龙蜥社区国密生态体系

张天佳

龙蜥社区商密SIG Maintainer

阿里云

目录


国密简介和现状

商密算法体系

从2010年起，国家密码管理局陆续公布了国内研制的若干密码算法。

从2015年起，SM2，SM3，ZUC，SM9，SM4算法陆续成为ISO/IEC国际标准。

伴随着相关法律法规的完善，我国商用密码国际标准体系已初步成型。

行业现状

密码作为安全基础设施，已经非常成熟。

商用密码标准体系相对完善。

法律法规体系基本形成。

行业成熟

为密码生态提供更多的选择。

国内信息安全基础设施的多样化需要。

密码多样化

作为基础设施，在操作系统和基础软件中的支持有限。

行业和社区解决方案众多，但各自为战，没有形成社区合力。

合规门槛高，行业排他性强。

国密碎片化严重

与主流国际算法相比，国密支持度低。

性能差，没有硬件指令支持。

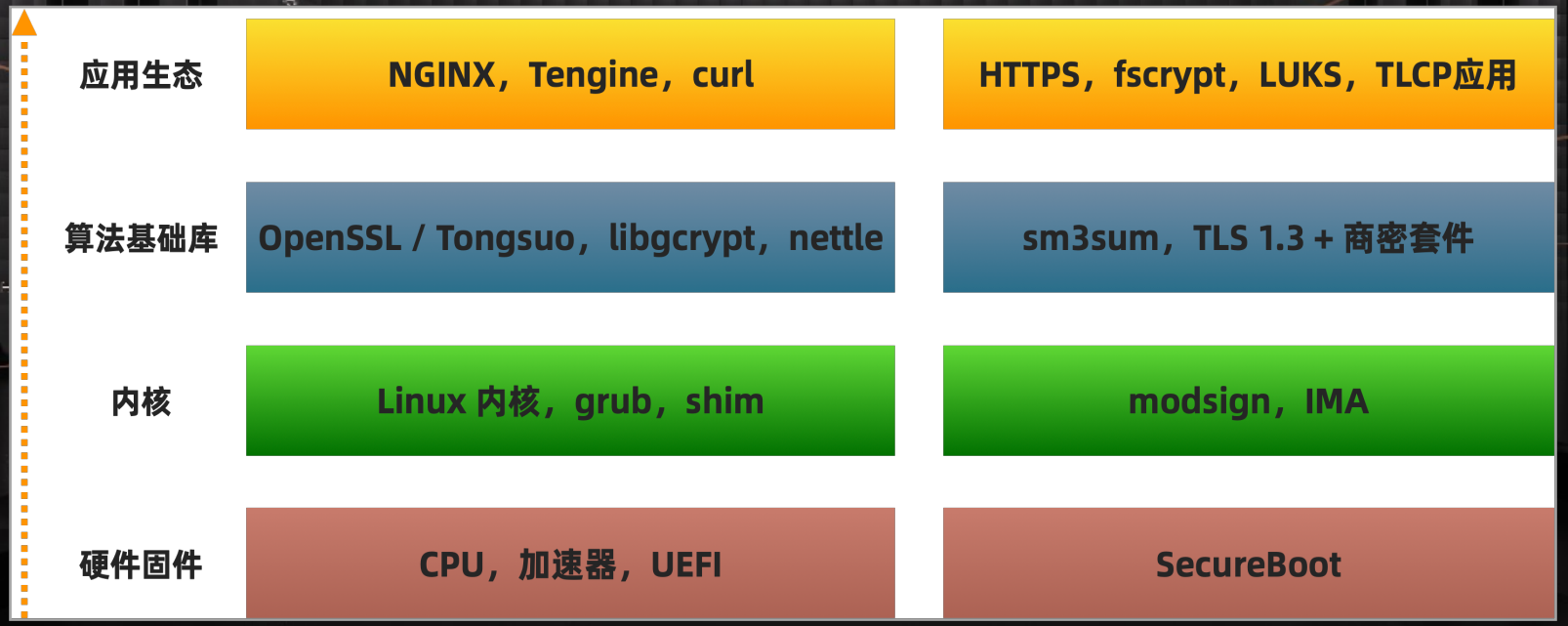
常常是为合规服务，仍然有很多应用场景不支持国密。

用户体验差


商密软件栈SIG介绍

商密软件栈SIG

让天下没有难用的国密



目标：建立以国密算法为主的系统组件，在固件，bootloader，内核以及基础应用中支持国密算法，基于Anolis OS社区发行版构建开箱即用的国密技术栈及解决方案生态

《商用密码技术最佳实践白皮书》

PDF 下载地址：https://openanolis.cn/shangmi

白皮书电子版：https://openanolis.github.io/whitebook-shangmi

白皮书电子版 git 仓库：

https://github.com/openanolis/whitebook-shangmi

（本仓库接受勘误及PR，欢迎贡献优质内容，共建商密生态）

社区开发原则

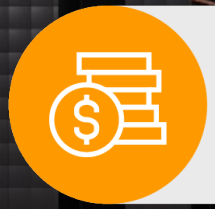
原则：依托基础软件上游社区，为已有的轮子支持商密算法，不重新造轮子

国密算法社区支持情况

原则：依托基础软件上游社区，为已有的轮子支持商密算法，不重新造轮子

开源软件名称	SM2	SM3	SM4	PKCS#7	X509	commit数	修改行数
gnulib	-	✅	-	-	-	5	-5/+1046
libgcrypt	✅	✅	✅	-	-	22	-155/+4202
linux	✅	Y	Y	✅	✅	68	-1536/+15478
RustCrypto	❌	✅	Y	-	-	1	-0/+851
ima-evm-utils	✅	✅	-	-	-	5	-13/+97
ltp	❌	✅	✅	-	-	2	-7/+30
libkcapi	-	✅	✅	-	-	2	-3/+287
nettle	❌	✅	✅	-	-	11	-11/+1241
OpenSSL	Y	Y	✅	Y	Y	14	-81/+471

Anolis OS 8.8 内置完整国密能力



性能优化
ANCK 5.10，SM4提升40倍

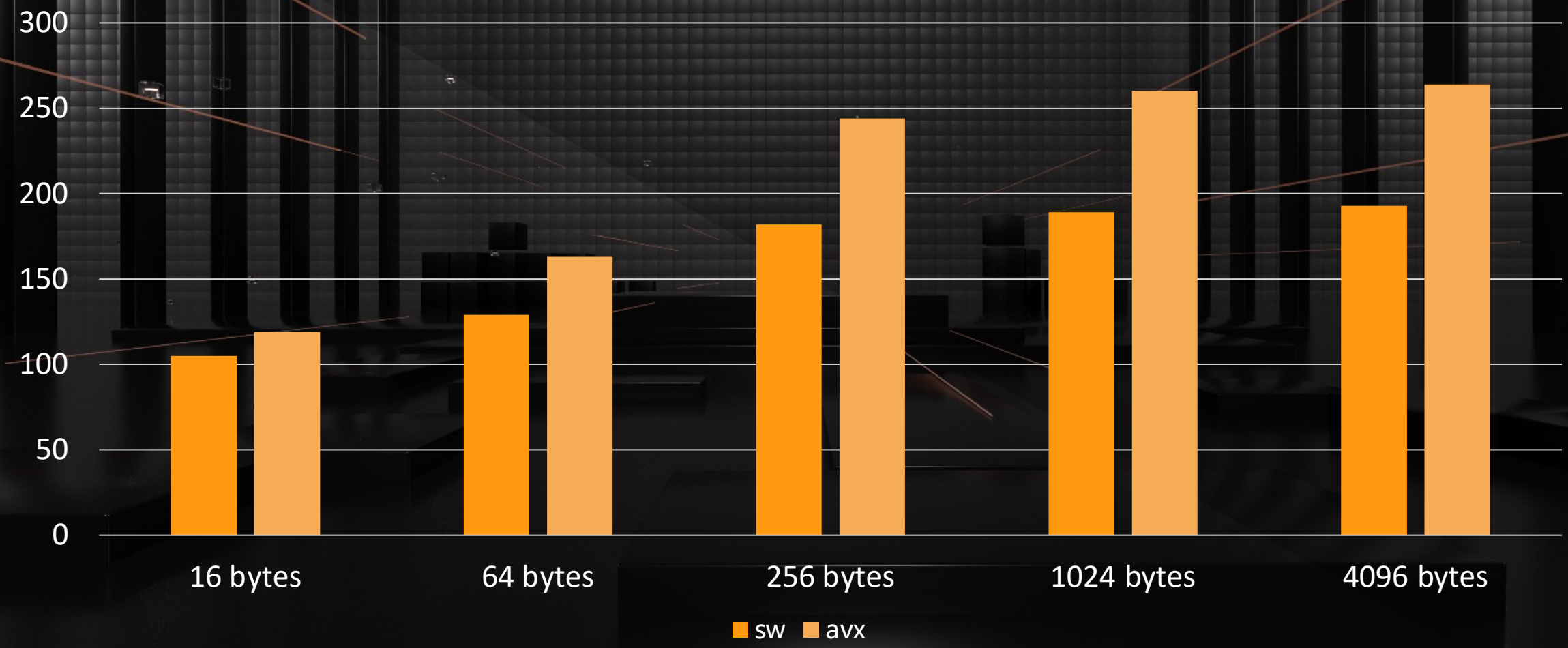
内置商密
OpenSSL支持SM2签名能力

开箱即用
不依赖任何外部组件

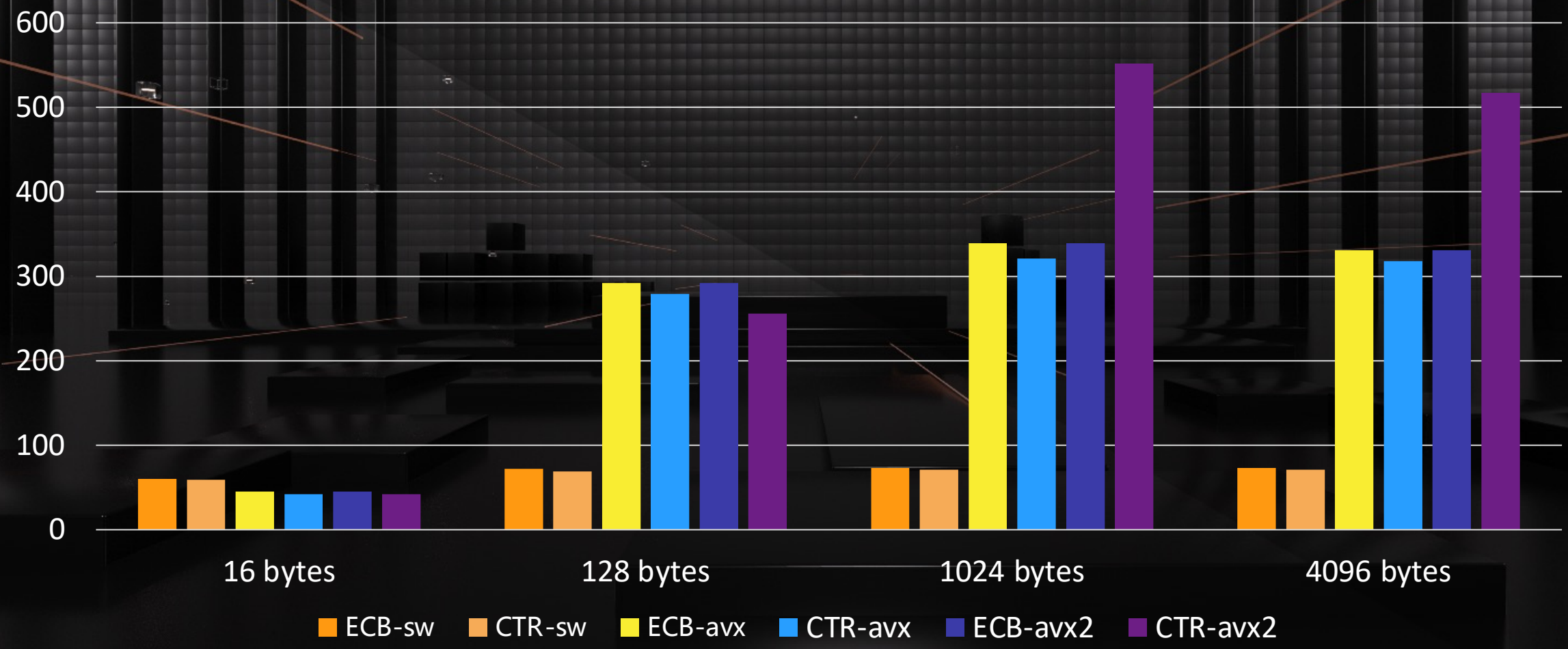
兼容稳定
向前兼容，补齐国密能力

国密应用场景

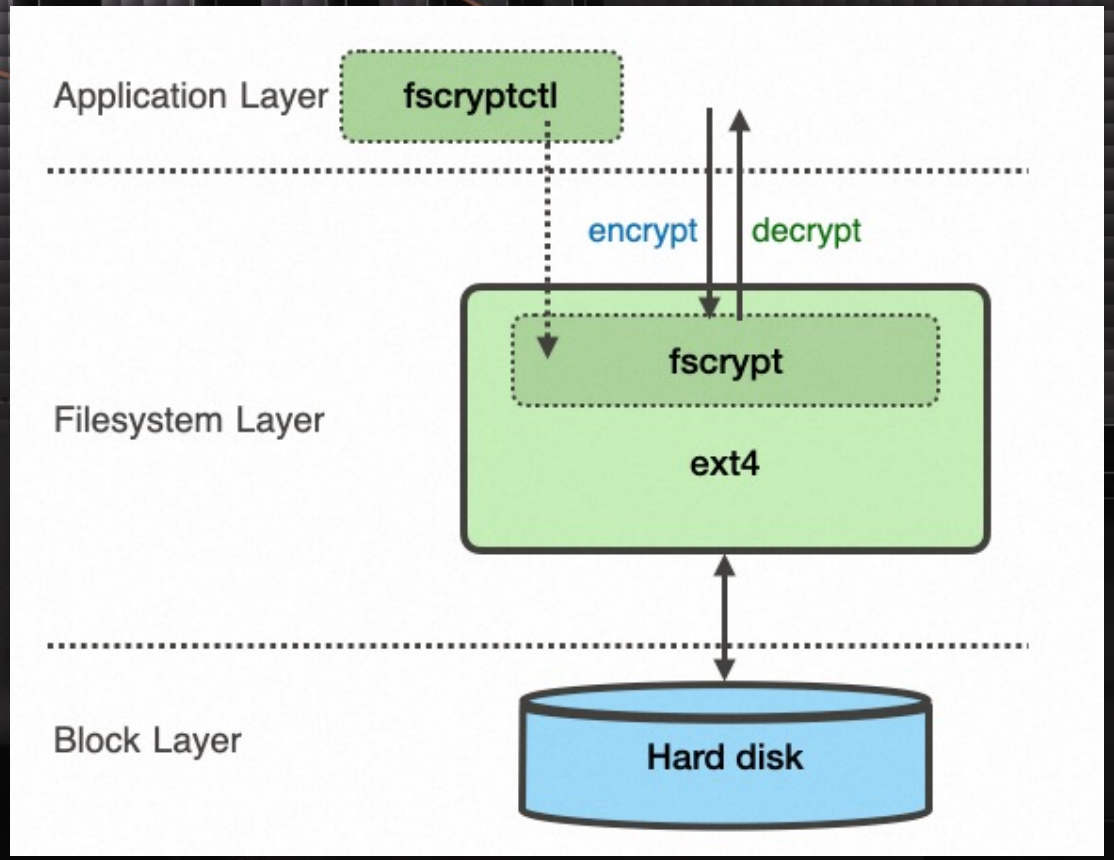
x86指令集优化 – SM3



x86指令集优化 – SM4



文件加密（fscrypt）




```
> fscryptctl add_key /mnt < /tmp/keyfile
23086a13ed81fd75ca5fe9b8f2ff25c7
> fscryptctl set_policy \
    --contents=SM4-XTS \
    --filenames=SM4-CTS \
    23086a13ed81fd75ca5fe9b8f2ff25c7 \
    /mnt/test
```

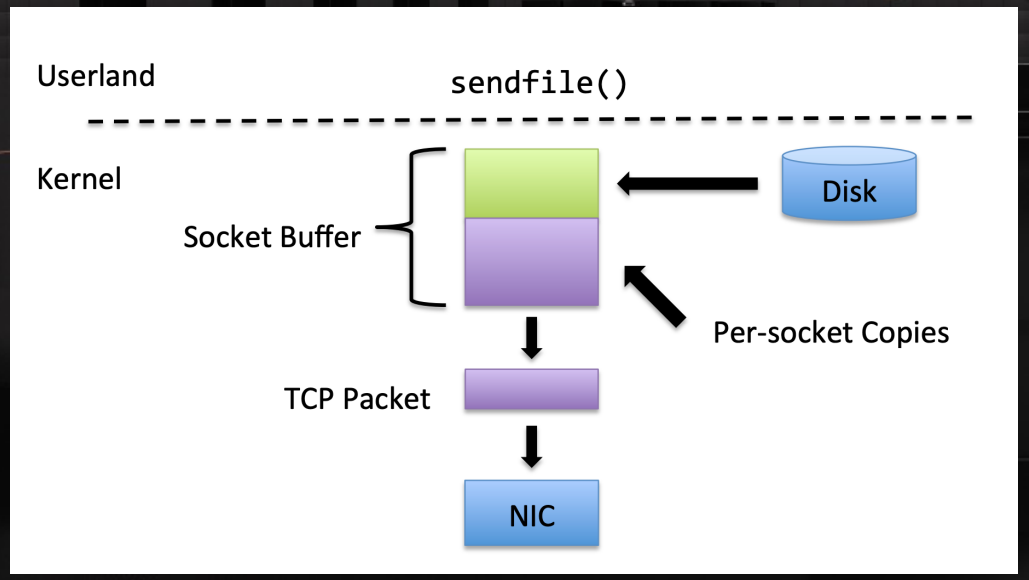
```
root@vm-amd64 /mnt/test tree
.
├── JHj63LH6s_e2WCoK6v9cJ9_TmxQfDKuTGIGmfJ6FjJhcTWSCMBO_Xw
├── SJMCpbBT9qU41pYqh258LJpNOkrkxjF-0KqQJfED79ljuRvadXqJ-g
│   ├── 5Oe52h6fkmZlrki1B90qWgMlAx9wfgHyDnTjE9_KDiJz0c__uP6DFw
│   ├── dCBa4yOndL3rw1enWE8enR0G_HtjqykHX3-UBC3EaItXqZwHdTU7nQ
│   └── eIca9dsc41TiizW3IEyyhC70-GvyrOE23a6iGuWQhWxRtQmH3hthPA
└── TF4D20xgD0Mwz4krxgOHoe23ZgSNJ-GDRZh9Sc2NW0AFGRSKPPTeBw

1 directory, 5 files
```

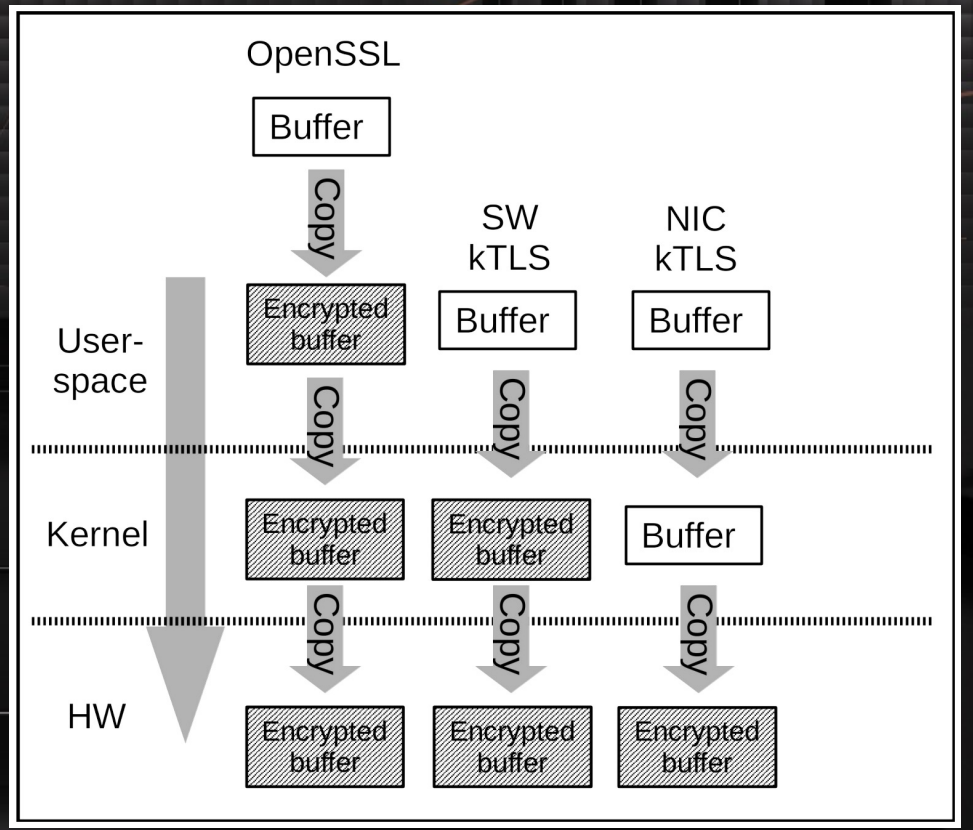
Kernel TLS (KTLS)

KTLS通过把TLS中的数据平面卸载到内核，减少用户态和内核的数据拷贝，是TLS的重要加速手段

ANCK 5.10 内核支持 KTLS 使用 SM4 GCM/CCM算法：

```
#define TLS_CIPHER_SM4_GCM                55
#define TLS_CIPHER_SM4_CCM                56
```





SM2 支持无 Za 的签名

Za = SM3 (entla || distid || a || b || xG || yG || xA || yA)
hash = SM3 (Za || Message)
sig = SM2_sign(hash)

PR：https://github.com/openssl/openssl/pull/20853

```
# 生成证书签名请求
openssl req -verbose -new -sm3 \
        -sigopt "sm2-za:no" -key sm2.key -out sm2.csr

# 签名CSR
openssl x509 -req -days 10000 -sm3 \
        -sigopt "sm2-za:no" -vfyopt "sm2-za:no" \
        -extfile genkey.conf -extensions v3_req \
        -CA ca.cert -CAkey ca.key -CAcreateserial \
        -in sm2.csr -out sm2.cert
```

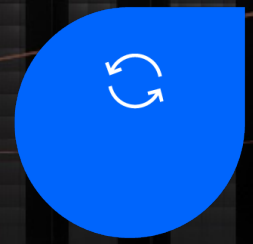

未来规划

TODO

更多场景支持

优化无止境

增强产品能力



合规

SIG地址：https://openanolis.cn/sig/crypto

Anolis 商密软件栈 SIG

242 人

扫一扫群二维码，立刻加入该群。