国产X86方案夯实嵌入式/工控安全

薛刚汝

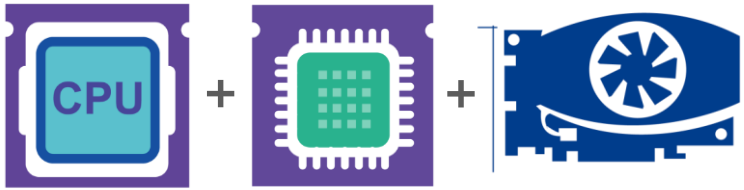
上海兆芯集成电路有限公司

兆芯

目录

上海兆芯

国内技术领先的IC设计公司



兆芯是国内唯一掌握
中央处理器+芯片组+图形处理器三大核心技术的公司

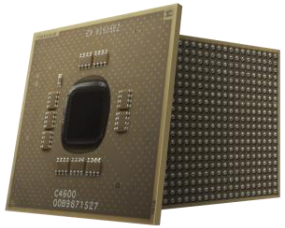
产业化能力强，服务专业、高效。

- 国内唯一同时具有“x86 & ARM SoC”芯片设计能力的公司
- GPU芯片设计能力国内领先，可比肩国际一流水准

兆芯产品

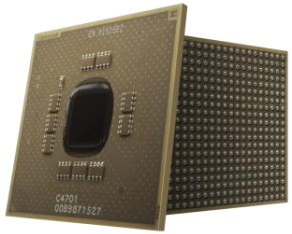
开先®

ZX-C 系列处理器



开先®

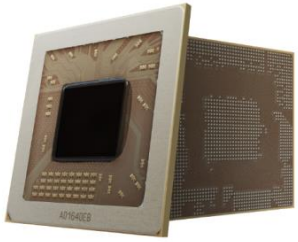
ZX-C+ 系列4核处理器



ZX-100S芯片组

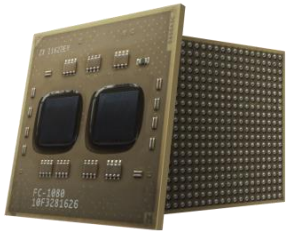
开先®

ZX-D 系列处理器



开胜®

ZX-C+ 系列8核处理器



ZX-200 IOE芯片

完善的产业链生态系统


操作系统
神州网信
deepin 深度科技
中科方德
工艺
华力微电子
BIOS
BYOSOFT
中电科技
应用软件
整机厂商
Lenovo
INESA
SUPERCLOUD
清华同方
集成商
东华软件
Neusoft东软
TAIJI 太极
合作伙伴

应用领域

兆芯 + 嵌入式\工控

地铁闸机

充值机

发电工控机

机上娱乐系统

医疗设备

启明星辰

Hillstone 山石网科

天融信 TOPSEC

研祥智能股份 EVOC INTELLIGENT TECHNOLOGY

INESA NETWORK 仪电智通

众新科技

XIK embedded

CASWELL Complete Your Solution 北京瑞祺电通科技有限公司

SANGFOR 深信服科技

ADVANTECH 研華科技

中力恒兴

LS PLATFORM 立华科技

JWIPC

NEXCOM The Intelligent Systems

兆芯解决方案特点

X86全兼容

- ✓ 兼容Windows及国产操作系统
- ✓ 软件无缝切换，最快实现办公应用迁移
- ✓ 兼容上亿种软件及上千种外设

安全可控

- ✓ 处理器微架构由上海及北京团队独立设计研发
- ✓ 处理器、芯片组、图形处理器完全自主研发，全部环节透明可控

产品稳定、可靠

- ✓ 温度循环测试
- ✓ 热冲击测试
- ✓ 高温存储
- ✓ 压力测试
- ✓ 保证整机无故障运行大于10W小时

产业化能力强

- ✓ 兆芯供货品质良率可达99.8%以上
- ✓ 量产经验丰富，能根据客户需求，提供满足质量标准的芯片数量
- ✓ 服务专业、高效：在北京、上海、深圳设有专业的FAE服务团队

兆芯CPU“安全可控”

- 目前掌握着CPU，GPU和芯片组三大核心芯片共计480万行研发代
- 掌握全部研发环节
- 不存在“不明确”、“高特权”的功能模块
- 不存在“秘密”指令
- 微码补丁机制能快速地、及时地修补CPU的漏洞，减少被攻击的机
- 微码补丁机制由高强度加密技术来保证防篡改和防泄漏

安全“身份”


TCG“贡献级”成员
全国信息安全标准化技术委员会成员单位
可信云社区成员
安全身份
网络安全产业联盟成员单位
商用密码产品生产单位
可信计算产业联盟成员单位

兆芯CPU的硬件安全功能

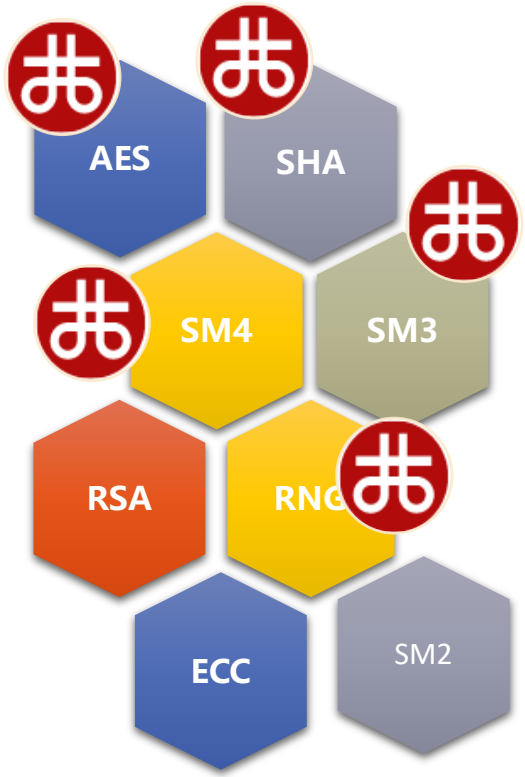
密码加速指令

安全启动技术

可信计算技术

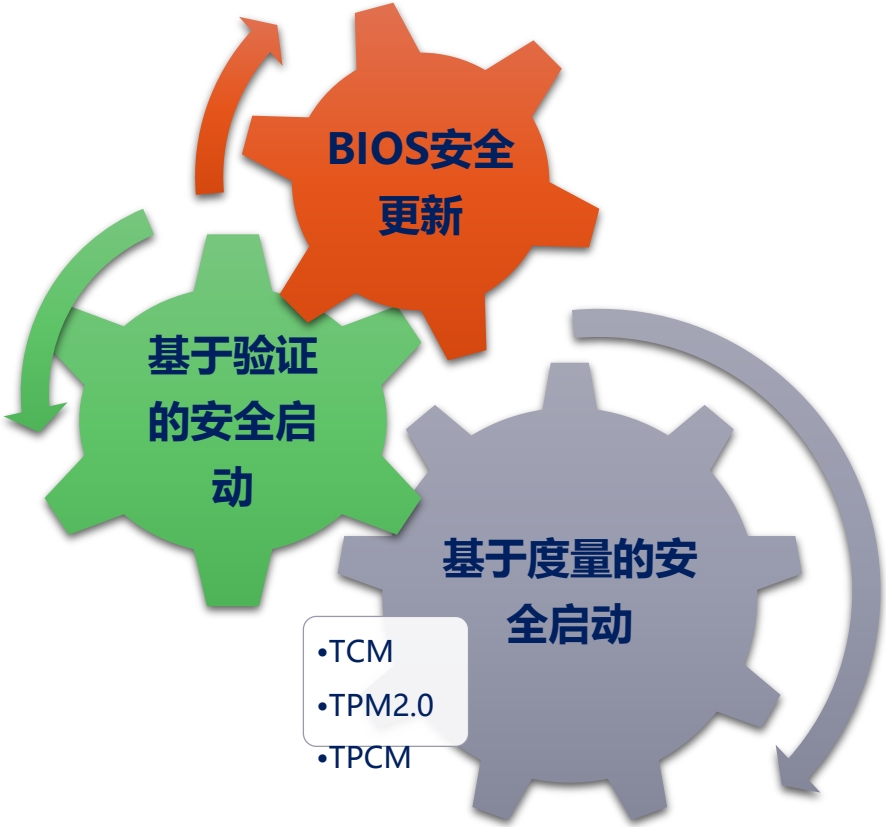
虚拟化安全

硬件安全功能——密码加速指令



- **指令名称**
  - GMI
  - AESNI, SHA Extension
  - Padlock
- **优势**
  - 便于使用
  - 性能提升
  - 算法“防篡改”
  - 计算过程”防泄漏”
- **兆芯国密算法支持**
  https://github.com/ZXOpenSource/OpenSSL-ZX-GMI
- **应用场景**
  - 数据加密存储
  - 数据加密传输
  - 应用数据加密

硬件安全功能——安全启动技术



- 硬件支持
- 与国产BIOS厂商合作
- 符合国内外相关标准的要求

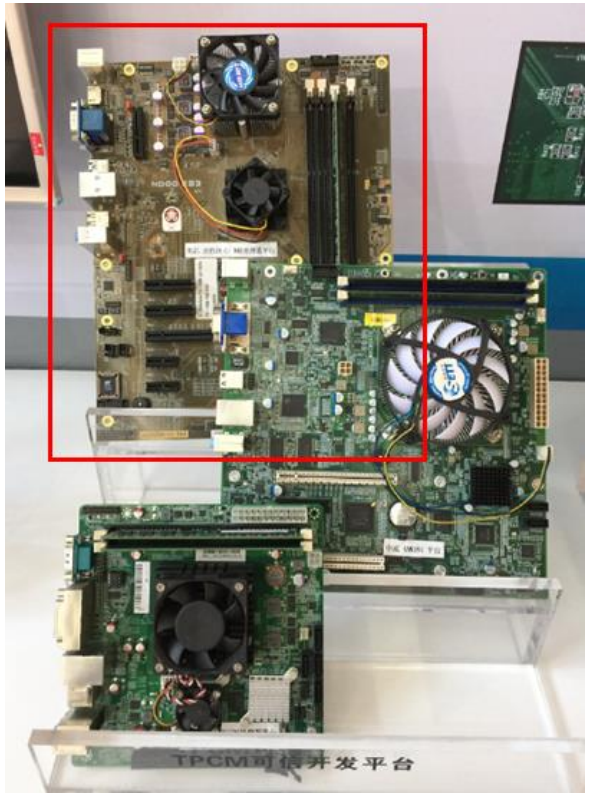
硬件安全功能——可信计算技术

基于TPCM的可信计算方案

兆芯可信计算技术（ZX-TCT）

基于TPCM的可信计算方案

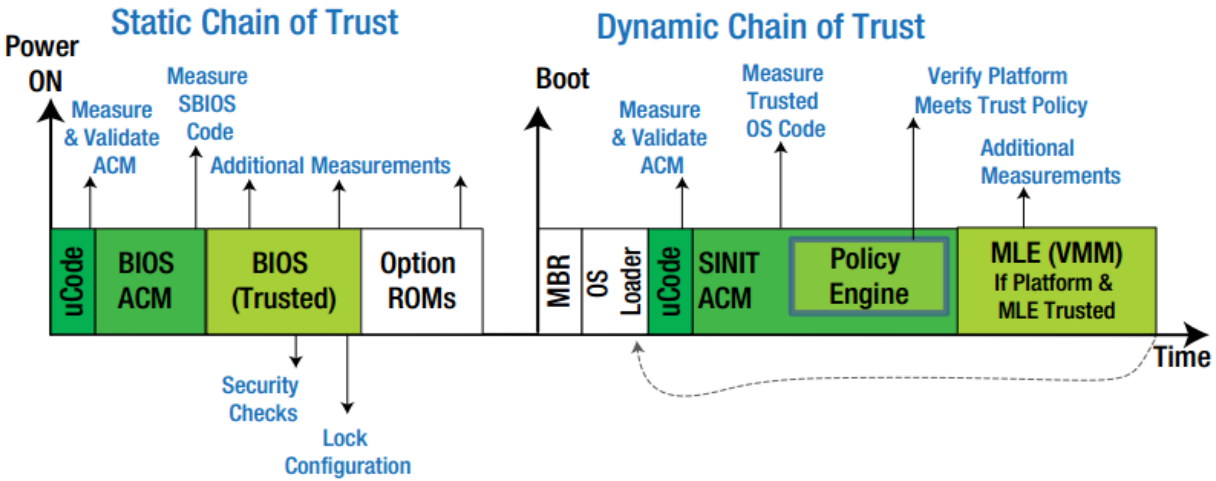
- **与华大半导体合作开发**
- **兆芯CPU+兆芯chipset+华大TPCM卡**
- **实现：**
  - 上电顺序控制
  - BIOS主动度量
  - 可信操作系统度量
- **未来计划**
  - 可信平台度量
  - 物理端口可信监管
  - 物理内存主动度量防护



硬件安全功能——可信计算技术（ZX-TCT）

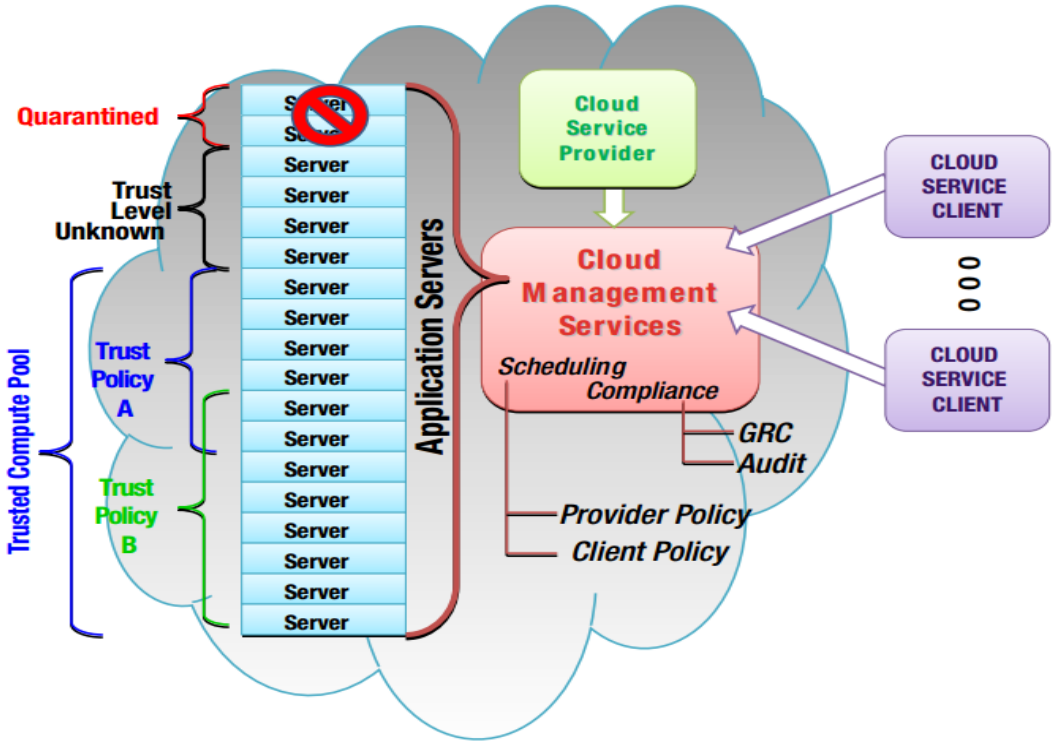
- 兼容Intel TXT（Trusted eXecution Technology）
- 构建系统启动时基于CPU的静态信任链
- 构建系统运行时基于CPU的动态信任链
- 可用于构建可信计算池，实现可信云计算

硬件安全功能——可信计算技术（ZX-TCT）



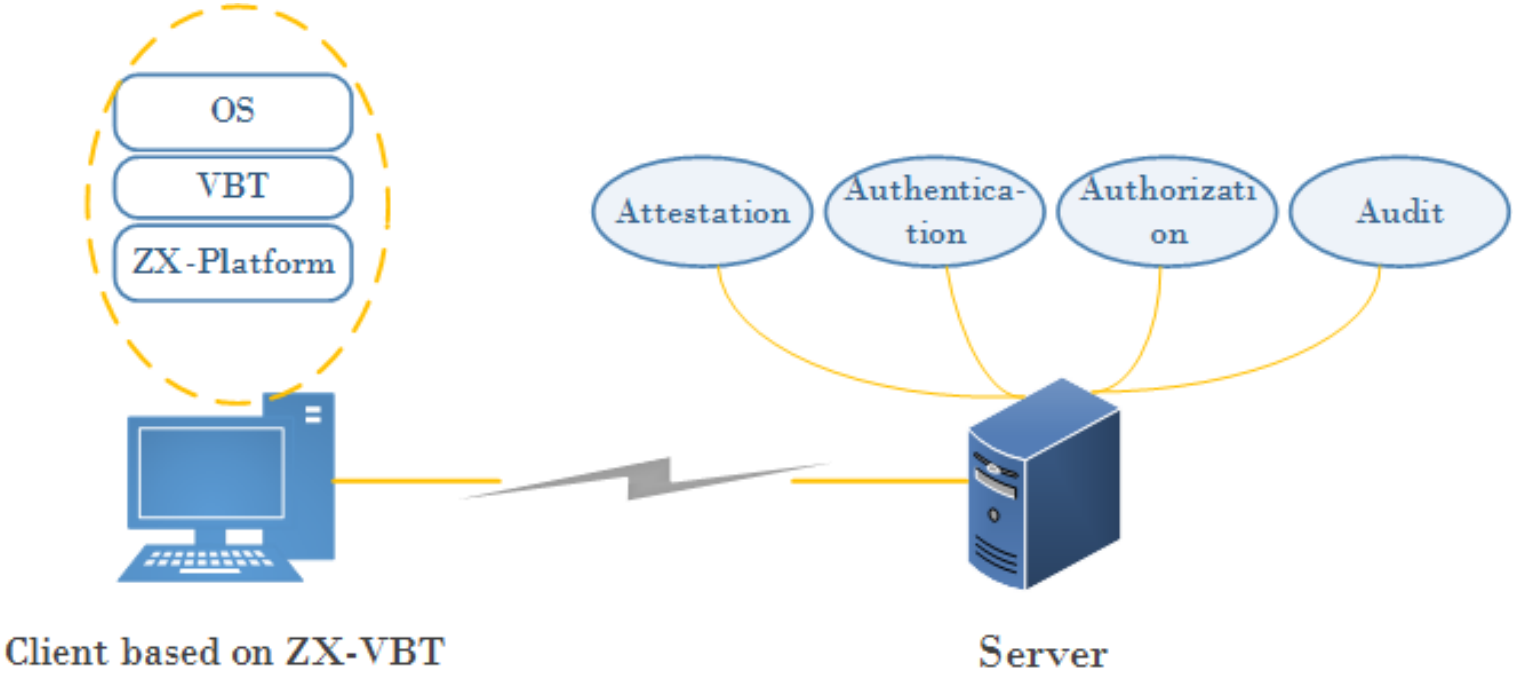
- 建立可信执行环境
- 以CPU为信任基
- 与TPM/TCM交互

硬件安全功能——可信计算技术（ZX-TCT）



- **满足合规要求**
  - GRC
  - 审计
- **满足CSP及客户的策略要求**
- **安全分等级**

硬件安全功能——基于虚拟化的安全



硬件安全功能——基于虚拟化的安全

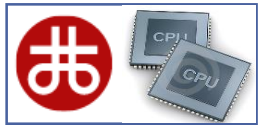
- **可信终端解决方案**
- **可用于PC办公、物联网网关或者工控网关等领域**
- **特点**
  - **Attestation**
    - 利用TPM保证终端的可信；
  - **Authentication**
    - 对使用终端的用户使用RBAC(基于角色的访问控制)
  - **Authorization**
    - 根据用户角色为用户配置恰当的授权策略；
    - 控制诸如U盘、硬盘等设备的使用；
  - **Audit**
    - 监控终端内核;
    - 检测并拦截隐匿的rootkit和APT等高级威胁；

基于兆芯CPU的网络安全

- 国产化网络安全设备越来越受到关注，也得到了一定规模的部署
- Open Network Platform架构参考设计和DPDK技术在网络安全设备（如防火墙和安全网关）中被广泛使用
- 兆芯CPU和芯片组实现了ONP架构和DPDK要求的硬件功能

基于兆芯CPU的云计算

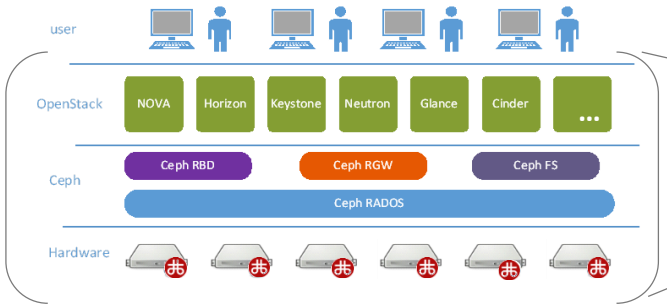
- 国产化计算机在云计算基础设施中的应用方兴未艾
- 兆芯云计算解决方案“整装待发，扬帆起航”

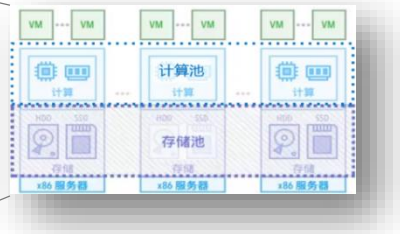


兆芯云计算解决方案——软件定义基础架构

兆芯硬件平台 + openstack + ceph = 兆芯云计算解决方案

- 按需采购
- 弹性扩展
- 快速交付
- 简化管理
- 单一支持

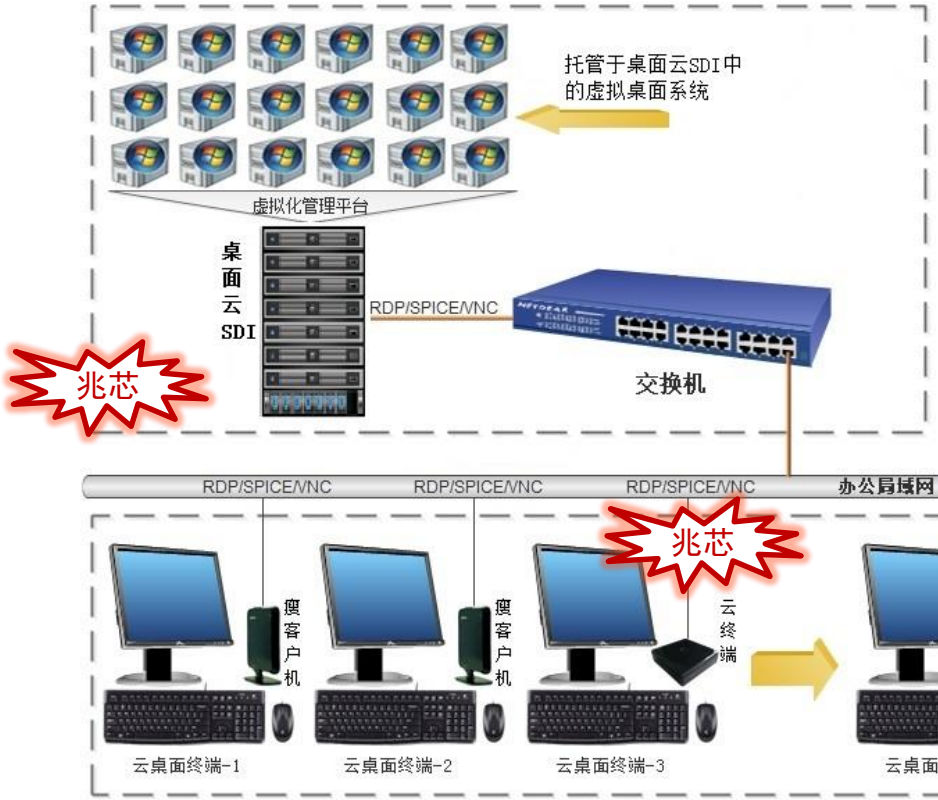




未来计划：构建“安全可控+可信”的云计算平台

- 融合国产软硬件，合作增强云安全

兆芯云计算解决方案——桌面云应用场景



- 数据安全
- 集中化管理
- 高可用性保证
- 弹性扩展
- TCO降低

政府
- 安全办公
- 电子政务
- 社区服务
- 办事大厅

教育
- 多媒体教学
- 远程教育
- 偏远学校
- 图书馆

大企业
- 安全办公
- 外包开发
- 分支机构
- 移动办公

医疗
- 社区工作站
- 远程医疗会诊
- 区域信息平台
- 健康档案管理

总结

兆芯为嵌入式/工控提供安全的x86解决方案

兆芯CPU提供了硬件安全功能

- 密码加速指令
- 安全启动技术
- 可信计算

兆芯本着开放的态度，希望能和更多的厂商合作！

扫描二维码

关注兆芯官方微信

谢谢

兆芯