

第十八届全国大学生信息安全竞赛-作品赛 决赛获奖名单

一等奖（44项）

作品名称	奖项级别
帧行密护——基于BFI无线感知的人体行为识别与隐私保护系统	一等奖
鸾鸟网安——智能网络攻防一体化平台	一等奖
面向短视频的多模态舆情安全威胁感知系统	一等奖
状态转换漏洞：一种新的Web竞态漏洞发现与检测	一等奖
PrivSeek: 基于秘密分享的轻量级大语言模型密态推理系统	一等奖
图文溯源：面向视觉语言模型的多模态全过程水印系统	一等奖
强化学习和LLM驱动的5G空口协议模糊测试系统	一等奖
基于大模型的网络自动化渗透与安全加固系统	一等奖
鉴卫：基于双路协同的网页端深度伪造检测系统	一等奖
PromptGuard——基于内容级输出相似性的Prompt版权保护系统	一等奖
EchoShield: 基于对抗扰动的语音内容隐私保护系统	一等奖
SonicGuard: 基于对抗扰动的语音隐私主动防御系统	一等奖
面向 AIGC 的溯源水印嵌入与检测系统	一等奖
威胁慧眼-知识驱动的智能威胁情报构建和分析平台	一等奖
明鉴——基于大模型的语义驱动智能合约漏洞定位平台	一等奖
SQLiPecker——基于Multi-Agent的SQLi漏洞检测系统	一等奖
安眸：面向社交场景的网络异常监测与舆情可视分析系统	一等奖
M-FUSE: 面向多层次安全的高效数据隐私融合计算平台	一等奖
DeepPot: 基于大语言模型的智能蜜网威胁狩猎系统	一等奖
IoTStateFuzzer——基于模型学习的物联网设备业务逻辑漏洞检测系统	一等奖
CyraSafe-扶光大模型服务安全风险评估平台	一等奖
DoTA: 基于污点分析的面向拒绝服务攻击的智能合约分析框架	一等奖
基于语义-行为建模LLM的反沙箱检测系统	一等奖
DroneSentry: 基于射频指纹的非法无人机小样本开集识别系统	一等奖
MimicLock: 基于不可学习样本的语音克隆防护系统	一等奖
MaskSentinel: 面向主流视频通信应用的即插即用深度伪造快速检测预警系统	一等奖
SigTrace: 基于数字签名的电子文档泄露溯源系统	一等奖
隐波缉影——基于电磁波衍射模型的低成本隐藏摄像头定位系统	一等奖
智鉴千行-基于指令微调与双阶段知识增强的漏洞检测系统	一等奖
面向信息安全试验的网络攻击负载生成系统	一等奖
RAGFlow: 基于大模型跨模态语义增强的智能合约攻击检测系统	一等奖
GAIGuardian: 面向生成式AI的动态演化监管系统	一等奖
数维链——区块链+AI双轮驱动下的数据层级确权与安全流通平台	一等奖
SymRecover++: 基于弱源码的智能符号表重建工具	一等奖
CANGenius——车载CAN总线智能模糊测试系统	一等奖
V2X-Safer: 大模型生成场景驱动下的 V2X 车路协同 ADS 安全检测系统	一等奖
声影真知——基于视听觉表示学习的零样本深度伪造检测	一等奖
FLARE: 面向商用大模型的事实与逻辑双通道幻觉检修系统	一等奖
一种基于国产硬件的数字货币冷钱包	一等奖
基于加密指令标签的计算安全处理器设计与原型验证系统	一等奖
PassSlayer——零信任全覆盖无密码认证系统	一等奖
支持跨域多方可验证的分布数字身份系统设计与应用	一等奖

作品名称	奖项级别
支持HarmonyOS NEXT的密文关键词检索完整性验证	一等奖
SwiftIrisAuth——基于LWE的链上虹膜认证系统	一等奖

二等奖（66项）

作品名称	奖项级别
面向短视频平台的AIGC视频检测与版权保护系统	二等奖
SafeIDS: 基于数据增强和集成学习的网络入侵检测系统	二等奖
智瞳: 面向串谋行为的恶意小程序检测系统	二等奖
HT-Detector: 面向硬件木马检测的集成电路硅前安全评测EDA工具	二等奖
明瞳——基于移动端GUI智能体的iOS变身APP检测系统	二等奖
基于CodeQL的C/C++同源漏洞检测	二等奖
新域密链: 洋葱分层式天地协同安全通信指挥链	二等奖
控制流约束下代码复用攻击检测与风险评估系统	二等奖
VideoGuard: 基于大模型的短视频有害内容检测与预警系统	二等奖
WaterVeil——基于UDH编码驱动的屏摄鲁棒可溯源水印系统	二等奖
DejaVuzz	二等奖
InAPSage: 智能驱动的内网攻击路径推演系统	二等奖
蜂鸟电磁眼: 便携式的无人机射频智能监视系统	二等奖
MalAgent: 鸿蒙及跨生态恶意软件深度解构与检测系统	二等奖
融合多模态注意力与群体认知的网暴信息检测与取证系统	二等奖
FadeMind: 面向扩散模型的多概念遗忘系统	二等奖
“智感天盾”——无人机多模态探测与反制系统	二等奖
Sec-Protector: 基于大模型的多智能体系统密钥泄露检测工具	二等奖
SmartPatchAnalyzer: 基于大模型的二进制漏洞Patch对比与代码审计系统	二等奖
鹤迁云: 大模型驱动的开源库国产化迁移平台	二等奖
多协议动态化智能网联汽车异常流量检测系统	二等奖
MalGuard-大模型驱动的社交媒体恶意图像细粒度检测系统	二等奖
OS Agent 环境注入评估与防御平台	二等奖
MoLLaFuzz——基于LLaMA生成式大语言模型的工业协议漏洞挖掘	二等奖
CIBPU: 冲突不可见的安全分支预测单元	二等奖
绘隐鉴权-支持用户端预览的版权图像共享平台	二等奖
ChainSafeFort——灵鉴智能合约检测扩展中核	二等奖
基于动态交易网络的Web3恶意账户细粒度检测系统	二等奖
CallGuard: 面向实时语音通话场景的AIGC风险感知与主动防御系统	二等奖
隐士——面向隐私保护的智慧视觉系统	二等奖
暗流智瞳——基于 LLM 的 Tor 暗网流量未知威胁发现系统	二等奖
洞玄: 基于bert模型的固件漏洞检测系统	二等奖
LiteGuard: 基于高效单帧图像与时序残差分析的轻量级深伪检测APP	二等奖
基于Intel SGX的多层级动态可搜索加密系统	二等奖
基于潜在可分离性的模型后门攻击检测系统	二等奖
鉴影: 跨平台黑灰产溯源取证智能体	二等奖
HSRB-FL: 异构场景下安全鲁棒的区块链联邦学习系统	二等奖
大语言模型驱动的移动应用密码技术安全审计系统	二等奖
破影猎手——面向数字人视讯电诈的实时监测与预警系统	二等奖
隐私政策大语言模型多智能体系统	二等奖
ThreatHunter: 基于AI Agent的自主渗透和系统安全风险评估平台	二等奖
知识库与人工智能赋能的分布式入侵检测系统	二等奖
CodeSleuth: 基于代码风格指纹的软件供应链安全智能感知与溯源系统	二等奖

作品名称	奖项级别
声盾锁界——自适应录音屏蔽器	二等奖
基于哈希函数的后量子数字签名方案的国产化替代研究与应用	二等奖
ProtoMind——基于大模型的智能协议解析与自动化测试系统	二等奖
VulRator-基于模糊学习的函数级别漏洞挖掘和搜索模型	二等奖
基于大语言模型的威胁情报感知与安全防护引擎	二等奖
基于语义分析与混合神经网络的SQLi检测系统	二等奖
基于多模态Agent的工业异常检测平台	二等奖
鲸鱼——基于模型微调和知识蒸馏的恶意流量检测系统	二等奖
IVN-Defender：面向车内网络的分层入侵检测系统	二等奖
PrivScope:小程序隐私合规检测系统	二等奖
基于大模型反幻觉增强技术的代码漏洞挖掘系统	二等奖
音落留痕：基于口令猜测模型的键盘声学安全检测系统	二等奖
暗域密盾——Mindspore 赋能的四阶全互联细胞神经网络超混沌图像加密传输系统	二等奖
面向深度人脸伪造的肖像保护平台	二等奖
FALCON：基于大模型的多智能体工控固件漏洞检测系统	二等奖
DP-Shield：基于差分隐私的网络侧信道攻击防护系统	二等奖
“獬豸”：基于高效函数秘密分享的轻量级可扩展电子投票系统	二等奖
SpecProbe：面向处理器微架构安全的漏洞检测系统	二等奖
基于 SM4 加密的后量子投票系统	二等奖
支持流式轻量测量与多维扩散异常检测平台	二等奖
基于跨模态语义交互的社交媒体虚假新闻检测系统	二等奖
LLMMoat：面向大模型全链路的越狱攻击检测和防护系统	二等奖
AIGCTraceShield大模型生成内容溯源平台	二等奖

三等奖（88项）

作品名称	奖项级别
ICS-Aegis:基于多智能代理的工业控制系统自动化漏洞验证系统	三等奖
基于多源异构数据级联分析的黑灰产移动应用检测及其团伙挖掘	三等奖
Security-Coding Agent——基于静态分析和动态模糊测试的多智能体代码安全系统	三等奖
基于 AI Agent 和 LLM 的自动化漏洞修复系统	三等奖
RotorSpotter：无人机检测与定位轻量级系统	三等奖
“火感天眼”-基于异构感知与SAC强化学习的火场预警、逃生与救援系统	三等奖
PASVault：基于深度学习蜜加密技术的抗泄露口令管理器	三等奖
智盾哈希——基于深度哈希技术的恶意软件检测平台	三等奖
多模态水印辅助的智能驾驶风险警示鲁棒识别系统	三等奖
NeuroShield——面向硬标签场景的深度神经网络抗提取防御系统	三等奖
智盾图谱——基于知识图谱与大模型的软件组件安全智能管家	三等奖
青蓝洞见：师生协同的污点模式学习与引导式智能漏洞挖掘系统	三等奖
PassMind：大模型驱动的可演进口令强度评估系统	三等奖
AetherCTF：自进化智能体驱动的次世代CTF实训平台	三等奖
AxoraFL：基于区块链的安全高效联邦学习安全聚合系统	三等奖
智驾盾——基于鲁棒性安全联邦学习的云边端高效分心驾驶行为协同预警系统	三等奖
星零智御——基于零信任架构与联邦学习的抗量子卫星通信安全系统	三等奖
漏洞猎鹰VulnFalcon——精准漏洞根因定位系统	三等奖
图鉴天工——多功能遥感安全检测与应用平台	三等奖

作品名称	奖项级别
AudioDefender: 多任务学习驱动的音频伪造检测系统	三等奖
LLM-SecGuard: 基于多维心理学的大模型越狱安全评测平台	三等奖
PicGuard: 绘画图像的主动对抗防御扩散模型	三等奖
凌瞳——基于大语言模型的IPv6智能测绘与安全运维系统	三等奖
针对内容安全审核平台的可靠性评估系统	三等奖
“颜盾”——基于自学习扰动的图片隐私防护系统	三等奖
智盾隐投——基于门限环签名的抗量子攻击电子投票系统	三等奖
多模智盾: 多模态多场景的人工智能模型版权保护与评估平台	三等奖
高熵的物理层密钥生成及安全性评估	三等奖
基于阈值与混合行为分析的僵尸网络恶意域名检测系统	三等奖
面向内容理解的选择性图像加密系统	三等奖
“检密”密码算法正确性与一致性验证平台	三等奖
DeepTraceAudit 基于数据流和控制流的代码审计系统	三等奖
RAGFUZZ——基于大模型的第三方库自动化模糊测试系统	三等奖
深鉴真知——基于多模态对比学习的真实环境多媒体篡改检测系统	三等奖
AI卫士: 大模型的自动化评估平台	三等奖
基于虚幻引擎(UE)5的模拟现实类信息安全基础教育严肃游戏系统	三等奖
司法卫士: 裁判文书网大模型聚汇分析与辅助决策系统	三等奖
智护电网: 基于隐私计算的电力大模型预测系统	三等奖
灵析: 大模型协同的智能漏洞挖掘系统	三等奖
安全之钥——轻量级密码算法的唯密文故障分析软件	三等奖
大语言模型生成式安全自对齐训练评估平台	三等奖
MiniSentry——基于任务驱动的规避型恶意小程序检测系统	三等奖
面向服务与流量双重欺骗的弹性蜜罐防御系统	三等奖
VarColenc: 云端加密压缩键值存储的可变长度列式分包方案	三等奖
心电密码	三等奖
紫穹: 基于LLM的自动化渗透测试和漏洞修复系统	三等奖
面向自动驾驶远程劫持攻击的三级协同防御方案	三等奖
Deep Shield——基于FreqNet的AI伪造图像识别系统	三等奖
基于YOLO的图像敏感信息智能检测与掩盖系统	三等奖
护颜幻盾: 面向全生命周期的智能人脸信息保护平台	三等奖
量子云仓——基于后量子密码算法的文件加密存储系统设计与实现	三等奖
基于AIGC的构造式图像隐写算法设计与系统实现	三等奖
智翼空链——基于深度强化学习与后量子密码的eVTOL空域管理系统	三等奖
MASPom: 多智能体架构下大模型舆情监测与分析系统	三等奖
擎翼盾-MA: 无人机动态通信欺诈实时拦截系统	三等奖
AI换脸风险预警	三等奖
DomainGuard: 恶意域名实时检测系统	三等奖
SQLXGuard: Web下的SQL哨兵	三等奖
基于容错预约束的环链端到端加密监管通讯系统	三等奖
基于跨模型通用对抗水印的人脸图像保护微信小程序	三等奖
面向动态网页的Web漏洞扫描器的研究与实现	三等奖
云驿密匣——基于鸿蒙系统的国密邮件安全传输系统	三等奖
NetDefender——基于深度学习的恶意流量智能检测平台	三等奖
基于语义解耦的联邦式隐私音频伪造检测系统	三等奖
LLM-GUARD: 面向线上大语言模型的多模态数据保护系统	三等奖
智链鹰巡: 基于可信分片区块链和强化学习的多无人机自主协同控制系统	三等奖
VoiceGuard——多模型韵律保持语音防护系统	三等奖

作品名称	奖项级别
ShareScanAgent:基于大模型Agent的共享隐私检测系统	三等奖
AndroAnalyzer: 基于图表示学习的安卓恶意软件检测系统	三等奖
洞玄: AI Agent驱动的智能系统安全风险评估平台	三等奖
基于 YOLO11 与 LSTM-T-AKF 融合的无人机隐私保护与抗欺骗系统	三等奖
面向流媒体语音的高效隐写分析系统	三等奖
限时可验和高效的安全数据检索系统	三等奖
IPv6网络安全态势感知与漏洞治理可视化平台	三等奖
基于耳道内提取心音的身份认证系统	三等奖
抗量子可扩展SM4国密算法的FPGA优化实现	三等奖
量子方舟——面向PQC迁移的混合证书签发和验证系统	三等奖
智链安盾——基于链式思维与反馈闭环的代码漏洞智能修复系统	三等奖
智瞳安网——基于设备指纹的以太网终端接入识别系统	三等奖
智能电网中隐私保护的用户参与式细粒度电器级需求响应系统	三等奖
智能网联车辆动态行驶场景下密钥自主生成系统	三等奖
骨振识息: 基于头部接触响应的智能用户认证系统	三等奖
动态可伸缩的FPGA可信机密计算环境	三等奖
“心安私语”——基于分级加密的多模态智能体隐私防护系统	三等奖
“灵哨”大模型安全检测平台	三等奖
瞳驭——高速公路场景下多模态感知与实时预警系统	三等奖
基于TCM安全芯片的可信内容发布与防篡改系统研究	三等奖
Secure Cloud——安全存储与可靠计算云平台先行者	三等奖

优胜奖 (146项)

作品名称	奖项级别
智核——基于强化学习的轻量级物联网PUF身份认证系统	优胜奖
基于差分隐私的联邦时序集成医学分割模型	优胜奖
摄界经纬——拍摄地智能识别与连续定位系统	优胜奖
御安慧瞳-软件漏洞智能检测与分析平台	优胜奖
医影智链——区块链赋能的医学影像安全存储与共享系统	优胜奖
LogAPT: 面向日志的APT检测与链路溯源系统	优胜奖
智鉴·云盾——基于深度学习的恶意代码检测系统	优胜奖
面向工控网络的小样本生成与入侵检测系统	优胜奖
DynASR——基于图表示学习的多阶段攻击行为耦合检测与动态场景重构系统	优胜奖
M2X-Guard:基于多引擎协同与多模态数据融合的XSS检测系统	优胜奖
数囊信舱——基于数据对象的政务可信数据空间构建	优胜奖
基于负数据库的隐私保护脑电波识别系统	优胜奖
闻声识机——开集环境下手机型号鉴别系统	优胜奖
SVD-GAN驱动的区块链交易异常检测系统	优胜奖
碳链宝: 基于联盟链与Agent的碳市场全流程保护与交易平台	优胜奖
图片防篡改及水印生成检测系统	优胜奖
智界-深度学习模型隐私风险评估与安全防御系统	优胜奖
基于同态加密与双CA信任架构的车联网联邦学习安全增强方法	优胜奖
基于深度学习的网络攻击检测系统	优胜奖
火眼金睛——多模态视频篡改检测与定位系统	优胜奖
基于谓词加密的分布式无人机群组安全通信系统	优胜奖
SafeGuard: 融合数据增强和对比学习的异常流量识别平台	优胜奖
玄鉴: 基于选择性状态空间模型的恶意流量分类系统	优胜奖
轻量级跨平台动态可搜索加密数据库系统	优胜奖

作品名称	奖项级别
基于联邦安全的工业互联网DDoS防护系统	优胜奖
面向流媒体平台的递进式恶意域名挖掘系统	优胜奖
基于小型机器狗的信息安全多维动态防护系统设计与实现	优胜奖
ConfGuard: 基于置信度过滤与DistilBERT的CAN总线入侵检测系统	优胜奖
寰驭通安——基于国密周期性可否认环签名方案的车联网溯源平台	优胜奖
智控模测: 融合语言模型与物理感知的工业协议模糊测试框架	优胜奖
枢阵隐私-基于隐私计算的数据共享平台	优胜奖
支持双重版权保护的结构化数据水印平台	优胜奖
极速木马猎手: 轻量化远程访问木马早期检测与终止系统	优胜奖
「智镜·无垠」——基于知识图谱与DeepSeek 的全维度反诈中枢	优胜奖
支持多模态的大模型安全等级评测与加固系统	优胜奖
御网天鹰——全流量驱动的大模型自动化漏洞挖掘系统	优胜奖
基于大语言模型的自动代码修复工具设计与实现	优胜奖
面向向量数据库的自适应数据水印系统	优胜奖
密算智行: 基于安全多方计算和低秩矩阵分解的路况预测系统	优胜奖
ImageGuard: 基于SRE-LICM算法的图像隐私保护系统	优胜奖
DeepTestX: 基于大语言模型的深度学习库智能模糊测试系统	优胜奖
隐私防护者, 基于双混沌系统的数据安全防护系统	优胜奖
双模态 CoT 后门: LLM/VLM 具身智能的知识图谱增强攻防	优胜奖
智安御灾——基于多模态隐私安全联邦学习的自然灾害跨域协同预警系统	优胜奖
基于LightGBM的抗翻录鲁棒水印系统	优胜奖
D&S IoT-基于动态函数级模糊测试和静态分析的物联网漏洞发现系统	优胜奖
面向人脸定制化生成模型的主动防御系统	优胜奖
御网苍穹-基于机器学习的无人机集群网络入侵检测	优胜奖
车联网协同式异常检测系统: 联邦学习架构下的高精度入侵防御与隐私保护	优胜奖
棱鉴——基于深度学习的AIGC图像鉴别和篡改识别溯源系统	优胜奖
智鉴先锋——基于大模型智能体的音视频内容风险智能分析系统	优胜奖
散钥于众, 聚信于签——基于口令防护的门限盲化钱包方案	优胜奖
Fenrir-基于MCP的自动化代码审计工具	优胜奖
基于大模型技术的软件漏洞全流程管理	优胜奖
基于加密QR码的快递隐私分级保护系统	优胜奖
GUIAgent安全评测平台	优胜奖
基于全同态加密的去中心化肺炎识别系统	优胜奖
基于入侵检测技术与混合Transformer的智能网络安全防护系统	优胜奖
基于关联数据具有自主身份属性约束的选择性披露凭证	优胜奖
匿查查——基于PEPSI的恶意文件共享检测系统	优胜奖
面向车联网的高效且安全的联邦学习系统	优胜奖
智能网络安全实训云平台	优胜奖
多模态谣言检测系统	优胜奖
基于BERT和Deepseek-r1改进的大语言模型防御器	优胜奖
区块隐锋-抗关联生成式区块链隐蔽通信系统	优胜奖
et3	优胜奖
Android应用程序隐私合规检测系统	优胜奖
日新钥异: 长期服役物联网安全无线密钥生成系统	优胜奖
毓秀智骨平台——基于AES的加密通信与双向认证的Cobb角测试系统	优胜奖
《面向移动车联网的匿名凭证认证系统》	优胜奖
基于国密SM9的通用身份认证与加密通信系统	优胜奖

作品名称	奖项级别
ICDefender: 面向工业控制流网络的小样本生成与检测系统	优胜奖
AegisCode——上下文感知驱动的项目级安全增强代码自动生成系统	优胜奖
ECU-SecCom: 车载ECU安全通信系统	优胜奖
QQQDefender: 低成本高效发展的分布式恶意软件检测系统	优胜奖
ETGuard: 电网智能终端设备威胁狩猎系统	优胜奖
基于ECDH算法的无人机安全通信系统	优胜奖
云盾慧眼	优胜奖
轻量级入侵防御系统	优胜奖
睿眸-智能恶意威胁分析系统	优胜奖
零落盘动态执行远程运维引擎	优胜奖
IntelliFuzz-NLP: 基于模糊测试的智能自然语言处理系统测试平台	优胜奖
基于模糊测试的智能合约漏洞检测系统	优胜奖
声鉴未来——电信反诈智能平台	优胜奖
LSTC: 基于半全局三角中心的网络暴力溯源与预警平台	优胜奖
护城卫士——基于联邦学习的城市安防智能分析平台	优胜奖
视界增强——基于对抗训练的目标检测模型鲁棒性强化系统	优胜奖
云御安途: 基于CPABE的云边多网抗合谋多权威加密系统	优胜奖
基于扩散模型的可恢复图像安全保护系统	优胜奖
基于强化学习的大语言模型安全对齐方法	优胜奖
基于混合专家模型的大模型评估系统	优胜奖
伪装者-射频指纹识别攻防研究与实现	优胜奖
慧语星枢——基于提示词工程的二进制漏洞检测平台	优胜奖
基于联邦深度学习和同态加密的疾病诊断医疗系统	优胜奖
玄壁——Linux主机安全防护平台	优胜奖
基于CNN-TCN-Attention混合神经网络的新型入侵检测系统	优胜奖
“清风”智能新闻鉴伪平台	优胜奖
安驰星盾: 基于自适应多模态网络入侵智能分析平台	优胜奖
加密通信应用程序	优胜奖
密网绘途——基于联邦学习的地图数据隐私保护与安全共享系统	优胜奖
X-Comp: 移动应用隐私合规实时测评系统	优胜奖
“海空之眼”——基于风光互补的水空协同海洋牧场安全监测平台	优胜奖
源御——基于iOS的移动网络入侵检测系统	优胜奖
基于光学编码与混沌加密的高安全性数据传输系统	优胜奖
基于C/S架构的用户上网行为管控平台	优胜奖
医域智穹——隐私协议语义感知的医疗数据可信中枢	优胜奖
高效隐私盾: 机器遗忘架构ForgetSys-Pro	优胜奖
青铜链脑 FuzzOrb: 融合模糊测试与AI大模型分析的智能合约守护系统	优胜奖
基于大模型技术的漏洞静态分析自动化工具	优胜奖
一验万年——公开可验证的同态数据封装机制隐私计算服务平台	优胜奖
御音卫士——基于组合防御的智能座舱语音对抗防御系统	优胜奖
一种无监督式的深度伪造检测系统	优胜奖
“棱镜守护” 动态访问控制加密·指纹盾	优胜奖
隐心智链: 基于匿名加密与大模型的心理守护平台	优胜奖
“狡狴”——文生图场景下的内容安全守护神兽	优胜奖
面向工业物联网的跨平台可信数据管理与安全预警系统	优胜奖
VisionGuard AI——多模态图像真实性智能检测系统	优胜奖
LLM-Guardian: 大语言模型安全评估系统	优胜奖
智谱芯界 (GuardGLM): 基于国产大模型的多应用隔离防护系统	优胜奖
凌悟RAG智慧引擎——大模型幻觉缓解方案	优胜奖

作品名称	奖项级别
鉴真——面向中文语义的跨模态新闻伪造检测平台	优胜奖
Falcon: 基于路径敏感稀疏分析的供应链漏洞挖掘系统	优胜奖
地脉舆擎——基于复杂网络的事故舆情监控系统	优胜奖
火焰越权漏扫系统	优胜奖
天盾-智能反恐侦察车	优胜奖
基于国密算法的CA认证中心	优胜奖
同态加密下的多模态安全融合分析系统	优胜奖
幻彩织影——基于语义引导的双重伪装迷彩	优胜奖
ATWatch: 基于动态图神经网络的金融异常检测系统	优胜奖
抗量子安全导向的多域标识认证与用户可追踪机制研究	优胜奖
玄鉴-MirrorNet: 区块链赋能下的网络安全事件记录分析服务系统	优胜奖
共鉴——抗恶意干扰的多无人机协作感知安全系统	优胜奖
VeriFace: 基于多模态融合的抗Deepfake攻击身份认证系统	优胜奖
融合威胁情报与多智能体的网络入侵检测系统	优胜奖
PDM&Fuzz: 基于扩散模型的协议漏洞自动化挖掘系统	优胜奖
AeroTrust AI 航材智能溯源链	优胜奖
面向无人机的“云-网-端”数据安全审计协议研究	优胜奖
按图索骥、逐影溯源——视觉媒体溯源取证平台	优胜奖
跨模态语义融合的虚假新闻检测与取证系统	优胜奖
隐询智索——抗泄漏的多模态隐私查询系统	优胜奖
潜痕——面向AIGC的水印版权维护平台	优胜奖
基于无害化后门的RAG数据库水印技术	优胜奖
VeriDome——多模态深度伪造内容检测系统	优胜奖
VulTracer: 基于大模型提示词增强的源代码漏洞检测系统	优胜奖
智鉴——基于多模态大模型的深度伪造图像检测系统	优胜奖
基于大语言模型的智能化漏洞检测与分析系统	优胜奖

第十八届全国大学生信息安全竞赛作品赛组委会
西安交通大学网络空间安全学院

2025年8月16日

