



Occlum

Secure and Efficient Multitasking Inside a
Single Enclave of Intel SGX

蚂蚁金服 闫守孟



ASPLOS'20 论文

Occlum: Secure and Efficient Multitasking Inside a Single Enclave of Intel SGX.

Youren Shen* (Tsinghua University)

Hongliang Tian* (Ant Financial Services Group)

Yu Chen (Tsinghua University & Peng Cheng Laboratory)

Kang Chen (Tsinghua University)

Runji Wang (Tsinghua University & Ant Financial Services Group)

Yi Xu (Tsinghua University & Ant Financial Services Group)

Yubin Xia (Institute of Parallel and Distributed Systems Shanghai Jiao Tong University)

Shoumeng Yan (Ant Financial Services Group)

*** H. Tian and Y. Shen equally contributed to this work**

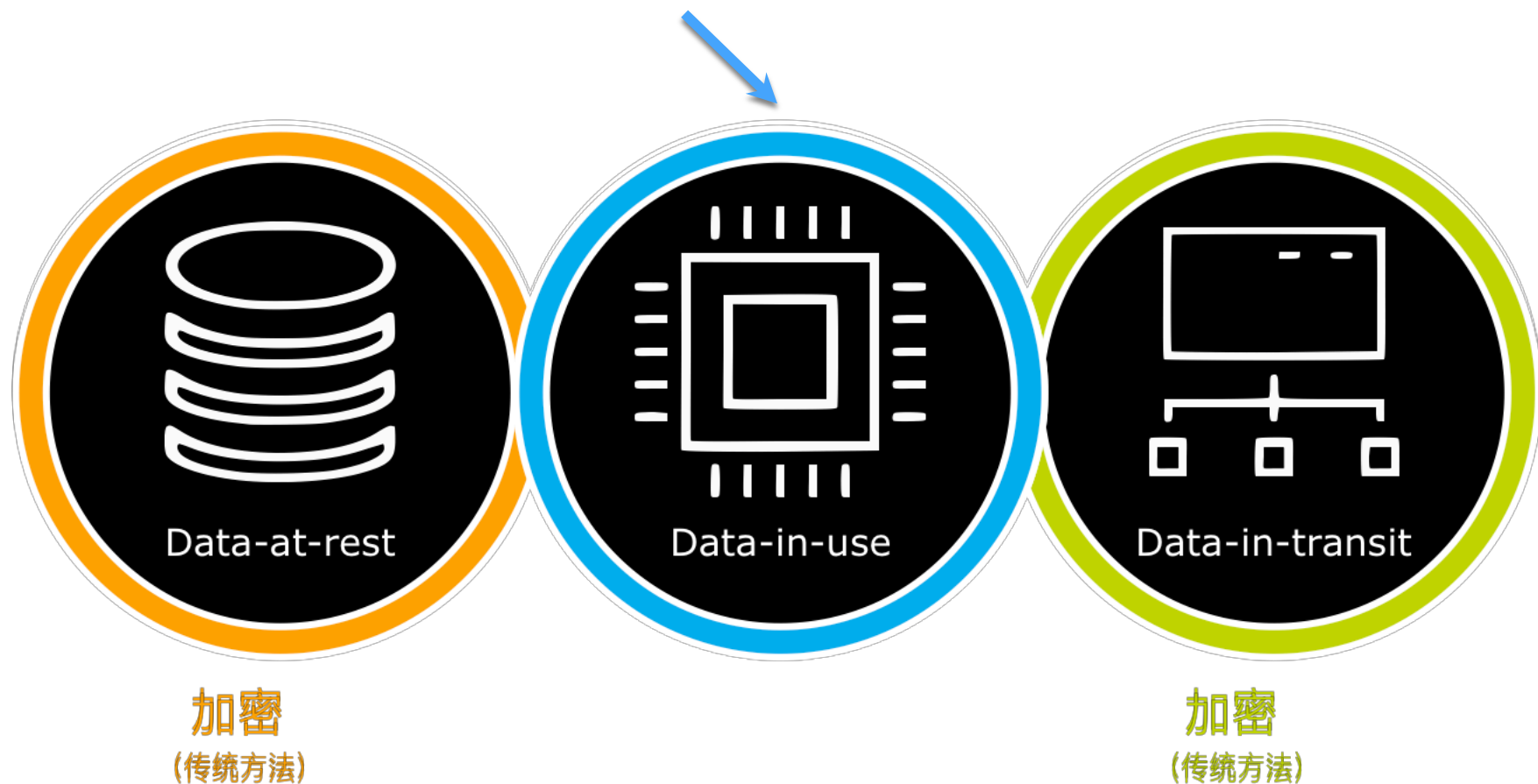


蚂蚁安全计算团队

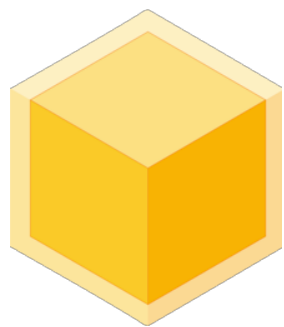
System x Security x Safety



安全计算要解决的问题



安全计算：国外动作频频



Google Asylo

2018年5月 发布



IBM Enarx

2019年5月 发布



**Azure Open
Enclave SDK**

2019年8月 捐给CCC



AWS Nitro Enclaves

2019年12月 接受Preview



安全计算：国内风云乍起

《基于可信执行环境的安全计算系统技术框架》 行业标准立项成功

牵头单位：中国信息通信院、中国移动

发起单位：蚂蚁金服

参与单位：华为、腾讯、百度、光之树、Oppo、360、高通、
大唐电信、中国电信、如家首旅、上海交大



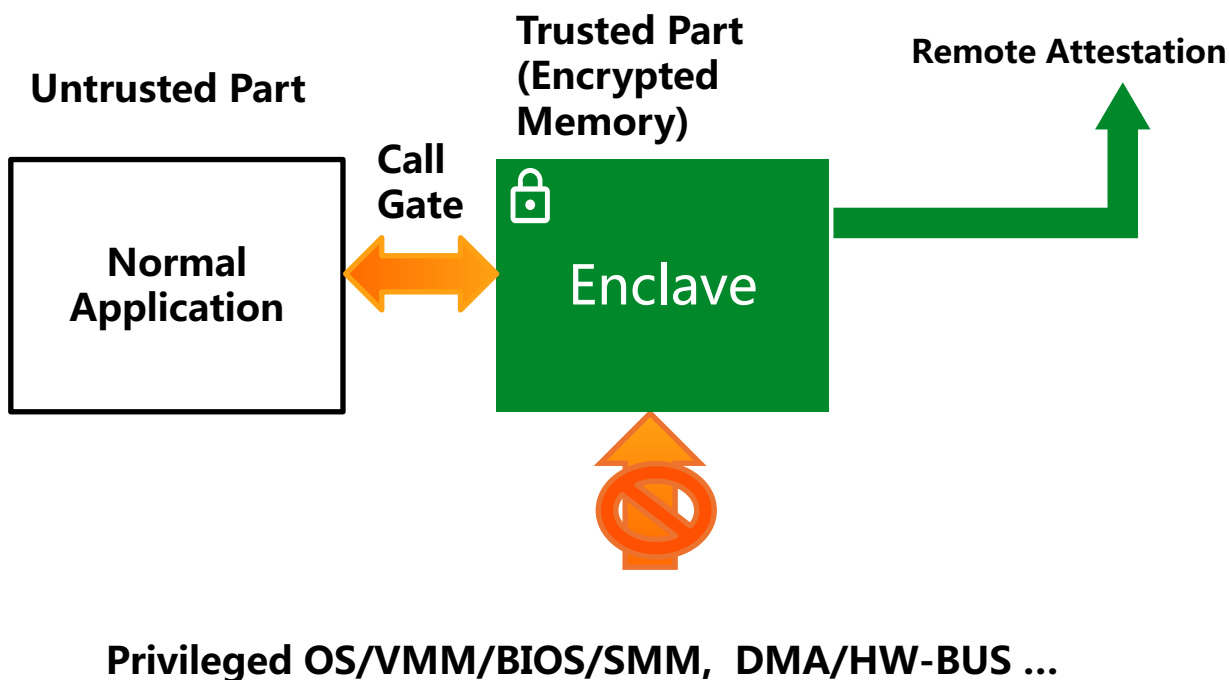
秘

蚂蚁金服 安全计算

为了不能丢失的秘密

Enclave: 运行时双向防护

内存加密，防止操作系统窥视业务
完整性检查，保证代码不被替换

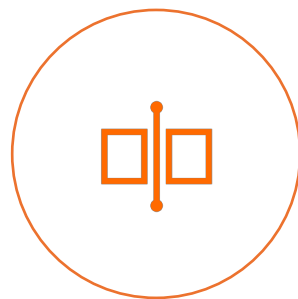


目前Enclave使用中的问题



需要改写应用

没有系统调用、多进程
多线程、基本库不完整



需要分割应用

需要把业务程序划分为
enclave内和enclave外的部分



未集群化

Enclave资源未纳入集群管理
Enclave集群未跟Kubernetes结合



SOFAEnclave

金融级、可扩展、开放Enclave体系





Occlum



主要特色

1. 极速进程启动，告别应用程序卡顿
2. 多种文件系统，透明保证数据安全
3. 内存和并发安全，更少bug、更值得信赖
4. 用户轻松上手，三行命令保护App
5. 蚂蚁金服业务场景打磨



极速进程启动

图1. 不同大小的进程启动时间

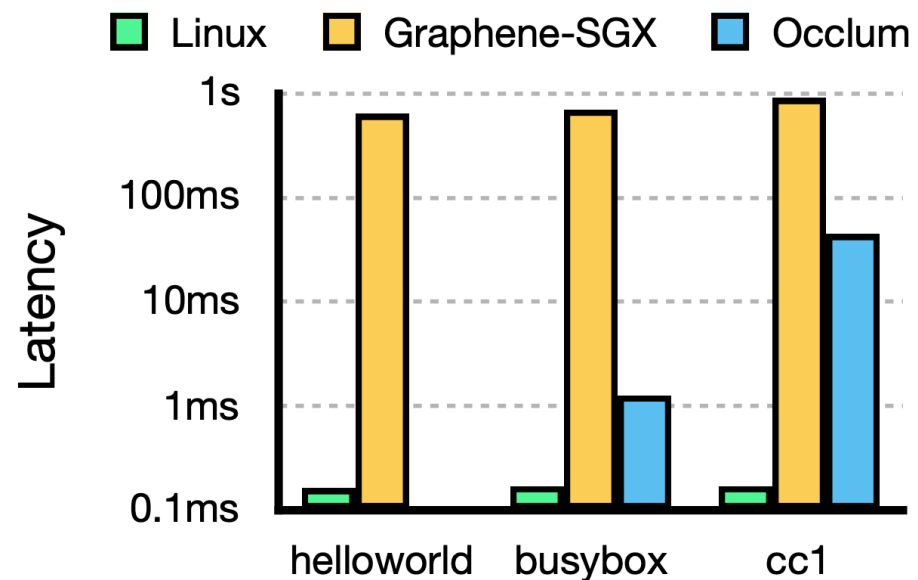
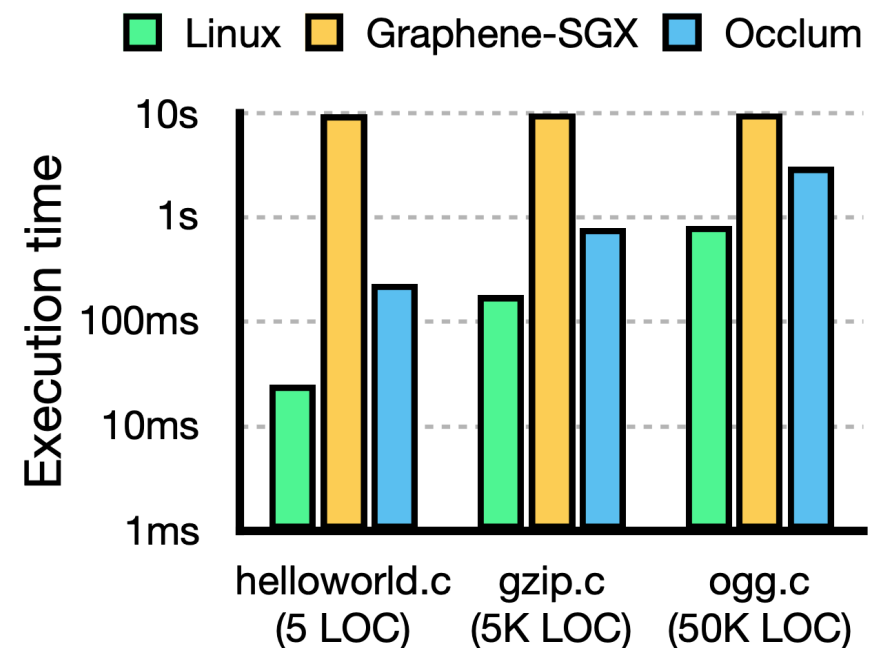


图2. GCC编译C文件的时间



对启动多个进程的负载，Occlum比Graphene-SGX快得多的多



多种文件系统支持

1. Read-only integrity-only FS （用于可信rootfs的分发）
2. Writable encrypted FS （用于安全存储运行时数据）
3. Untrusted host FS （与主机传输数据）
4. Ram FS （存储临时性数据）
5. Union FS （用于安全共享只读数据）

Graphene-SGX不支持



The diagram consists of a red line that starts from the right side of the text 'Graphene-SGX不支持', goes down, then left, then up, and finally left again to point at item 2 'Writable encrypted FS'. A second red line starts from the same vertical segment, goes down, then left, and finally left again to point at item 5 'Union FS'.



内存和并发安全

Memory safety in C and C++ remains largely unresolved... ASAN is heavily used at Google and across the industry and it has found [tens of thousands bugs](#).

From Google security researchers*

- Occlum是全世界首个、也是唯一的用Rust语言开发的TEE OS
- Occlum 90%以上的代码都是safe Rust，大大降低了出现内存安全和并发安全bug的几率

Occlum更值得用户信赖

* Memory Tagging and how it improves C/C++ memory safety. Kostya Serebryany, Evgenii Stepanov, Aleksey Shlyapnikov, Vlad Tsyrklevich, Dmitry Vyukov. Google. 2018



用户轻松上手

Hello World

Intel SGX SDK: 10+文件 , **300行**代码

Rust SGX SDK: 10+ , **200行**

Google Asylo: 4 , **100行**

Occlum: Linux 代码 , 1 file , **5行**
只需3条命令即可将Hello World跑在Enclave里




```
[tate.thl-occlum-dev|~/hello_world]  
└─
```

```
}
```

用户轻松上手

大部分人没入门就放弃的社区是火不起来的。

—— KATA安全容器创始人 王旭

Graphene-SGX

1. 配置环境和编译项目 (一天, 😞)

2. 理解100多行的Makefile (半天, 🤯)

3. 跑我自己的SGX app (终于! 😭)

Occlum

1. 直接下载Docker镜像 (10min, 😊)

2. 理解3条的Occlum命令 (5min, 🤔)

3. 跑我自己的SGX app (So easy! 😄)



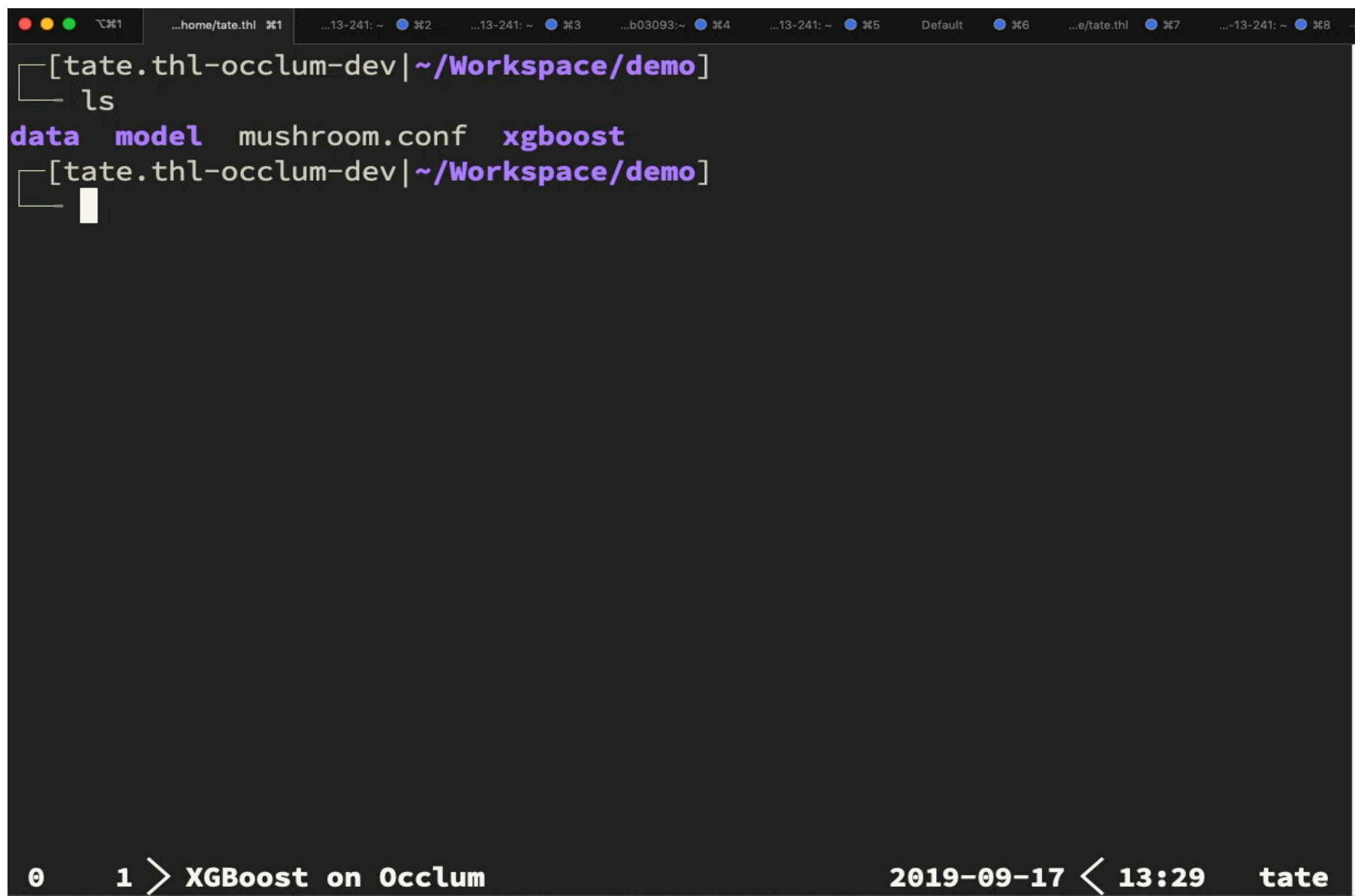
赋能大型应用安全计算场景

安全AI

- XGBoost
- TensorFlow
- OpenVino

可信编译

- WASM
- GCC
- LLVM



```
[tate.thl-occlum-dev | ~/Workspace/demo]  
ls  
data model mushroom.conf xgboost  
[tate.thl-occlum-dev | ~/Workspace/demo]  
█
```

0 1 > XGBoost on Occlum 2019-09-17 < 13:29 tate

Occlum快速迭代

更多特性

- 更多syscall
- 更多测试
- 多语言支持
- Glibc兼容
- Fork支持

...

0.8.0版

- 远程证明

2020年

2019/12

0.7.0版

- 二进制兼容

2019/11

0.6.0版

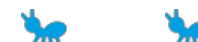
- 发布大量Demo

2019/10

0.5.0版

- Occlum CLI工具

2019/09



Practical Implications of Graphene-SGX

Research Project 2

August 13, 2019

Robin Klusman
University of Amsterdam
Security and Network Engineering
robin.klusman@os3.nl

Derk Barten
University of Amsterdam
Security and Network Engineering
derk.barten@os3.nl

Supervisor:
Gijs Hollestelle
ghollestelle@deloitte.nl

A. Conclusion

As becomes clear from our findings, there are significant implications when naively running arbitrary software in Graphene, both in terms of security and usability. A malicious Operating System can compromise enclave security in specific scenarios if no mitigations are implemented in the application itself. Furthermore, running an application in Graphene requires significant effort and know-how by the user. We deem Graphene to not be at a maturity level where it can be used for production purposes, as still numerous bugs and other issues exist. Graphene in our opinion does not provide a secure and stable framework to run applications. We do, however, believe that it provides a decent open-source tool to conduct further research on SGX. We, therefore, advise any developers opting to run their applications in Graphene to take particular care when doing so, while also taking note of the security history of SGX.



谢谢

欢迎加入蚂蚁安全计算团队！

欢迎学术、技术、和产品合作！

邮件 shoumeng.ysm@antfin.com

微信 32713933

Occlum开源项目 <https://github.com/occlum/occlum>

