存溢出冲突；待分配内存空间不预设置内存类型，可广泛应用于各种应用类型的安装，避免传统方法由于DTR>D_e时应用无法安装的风险，本文可安装的应用DTR最大值为M+D_e；指导SIM应用管理平台合理使用D_7参数，应尽可能不用D_7安装参数，避免过度占用RTR内存、造成内存资源浪费；应用删除释放的RTR内存，可回收作为DTR或RTR使用，提升了内存回收管理的灵活性，有利于后续应用的安装使用。遵循本文定义的内存管理原则，可最大程度提升SIM物理内存利用率，装载更多行业应用。

参考文献：

[1] 罗林. 移动通信网络优化现状及发展趋势[J]. 电子世界，2022(1)：156-157，159.
[2] 刘家祥，彭硕，蒋峥，等. 空天地一体化网络运营方法分析与挑战[J]. 移动通信，2022，46(9)：45-50.
[3] 罗拥华. 3G时代移动互联网发展分析[J]. 山东工业技术，2015(11)：148-149.
[4] 孙梦真. 4G时代移动互联网的发展趋势[J]. 数字技术与应用，2019，37(10)：208-209.
[5] 宫学源. 移动通信用半导体技术发展趋势浅析[J]. 新材料产业，2021(6)：38-40.
[6] 范建伟. 基于SIM卡的数字身份实现与应用[J]. 科学技术创新，2022(35)：91-94.

作者简介：
黄健文，毕业于武汉大学，工程师，学士，主要从事通信智能卡安全技术研究与SIM行业应用开发工作；黄健，毕业于广东工业大学，工程师，硕士，主要从事通信智能卡安全技术研究与SIM行业应用开发工作；蔡秋艳，毕业于北京邮电大学，工程师，硕士，主要从事通信智能卡研究测试工作。杨光，毕业于北京邮电大学，工程师，学士，主要从事通信智能卡研究测试工作。