ISCAS 中国科学院软件研究所学术年会
暨重点实验室科技活动周 2025 第十届

学术论文

基于动态完整性度量的机密计算运行时监控方案

李为，冯伟，秦宇，冯登国

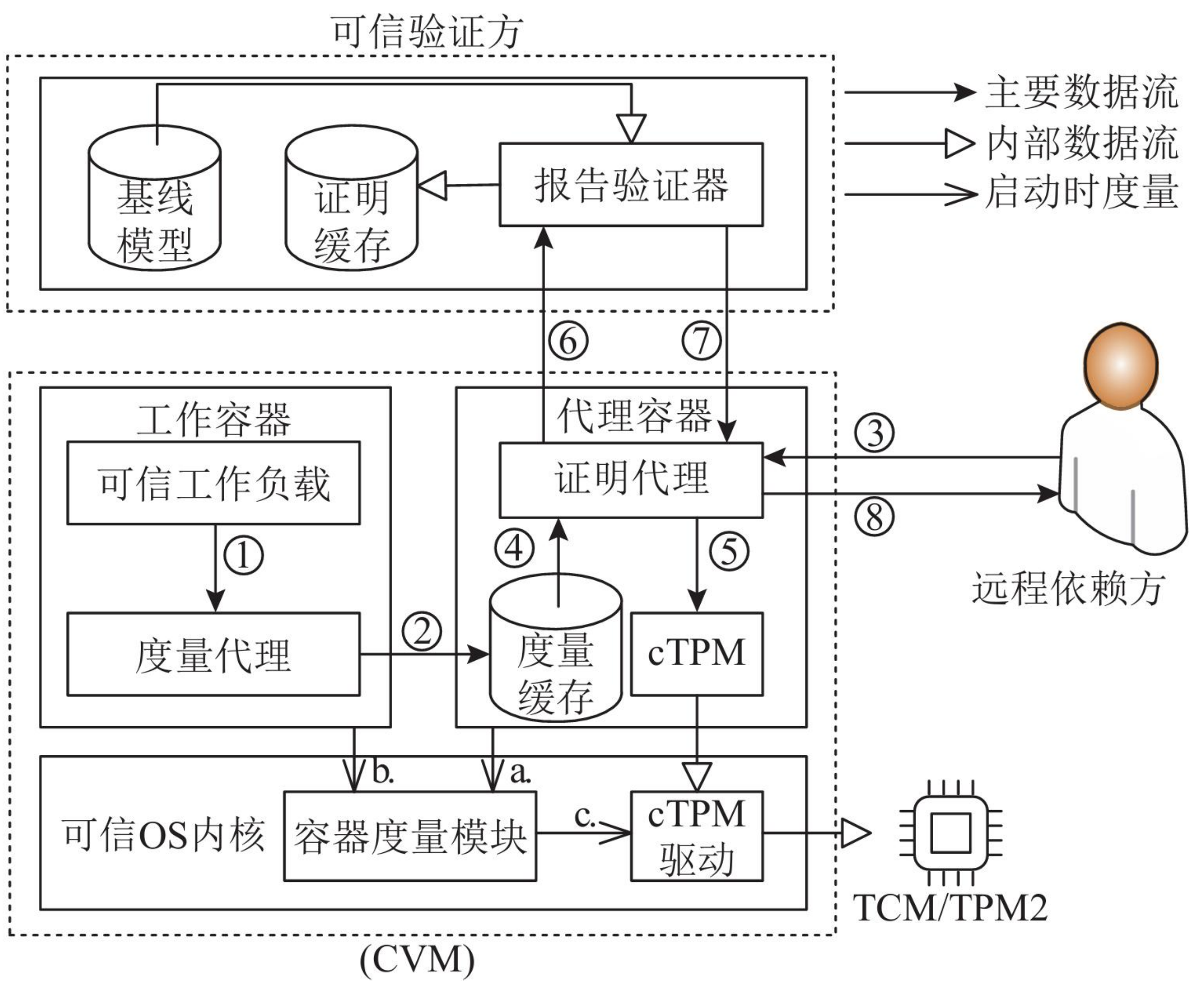
《计算机研究与发展》，2024

联系方式:
{liwei2018,fengwei2009,qinyu}@iscas.ac.cn

➢ 摘要

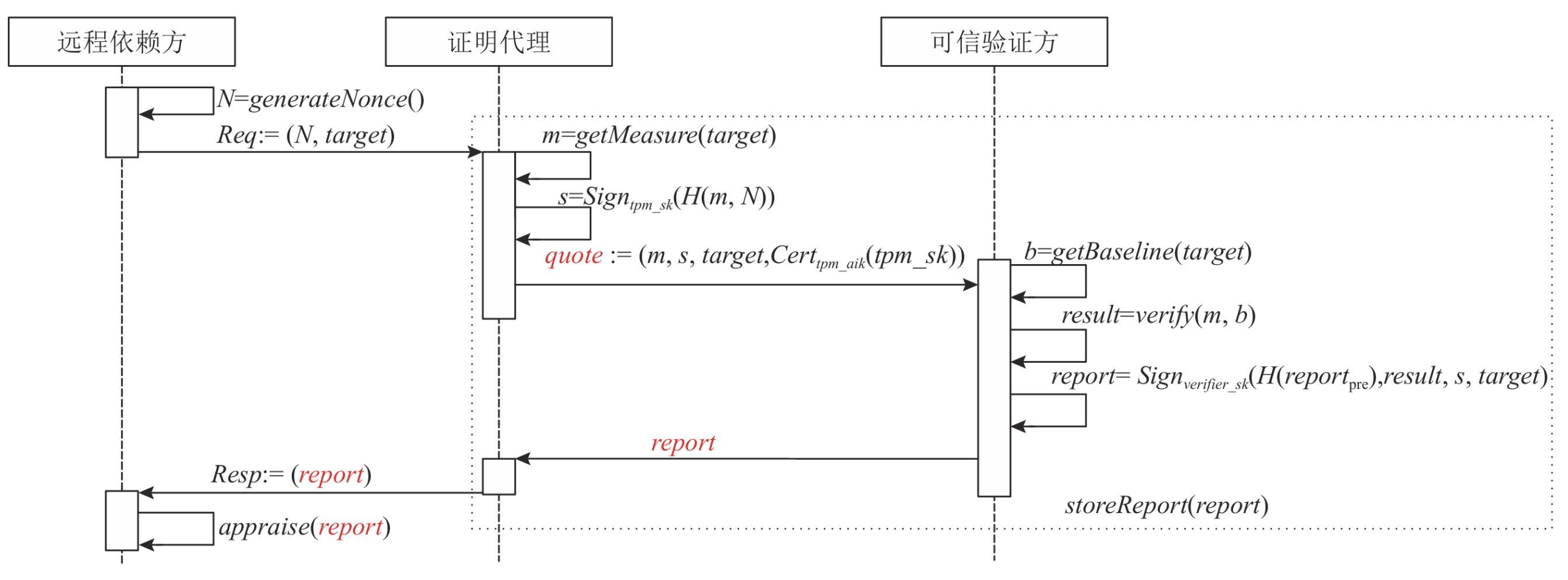
针对机密计算平台缺少运行时完整性保护问题，提出了一种基于动态完整性度量的机密计算运行时监控方案，通过向TEE中引入控制流和数据流度量和运行时远程证明，实现了机密计算平台内用户工作负载的运行时完整性保护。

➢ 系统架构



- **机密虚拟机CVM**
  - 采用系统级TEE
  - **工作容器**：内部运行可信工作负载，集成度量代理使其具备动态完整性度量能力
  - **代理容器**：与工作容器在同一个CVM，基于cTPM使CVM具备运行时证明能力
  - **可信OS内核**：内核度量模块，cTPM驱动
- **可信验证方**：接收证明报告，返回证明结果报告；包含报告验证器、基线模型和证明缓存3个子组件
- **远程依赖方**：远程用户，发起证明请求，获得证明响应；根据证明响应评估TEE是否满足运行时安全性

➢ 运行时证明



➢ 有效性验证

```
[
 {
  "from": "855ee82b",
  "bbid": "55b1855ee82b",
  "to": "8e84d960"
 },
 {
  "from": "855ee756",
  "bbid": "55b1855ee756",
  "to": "8e848ac0"
 },
 {
  "sensitive_area": "00000001",
  "bbid": "55b1855ee7b9",
  "data_pointer_num": "00000001"
 },
 {
  "from": "855ee871",
  "bbid": "55b1855ee871",
  "to": "8e710770"
 },
 {
  "from": "855ee89d",
  "bbid": "400055b1855ee89d",
  "to": "8e6d9d90"
 }
]
```

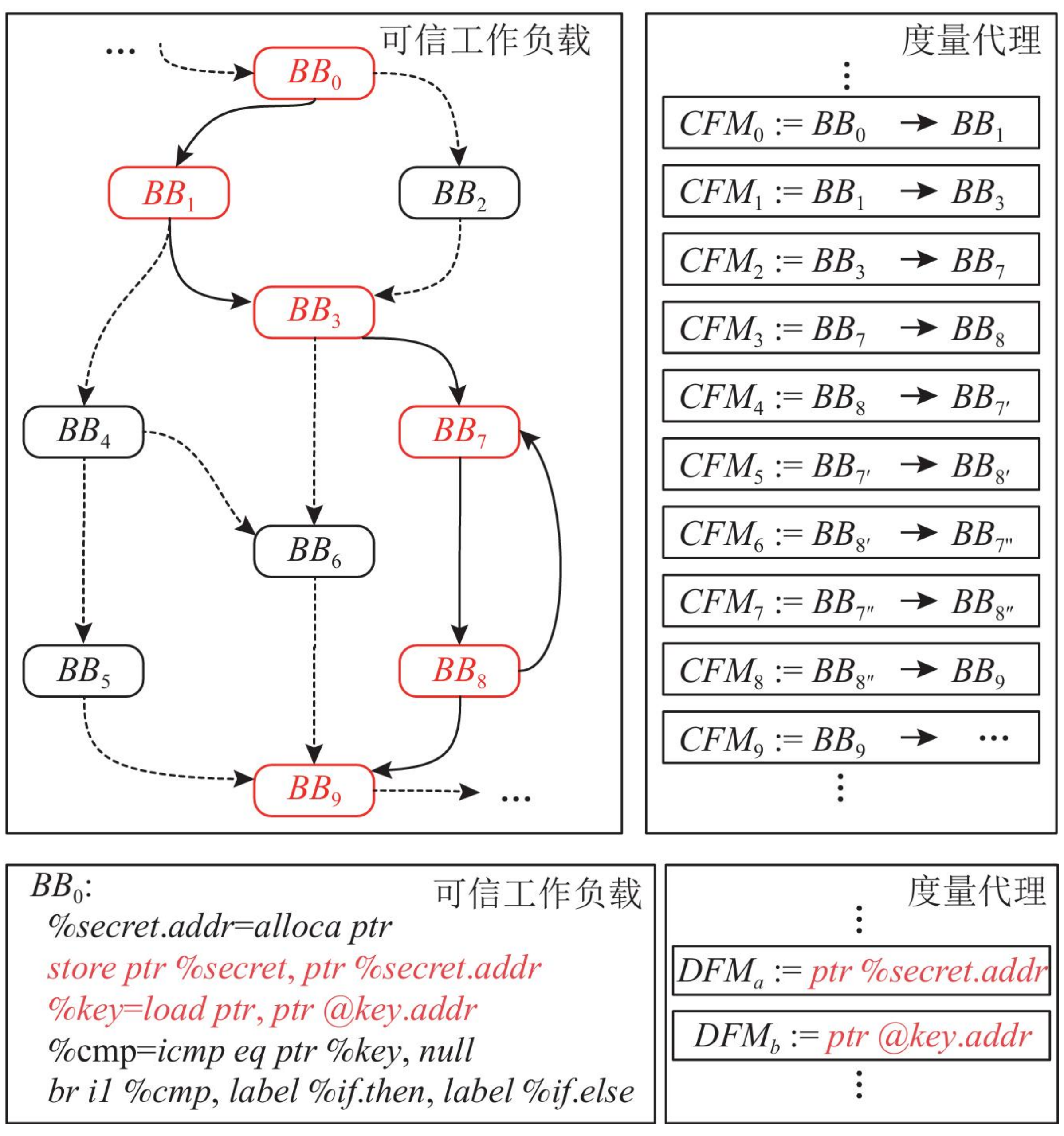
```
mov     al,0x0
call    3a10 <_Z9tracecallPvjz>
mov     rdi,QWORD PTR [rbp-0x30]
mov     rsi,QWORD PTR [rbp-0x28]
call    5850 <strcmp@plt>
cmp     eax,0x0
jne     3770 <get_secret_key+0x60>
mov     QWORD PTR [rbp-0x18],0x1

lea     rdi,[rbp-0x1c]
mov     rsi,QWORD PTR [rbp-0x8]
mov     rdx,QWORD PTR [rbp-0x10]
call    5860 <memcpy@plt>
mov     rdx,QWORD PTR [rbp-0x18]
lea     rcx,[rip+0x44a4]        # 7c30 <keys>
mov     rax,rdx
shl     rax,0x3
add     rcx,rax
lea     rax,[rip+0x4493]        # 7c30 <keys>
mov     rax,QWORD PTR [rax+rdx*8]
mov     QWORD PTR [rbp-0x38],rax
mov     rdi,QWORD PTR [rbp+0x8]
mov     esi,0x2
lea     rdx,[rbp-0x18]
mov     al,0x0
call    51a0 <_Z8traceretPvjz>
mov     rax,QWORD PTR [rbp-0x38]
add     rsp,0x40
pop     rbp
ret
```

➢ 主要贡献

- ✓ 提出了一种针对机密虚拟机/容器中工作负载的有效动态完整性度量方案，当**敏感工作负载在机密虚拟机/容器内运行时**，可以有效捕获工作负载**运行时控制流和数据流**的动态完整性度量值，弥补了启动时静态完整性度量的不足；
- ✓ 完成了对机密计算平台机密虚拟机/容器工作负载动态完整性度量结果的**运行时远程证明**方案，通过对比受保护程序的合法基线模型，可以对度量结果进行验证，并基于可信模块TCM/TPM2，**将运行时证明的信任模型与原机密计算平台TEE信任模型解耦**；
- ✓ 在多个机密计算平台（国产海光CSV、AMD SEV等）上实现了原型系统并进行验证，结果表明方案具有良好的安全性和性能开销，**是一种实用的机密计算运行时保护方案**。

➢ 控制和数据流度量



➢ 实现和评估

性能开销	平均值/%	中位数/%	最优值/%	最差值/%	测试耗时/s
普通 VM 总开销	14.65	8.44		71.42	40.5/59.3
CVM 总开销	16.11	10.73		71.48	41.7/60.6
动态度量开销	13.76	9.72		68.86	
通信开销	2.35	1.73		7.50	
CVM 相比普通 VM 开销提升	3.09	2.91	1.64	4.96	

使用CSV/SEV服务器作为机密计算平台，在其机密虚拟机/容器基础上进行了系统原型实现与实验评估，结果表明，方案在有效增强运行时安全性的同时，引入了约16%的性能损耗。