芯昇科技
XinSheng Tech

全球首款RISC-V超级SIM芯片的技术创新与应用

Innovative Technology and Applications of the World's First RISC-V Super SIM Chip

2024 年 8 月 August 2024

杭州 Hangzhou

目录

contents

公司简介

芯昇科技有限公司

依据中国移动“科改示范行动”整体改革布局，中移物联网分拆发展空间和市场竞争力较强的业务设立独立子公司，积极探索以资本为纽带的管控方式。2020年12月29日，芯昇科技有限公司在南京江北新区注册成立，并于2021年7月独立运营，于2024年5月28日注册地**迁址雄安新区**。作为中国移动旗下专业芯片公司，中移芯昇科技围绕物联网芯片优化升级，以促进国家集成电路产业振兴为目标，以“创芯驱动万物互联，加速社会数智化转型”为使命， 基于RISC-V开展技术攻关，致力于成为“最具创新力的物联网芯片及应用领航者”。

使命　创芯驱动万物互联　加速社会数智化转型

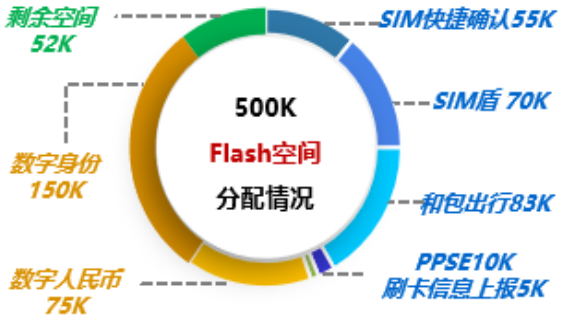
愿景　成为最具创新力的物联网芯片及应用领航者

1.1 超级SIM卡介绍

1.1 超级SIM卡介绍

- 超级SIM发展至今，已建立完整产业链，涵盖安全芯片、卡操作系统、SIM卡、终端、平台、应用等。
- 当前，超级SIM芯片面临核心技术封闭化、存储受限、传输速率及主频性能瓶颈等挑战，中国移动聚焦SIM卡代际升级，致力于国家信息基础设施建设，助力数字中国发展。

核心技术封闭化	缺少开源内核，技术迭代优化升级缓慢
存储受限	FLASH应用总空间500KB，仅剩余52KB无法支持OS安全升级
传输瓶颈	通信速率<0.3Mbps，传输照片、证照文件耗时较长
性能瓶颈	主频<40MHz，无法满足数字人民币等应用的高速计算需求



1.2 RISC-V超级SIM芯片优势

- 以解决当前产品技术卡点、痛点为目的，围绕RISC-V安全内核、RISC-V自定义扩展指令、大容量、高性能、高安全性、多接口等关键技术进行攻关，补齐大容量安全芯片在”存储--运算--传输”的短板，突破超级SIM芯片的技术瓶颈。

开源RISC-V
- 32位RISC-V安全内核
- 扩展指令集

大存储
- 2.5MB FLASH容量
- 多应用存储

多接口
- 支持多个接口，拓展物联网领域：7816/SWP/QSPI/SPI/I2C/UART

高安全
- 加密存储；
- 国际、国密算法及安全认证
- PUF

高性能
- CPU:120MHz
- 高速接口
- 算法性能、算力提升

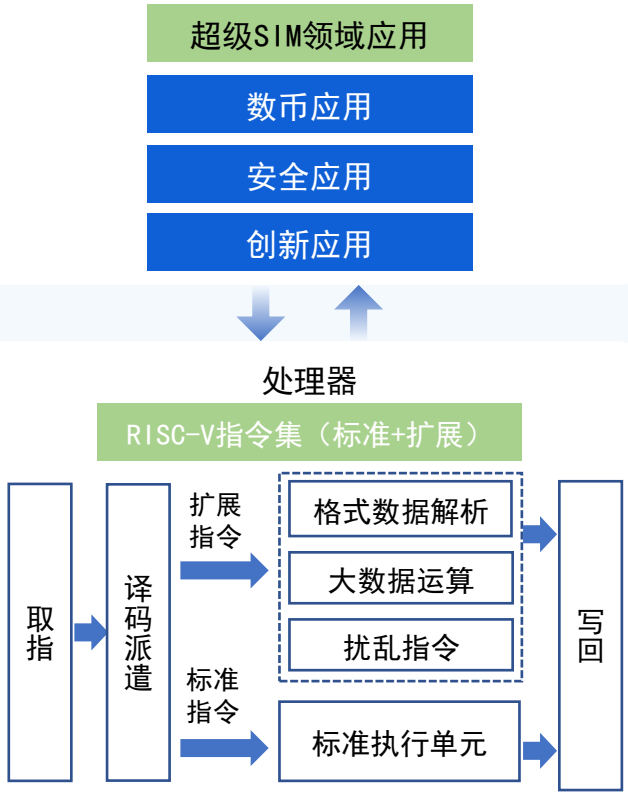
易拓展
- 产业延伸属性：SIM+繁荣

1.2 芯片优势（1/6）：开源高性能RISC-V内核

- 采用40nm先进工艺，国内首款首创应用于超级SIM芯片的高性能RISC-V安全内核，加速开源RISC-V应用生态。
- 基于RISC-V指令集灵活可扩展的独特优势，应用下沉至芯片底层，解决数币应用中交易时间较长等性能问题。

开源RISC-V内核

- 支持多级存储安全保护
- 高主频（120MHz）、内置16KB指令Cache
- DMA模块提升数据搬运性能
- 创新RISC-V自定义指令能力，大幅提升安全性或专用场景性能



1.2 芯片优势（2/6）：大存储

- 片上存储容量比现网超级SIM卡产品增加一倍，利于多行业应用存储及推广，应用装载数量提升4倍。
- 通过SPI/QSPI接口扩展片外Flash达到更大扩容能力。

大 容 量

2.5M字节
Flash存储器

72K字节
SRAM

64K字节
ROM

提供1.2M+字节用户空间

安装50+
超级SIM应用

1.2 芯片优势（3/6）：多接口

- 支持多接口，拓展物联网领域：7816/SWP/QSPI/SPI/I2C/UART。
- QSPI： 支持两路QSPI，支持20MHz时钟，针对外接扩展存储器进行读写数据时支持硬件级实时加解密，有效保证外接存储器中的数据安全。

1.2 芯片优势（4/6）：高安全

- 高安全的芯片系统级架构设计，全芯片超过100项安全性设计，在保障安全性的同时兼顾系统性能。

高安全

安全特性

安全内核，访问控制

安全传感器，加密存储；

算法

支持国际、国密算法：

支持SM9算法，RSA最高支持4096bit；

PUF（物理防克隆）能力

不可复制、不可预测、上电产生和掉电消失等特性的芯片物理“指纹”。

安全认证

EAL5+

银联卡芯片安全

国密二级

1.2 芯片优势（5/6）：高性能

- 支持多总线（数据总线、指令总线和系统总线），提升系统性能。系统整体可运行在120MHz主频以上。
- SIM卡通用接口7816传输速率最高提升10倍+，扩展了高速QSPI接口用于传输大数据。
- DMIPS算力提升一倍，算法性能大幅提升。

高性能

高性能芯片系统设计	• 多层总线架构设计，多接口系统设计，多存储器架构设计
CPU	• 高主频（120MHz），主频提升了**3倍+**
高速传输	• 7816：2.5M bps，通信速录提升了**10倍+**
算力	• 150+DMIPS，算力**翻一番**
算法性能	• 比现网超级SIM卡平均提升**2倍+** • 比《中国移动新一代超级SIM芯片技术要求白皮书》提升**30%+**

1.2 芯片优势（6/6）：易拓展

- SIM+生态繁荣：基于SIM高安全属性作为可信平台，通过多元接口扩展其他能力，，共同形成SIM+生态繁荣。

+蓝牙

蓝牙卡，打通苹果手机封闭环境，增加蓝牙传输能力

+定位芯片

高精度定位，实现RTCM原始观察量+差分数据一体化处理

+基带芯片

设备集成度更高，小型化

+NVM存储

扩展存储区域，借助安全能力实现加密保险箱

+指纹

增加生物特征属性

+X

基于SIM的特性扩展更多能力

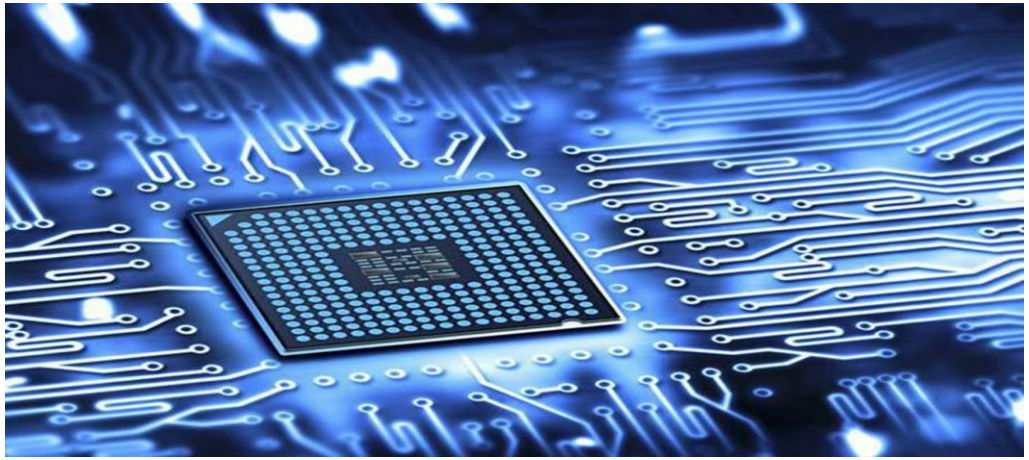
物联网开放平台

1.3 技术创新与突破(1/5):芯片与操作系统软硬结合，全面提升计算存储、通信、安全性能

- **芯片：**高性能、大容量、高速率、高安全、可扩展
- **操作系统：**混合架构、多语言、多线程、并行通信，支持OS更新

芯片

- **计算**：系统整体可运行在120MHz主频以上，主频提升**3倍+**，采用RISC-V内核
- **存储**：扩充容量，片上存储+片外Flash**10倍+**
- **通信**：7816传输速率提升**10倍+，**扩展了高速QSPI接口用于传输大数据
- **安全**：采用**物理防克隆PUF**技术，全芯片100项以上的安全性设计，可达到**EAL5+**高安全等级认证

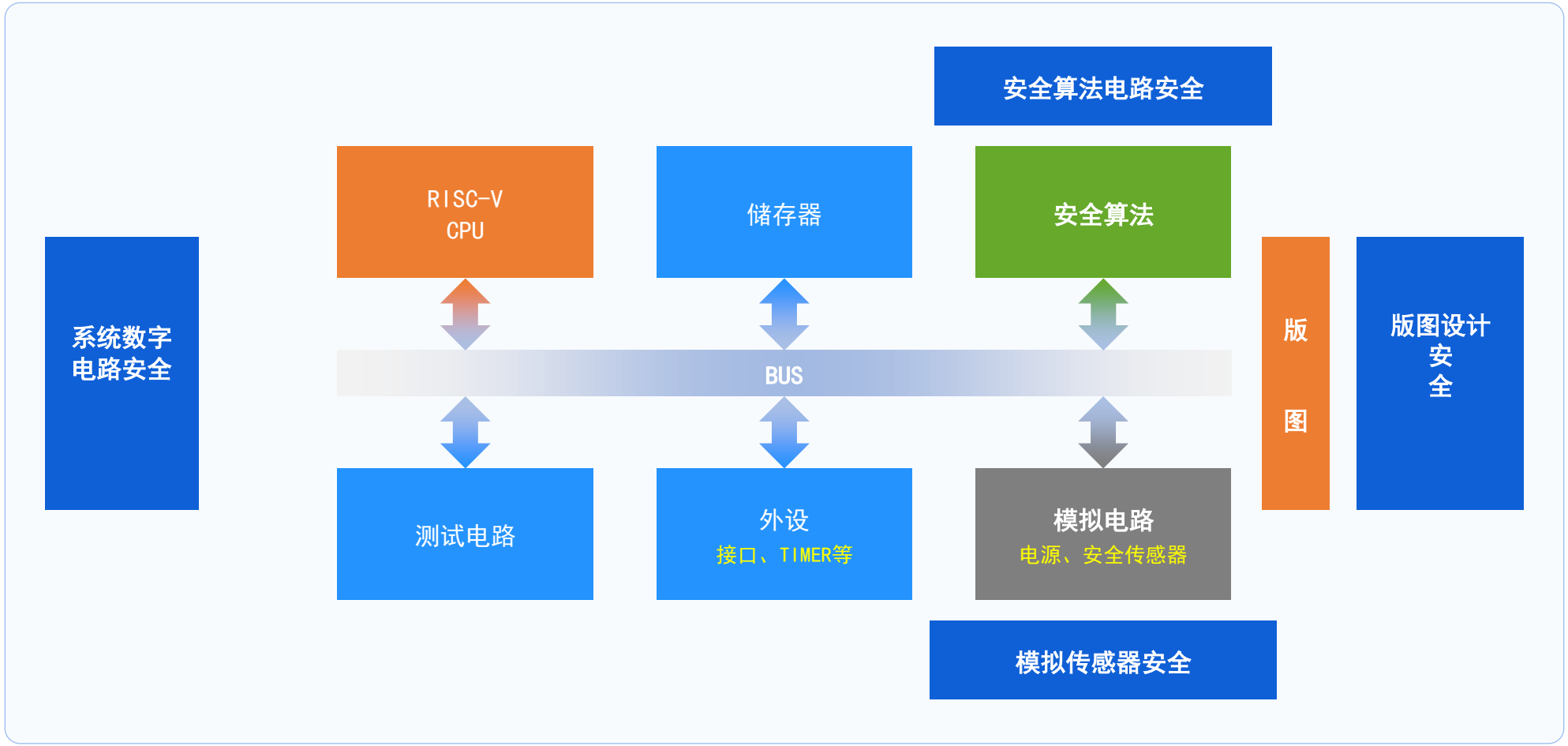


操作系统

- **创新**：自研Native多应用内核与**虚拟机**，采用Native+VM混合架构，兼顾运行效率与硬件兼容性，支持C++及Java多语言开发
- **高性能**：支持**多线程**、多事务操作，支持64位整型、浮点计算，支持字符串及多维数组
- **高速率**：支持高速7816接口（2.5Mbps），支持多逻辑通道**并行通信**，避免通信阻塞
- **可更新**：支持OS远程升级，支持**差分升级**实现快速更新。

1.3 技术创新与突破(2/5)：芯片整体安全性增强，技术水平达到国内领先水平

- 安全芯片采用了处理器指令执行时间均衡技术、存储器和总线加密和校验技术、测试模式硬Fuse保护技术、算法防DPA攻击技术、敏感信号隐藏技术等，做到CPU内核、总线数据传输、存储器保护、算法硬件实现、测试模式保护、模拟sensor功能和版图安全方面整体防护。



1.3 技术创新与突破(3/5):RISC-V专用指令能力，大幅提升专用场景性能

- 基于RISC-V指令集灵活可扩展的独特优势，从应用使用场景出发，提炼加速算法，针对应用效率、应用编写便利性及安全加固等多方面设计自定义专用指令，解决数币应用中交易时间较长、代码占用资源较大的问题。

扩展自定义指令集流程

- 应用场景 → 数币、安全、创新应用
- 性能需求 → 根据应用分析具体需求
- 提炼加速算法 → 提炼底层加速算子
- 定义专用指令 → 根据RISC-V规范，定义专用指令编码

应用分析

针对安全加固，增加混淆指令，进而增加应用代码反向分析难度，提升嵌入式软件安全，增加反编译破解难度，保护核心应用不被攻击泄露。

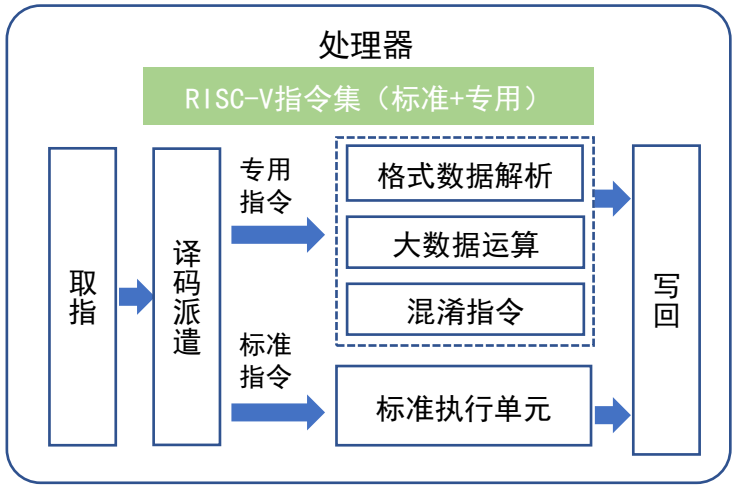
针对格式数据解析、大数据运算（频繁使用或字节长度受限等）能力进行扩展：通过扩展数据查找指令能够快速完成证书解析，使得应用格式数据查找的性能提升20%。

针对于运行在RISC-V上的操作系统进行分析，提炼需要加速的操作，以实现通过私有指令方式提升运行性能。

硬件实现

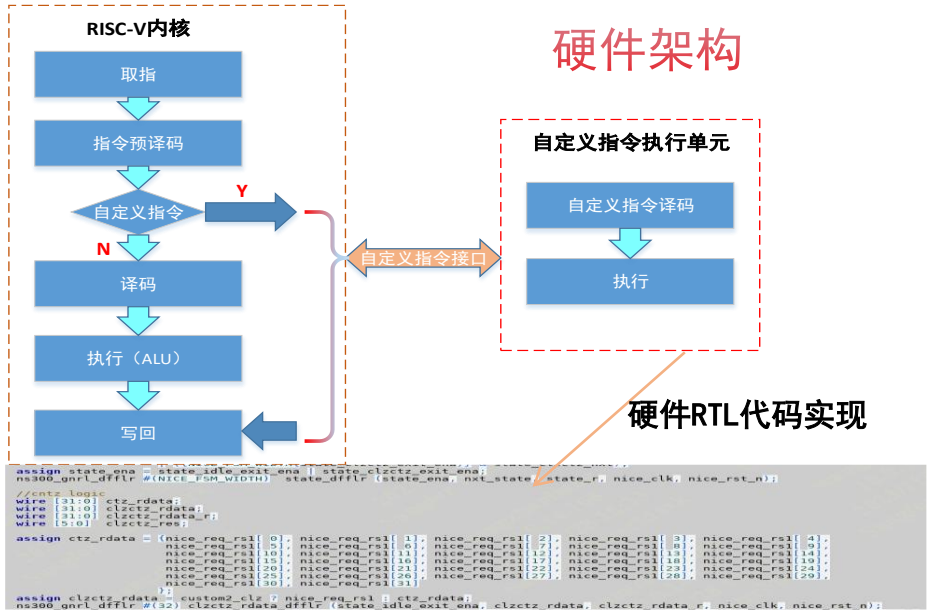
- 根据定义的专用指令，实现指令功能模块。
- 将完成的功能模块，通过RISC-V专用指令接口集成该功能。
- 通过软件编译调用专用指令，验证加速性能。

迭代验证



1.3 技术创新与突破(4/5):创新RISC-V自定义专用指令能力

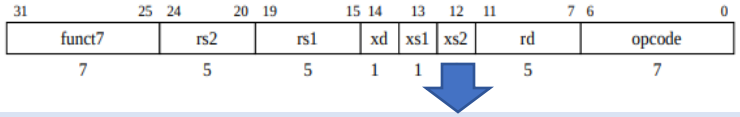
- 利用RISC-V内核的自定义指令接口实现专用指令功能，通过指令定义、硬件代码设计实现、编译器汇编嵌入等技术研究攻关，打通软硬件协同的开发路径，赋予应用下沉至芯片处理器指令集底层硬件的接口能力，实现应用执行效率提升。
- 实现按位计算”0”个数指令，加速OS任务调度性能。软件方案最大运行198个时钟周期，专用指令方案固定2个时钟周期完成指令执行。



指令	功能	编码
CUSTOM_CLZ	高位计算0个数	{0000000, 0, rs1, 110, rd, 1011011}
CUSTOM_CTZ	低位计算0个数	{0000001, 0, rs1, 110, rd, 1011011}

方案	说明	运行CPU时钟数
软件实现	循环遍历	6+6*（1~32）即12~198
扩展专用指令	采用CLZ、CTZ指令	2

指令定义



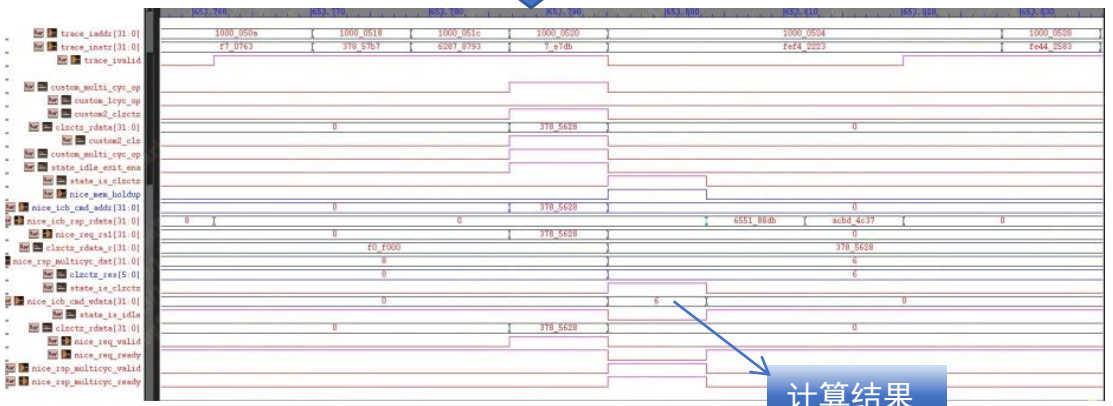
编译插入

```
asm volatile (
".insn r 0x5b, 6, 0, %0, %1, x0"
:"=r"(clz)
:"r"(0x03785628)      //对固定数据0x03785628进行计算，结果存到变量clz
);
```

汇编代码

```
asm volatile (
10000518:       037857b7                lui     a5,0x3785
1000051c:       62878793                addi    a5,a5,1576 # 3785628 <init.c.95ffd96f+0x37834d1>
10000520:       0007e7db                0x7e7db
10000524:       fef42223                sw      a5,-28(s0)
        ".insn r 0x5b, 6, 0, %0, %1, x0"
        : "=r"(temp)
        : "r"(0x03785628)
    );
```

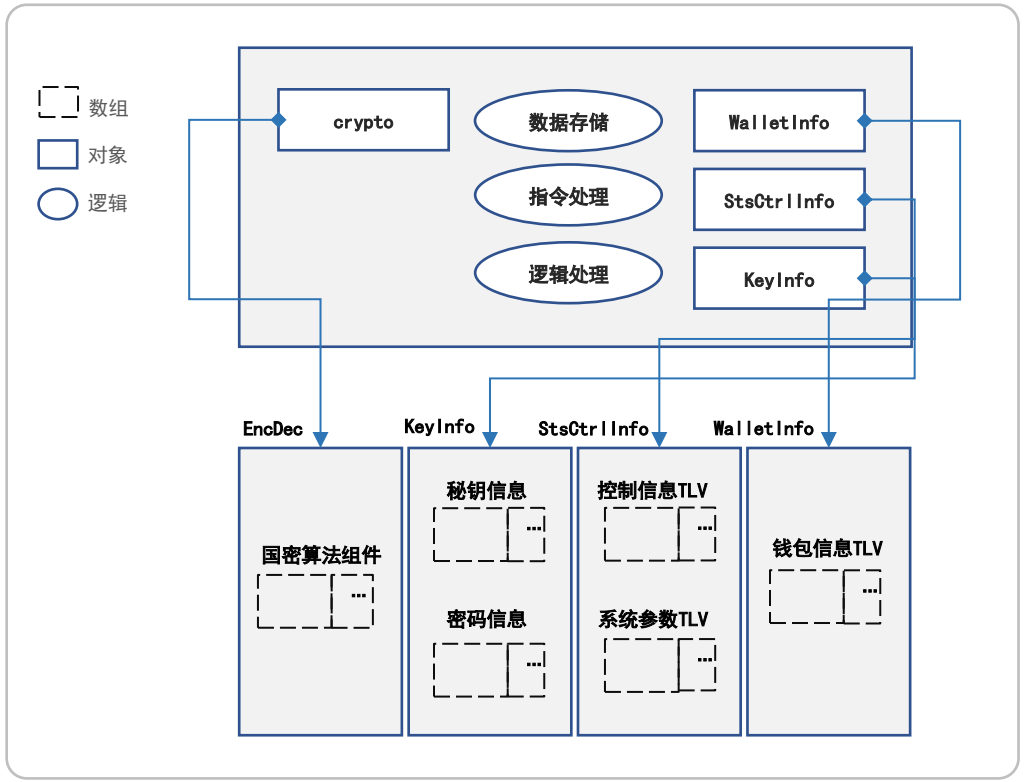
仿真波形



1.3 技术创新与突破(5/5):数字人民币应用设计方案

- 基于超级SIM的技术框架、自定义操作系统API标准，完成数字人民币卡应用的方案设计，达到数研所硬件钱包产品检测要求；
- 性能：识别应用中高频使用的证书解析、数据查找、多字节大数运算等场景结合芯片硬件能力进行设计，确保单离线付款平均执行时间<55ms。

应用架构



■ 遵循中国人民银行数字货币研究所发布的账户模式硬件钱包相关规范

实现差异举例

	原方案	新方案
数据存储	仅可用byte数组存储多字节数据，例如：6字节钱包金额 byte[] balance = new byte[6];	直接用int数据类型表示多字节数据，例如： 6字节钱包金额 int balance;
逻辑处理	判断钱包余额（6字节）是否充足的处理方式： 循环比较支付金额和钱包余额每字节大小，直到比较结束	调用大数运算：钱包余额直接减去支付金额
指令处理	个人化指令数据中，TLV控制信息处理： 循环判断每个TAG标签，并根据length长度读取具体标签值	直接调用COS底层实现的数据解析TLV处理方法

目录

contents

2.1 应用场景(1/2)

- 身份证、手机、钥匙、钱包必不可少的出门“四件套”在数字时代已经可以被一张超级SIM卡代替，能力覆盖“身手钥钱“便捷智慧出行。

身 份 证

基于SIM安全载体已实现网络ID身份，逐步趋向法定身份数字化

手 机

在SIM卡内使用量子会话密钥完成语音数据加解密，一次一密保护用户隐私

钥 匙

利用超级SIM卡NFC能力替代传统车钥匙，实现刷手机打开车门、启动车辆等功能

钱 包

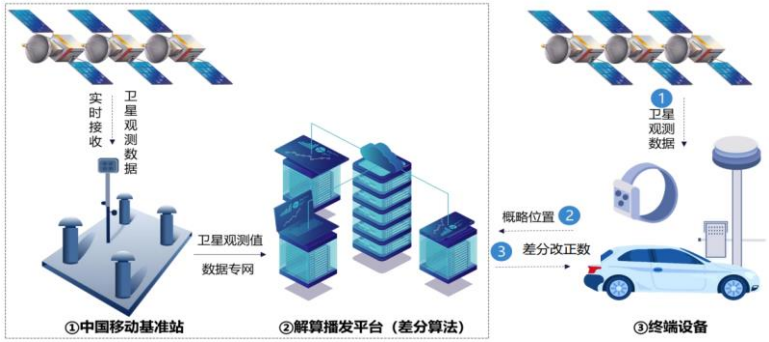
SIM卡硬钱包支持无网无电支付，23年7月在数币APP上线实现金融与通信跨界成果落地

2.2 应用场景(2/2)

- 超级SIM卡作为高安全智能基座，在卫星导航、金融、校园、物联网等多领域拓展构建丰富应用场景。
- 不断拓展新型应用：如基于超级SIM卡的安全芯片和密钥存储能力，打造量子超级SIM卡；可依托于号、卡、消息、通话、用户行为大数据开展反诈治理，联动公安/金融/互联网行业预警数据，赋能全行业环节治理，构筑全流程反诈防线。

高精度定位

利用差分信息实现厘米级定位精度



SIM盾安全应用

手机卡内激活金融CA证书，替代银行U盾

校园一卡通

校园消费、认证、水电、教学服务、自助服务等

超级物联网卡

应用在电子学生证上的超级物联网卡

2.2 应用解决方案（1/4）——超级SIM应用示范总体规划（1+2+N）

- 基于RISC-V超级SIM承载数字人民币、数字身份两大国家级基础设施，覆盖雄安新区全域个人用户和企业商户，推动雄安新区重点领域数字化转型，构建安全、便捷、高效的数字生态系统。
- 智慧通行解决方案是一个以数字身份底座为基础，超卡为载体，人工智能技术为核心的通用方案，旨在满足客户各场所出入管控的需求，可为园区、校园垂直行业提供通用能力，打造完整通行方案。

1个安全载体

RISC-V超级SIM卡

+

2个基础设施

数字人民币

数字身份

+

N个应用场景

01 超级SIM硬钱包 - 小微商户

02 超级SIM公交 - 和包出行

03 超级SIM数字身份 - 住房门锁

04 超级SIM数字身份 - 门禁通行

学生卡　　景区通行　　马拉松　　· · ·

2.2 应用解决方案（2/4）——超级SIM数字人民币-小微商户

- 数字货币——中国移动协同数字人民币运营机构打造SIM卡硬钱包SIM PAY产品，将数字人民币与具有广泛普及性和金融级别安全性的超级SIM卡的创新融合，基于央行账户模式新规范，支持单离线交易。

- 用户开通数字人民币SIM硬钱包；
- 使用NFC能力，“碰一碰”码牌或者POS机的NFC感应区完成付款；
- 商户开通数字人民币账户；
- 商户申领标签码牌或使用工行发放的pos机；

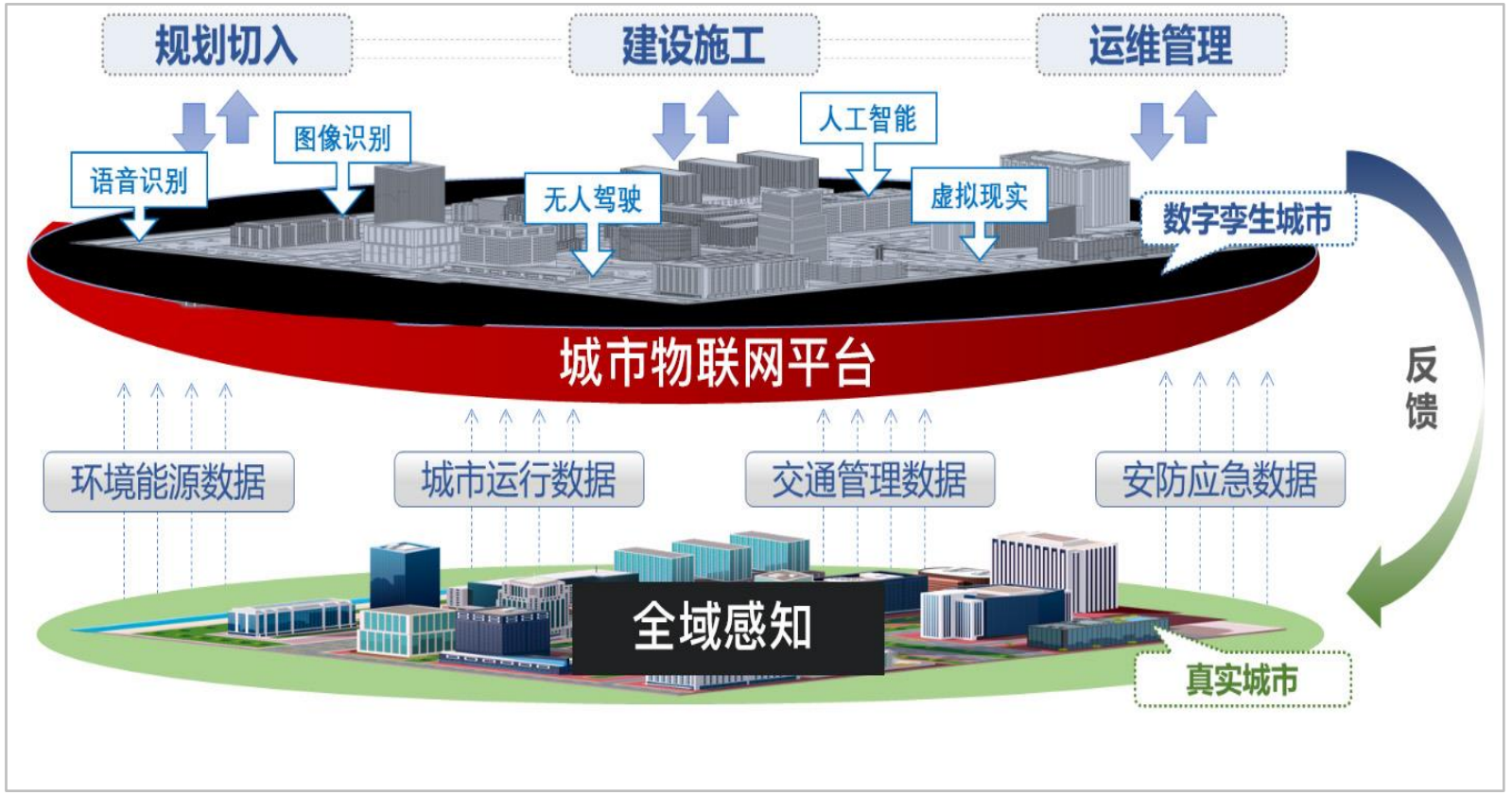
2.2 应用解决方案（3/4）——超级SIM数字身份-住房门锁

- 数字身份——中国移动联合公安部第一研究所研发SIM数字身份系统，通过在超级SIM卡中加载由CTID平台签发数字网证，实现公民隐私保护、认证留痕和数据可追溯的身份认证服务，利用超级SIM卡加载住房门锁，实现门禁权限在线开通，手机一碰即可开门。

2.2 应用解决方案（4/4）——构建创新高地，打造雄安智能感知未来之城

- 全域：依托雄安新区全域感知、空天地一体、网联汽车、智算中心等智能基础设施建设，建设“RISC-V之城”；
- 纵深：发挥中国移动市场规模优势，打造能源表计、超级SIM、智慧家庭等千万级应用场景。

全域：雄安建设“RISC-V之城”



构建雄安新区物联资源一张图，实现物联设备的“全域感知”，确保物联数据实时汇聚共享，实现物联服务能力“即插即用”

RISC-V生态建设

2024年4月，RISC-V工委会、芯昇科技、奕斯伟计算作为首批发起单位，联合成立雄安新区未来芯片创新研究院。

纵深：中国移动打造至少三个千万级应用场景

能源表计

超级SIM

智慧家庭

锚定RISC-V技术路线

Anchoring the RISC-V Technology Pathway

转化RISC-V攻关成果

Transforming RISC-V Research Breakthroughs into Achievements

繁荣RISC-V生态产业

Prospering the RISC-V Ecosystem Industry