

第十七届全国大学生信息安全竞赛-作品赛

决赛作品获奖名单

一等奖（48项）

作品名称	奖项级别
基于前缀引导的安全强化代码自动补全系统——SafeCoder	一等奖
大模型驱动的海量文本敏感信息检测系统	一等奖
基于GPS诱骗的无人机主动防御技术探索	一等奖
LeakSpy:数据贩卖平台主动感知与追溯系统	一等奖
基于双向情感与群体认识的网络暴力演化分析系统	一等奖
脉动声息——基于声学传感的智能用户认证系统	一等奖
信链：基于可编辑区块链的数据监管平台	一等奖
基于后门水印的可溯源联邦模型多方授权系统	一等奖
AuthLink：跨移动应用认证安全风险检测系统	一等奖
ImGuardian——面向社交媒体的AI生成图像风险感知，评估与监测系统	一等奖
安疆：针对恶意信号源的无人机移动测向与定位系统	一等奖
P-Oracle: 基于机器学习的协议安全性自动化分析平台	一等奖
GungnirFuzz: 基于深度强化学习的SDN控制器漏洞挖掘系统研究与实现	一等奖
御鹰——对抗传感器攻击的自主定位系统	一等奖
FakeX: AIGC图像检测与模型溯源平台	一等奖
VoxTracer:基于变分可逆神经网络的说话人溯源系统	一等奖
WASanitizer: 面向webassembly二进制的检测系统	一等奖
RKEGuardian: 自适应跳频技术增强的RKE安全通信系统	一等奖
净面——网站追踪实时检测与拦截系统	一等奖
重明之眼——基于大模型和多模态的后门检测系统	一等奖
基于开源情报的Web后门检测系统	一等奖
ScopeChecker-超级应用API-Scope错位检测系统	一等奖
鹰眼监察：非法无人机与飞控手的监管定位系统	一等奖
链安卫士：软件供应链漏洞检测系统	一等奖
VMForce：一种针对虚拟化混淆恶意软件的强制执行技术	一等奖
面向低功耗蓝牙设备的漏洞挖掘系统	一等奖
白泽护航--面向交通法律法规的无人驾驶系统自动化合规测试平台	一等奖
IntelliTracer: 生成式大模型版权保护与用户溯源服务	一等奖
字里乾坤——AIGC文本多比特水印系统	一等奖
基于社交网络图像的稳健隐蔽通信方法与系统	一等奖
隐秘OCR: 基于特征熵增与底纹补丁的图像文字信息保护系统	一等奖
WebInsight FusionMap: 动静全域网站测绘系统	一等奖

作品名称	奖项级别
DecoupleGuard——基于良性特征解耦的可靠后门防御系统	一等奖
ChannelEudemon——移动环境下基于ESP32嵌入式平台的对称无线信道密钥生成	一等奖
FreeGait: 基于无约束步态识别的身份认证系统	一等奖
安网驭行: 融合机器学习的多模式智能网联汽车入侵检测系统	一等奖
miniAuthX-小程序身份认证漏洞检测系统	一等奖
雾云存储中密物联网数据的去重存储与近似分析	一等奖
面向零信任安全的生成式威胁推断与验证系统	一等奖
基于深度学习与多模态融合的虚假短视频综合检测系统	一等奖
"独犴"——基于图神经网络的硬件木马检测系统	一等奖
PassInfinity: 基于可组合泛化知识的新型在线认证系统	一等奖
智耳: 智能无线网络安全监测与主动对抗系统	一等奖
星鉴——支持多域多模型的中文机器生成文本检测系统	一等奖
“窥盔”——基于高低频分离和隐私边缘隐藏的手机文件防窥系统	一等奖
基于图表示学习的区块链交易安全保护系统	一等奖
NoGPT-基于PPL和对数曲率的AI文本检测平台	一等奖
PinpointProbe: 面向匿名通信网络的跨域小样本网站指纹识别系统	一等奖

二等奖（72项）

作品名称	奖项级别
基于有限状态机的QUIC协议指纹识别系统	二等奖
数链金安: 基于数字身份与分片区块链的普惠金融隐私保护方案	二等奖
芯盾智防: 基于机器学习的鲁棒性硬件木马检测系统	二等奖
MyDataBase: 隐私保护的安全可验证外包数据库	二等奖
智盾幻绘——基于对抗攻击的FPS游戏反AI作弊系统	二等奖
HateSentry——基于大模型的多模态网络仇恨检测系统	二等奖
基于大模型RAG与Prompt的安全策略编排及智能响应系统	二等奖
EIGuard: 边缘智能场景下侧信道安全分析与加固系统	二等奖
面向QUIC的请求伪造攻击仿真与防御验证系统	二等奖
面向社交媒体的在线多模态谣言检测系统	二等奖
TrustVault: 基于ARM TrustZone的嵌入式加密数据库解决方案	二等奖
基于步态识别的无人机送货双向认证系统	二等奖
基于信息隐藏的分布式无人设备高效协同认证与蜜罐防御系统	二等奖
泽言: 面向人机协同的社交网络群体检测及意图识别系统	二等奖
以静制动: 静态物联网稳健动态无线密钥生成系统	二等奖
PRO-Face: 跨场景人脸视频隐私保护系统	二等奖
人脸图像防篡改水印生成器——一种基于对抗攻击的人脸图像主动保护系统	二等奖
问卷安——基于本地化差分隐私的安全问卷系统	二等奖
FortressHealth-PBFL: 强固隐私的联邦辅助诊断云平台	二等奖
溯防智印——支持溯防一体式版权保护的对抗水印系统	二等奖

作品名称	奖项级别
PrivTuner: 基于联邦学习的隐私保护语言模型个性化微调系统	二等奖
VidTrace: 面向AIGC新型威胁的短视频侵权行为识别与检测系统	二等奖
IntelliSimuPot——融合虚拟内存和工业过程仿真的可扩展高交互智能化动态响应蜜罐系统	二等奖
面向防AI伪造的音频扰动与签名水印系统	二等奖
Fed Privacy Shield	二等奖
SPLM:大模型与主动免疫赋能的V2G安全预警平台	二等奖
多元语音攻击智能检测系统	二等奖
融合个人信息与口令重用的口令验证系统	二等奖
ByzantineVK---基于鞅理论的抗投毒拜占庭鲁棒联邦学习平台	二等奖
“边城”——面向复杂对抗环境的多维密态数据采集与统计系统	二等奖
面向应急救援智能无人系统的安全跨域远程操控系统	二等奖
支持动态隐私溯源的分布式门限签名系统	二等奖
GrangeeSense:基于格兰杰因果关系的隐藏物联网设备识别系统	二等奖
基于Wi-Fi信号的人员感知与行为检测平台	二等奖
基于隐私水印对大语言模型生成文本的辨识与确权	二等奖
基于CKKS算法的人脸识别隐私保护方法	二等奖
大语言代码模型赋能开源物联网软件安全测试平台	二等奖
基于量子密钥分发的卫星电话嵌入式安全认证与通信系统	二等奖
语镜——面向可信LLM的安全风险检测与防御系统	二等奖
面向SM4加密算法的侧信道防护方案	二等奖
医数通——基于分布式增量可验证计算的医疗数据交付方案	二等奖
天镜智盾: 基于时序不一致性的恶意伪造检测系统	二等奖
融合量子密钥的IPSec VPN数据安全传输平台	二等奖
“隐秘哨兵”——基于eBPF与多模态大模型的安卓隐私泄露检测报警系统	二等奖
DeepShield (深盾): 鲁棒人脸伪造检测系统	二等奖
匿名安全和强追溯的分布式数字取证系统	二等奖
ZUC-256高性能安全软件实现及应用	二等奖
智合——基于数据胶囊概念的自动化隐私合规检测系统	二等奖
基于大语言模型纠错的不良短消息识别系统	二等奖
火眼金睛——面向内容安全的变体文本即时处理工具	二等奖
”蓝盾“——基于蓝牙嗅探与深度学习的非法蓝牙侦测与风险评估系统	二等奖
针对短视频平台的谣言视频检测系统	二等奖
ERASER: 面向多模态数据的隐私遗忘系统	二等奖
AlchemyShield: 面向文生图模型的艺术风格保护系统	二等奖
守护视界——基于强化学习的音视频暴力行为检测与主动跟踪系统	二等奖
面向Web接口的物联网设备固件漏洞自动分析系统	二等奖
AVID: 基于Inverse Diffusion的AI生成图像鉴别与溯源系统	二等奖
WeVote:基于区块链的自统计加权投票系统	二等奖
基于概念漂移识别的网络入侵检测系统	二等奖

作品名称	奖项级别
Palette——基于流量群匿名化的实时指纹攻击防御系统	二等奖
互联网用户侧资源注入潜在威胁与可感知性量化评估工具	二等奖
国产大模型驱动的智能合约生成、检测及修复一体化平台	二等奖
面向WebAssembly的网络端深度学习模型防御技术	二等奖
KRSFinder：基于字节码的混淆对抗与污点传播分析系统	二等奖
密码之芯：轻量级密码安全性分析与检测系统	二等奖
面向机器学习的后门攻击评测系统	二等奖
追本溯源——面向大语言模型生成内容的水印版权保护系统	二等奖
隧视——基于增量集成学习的恶意 DoH 隧道可解释检测系统	二等奖
面向V2G网络支持匿名支付的隐私认证系统	二等奖
LLM生成文本检测器	二等奖
基于遮挡增强步态识别的多模态智能安防系统	二等奖
“WIFI神探”-基于无线信道特征的盗版 WIFI 鉴定器	二等奖

三等奖（96项）

作品名称	奖项级别
基于随机神经网络的数据隐私保护的分布式训练系统	三等奖
智联联邦——基于增量联邦学习的流量攻击检测系统	三等奖
玄武智卫——基于云边端协同的无人智能设备安全管控系统	三等奖
寻声聚力——全方位舆情监测与态势感知系统	三等奖
基于对比迁移的物联网固件第三方组件漏洞分析	三等奖
基于深度学习的以太坊智能合约漏洞检测	三等奖
烽火轮：基于智慧交通ATT&CK知识库的车联网安全态势感知与防御系统	三等奖
芯盾：面向硬件木马检测的硅前安全评测EDA工具	三等奖
MPCTensorLib——面向深度神经网络的轻量级安全多方计算平台	三等奖
基于国密算法和生物特征认证的安全智能锁钥系统	三等奖
AntiTrolls——基于LLM和知识图谱的代理软件溯源与分析平台	三等奖
“MediSCI”——面向远程医疗的新型可逆隐写增强系统	三等奖
周全-基于“ML”+“规则”双擎驱动的数据库防火墙-蓬莱防火墙	三等奖
SPARSE：融合语义跟踪与路径分析的高级持续性攻击溯源系统	三等奖
“传语报安”——基于声纹识别的实时身份验证系统	三等奖
基于特征图建模和胶囊网络的恶意软件分析系统	三等奖
星网迷踪——面向OSN的基于鲁棒秘密分享的隐私图像保护方案	三等奖
HeadSonic：基于骨传导耳机的高效安全身份认证系统	三等奖
妙眼-基于Diffusion的图像识别对抗样本净化系统	三等奖
DiffMark：针对扩散模型的图像确权与溯源水印系统	三等奖
信创环境下的云中心安防系统	三等奖
DeepSentry:面向实时通信诈骗的深度伪造检测防御系统	三等奖
云端电子数据完整性审计系统	三等奖

作品名称	奖项级别
PCP: 基于隐私保护的高效的人脸识别系统	三等奖
基于国密算法和同态加密的安全人脸识别系统	三等奖
Beyond: NLP 软件测试与安全性增强系统	三等奖
基于注意力的VIT后门防御平台	三等奖
在线社交媒体虚假信息检测与抑制原型系统	三等奖
深度强化学习安全测试系统	三等奖
基于随机森林和bilstm的恶意流量检测系统	三等奖
Cognition Sentinel:基于动态协作检测的大模型驱动式社交平台认知对抗感知系统	三等奖
幽影停泊—基于国密的ZK-AVP远程泊车导引系统	三等奖
火眼金睛——AIGC时代全媒体深度伪造检测系统	三等奖
“Guardian”安防设备安全认证平台	三等奖
面向异构环境的双网络联邦工控入侵检测系统	三等奖
FalconGuard-抗Deepfake和LLM增强的虚假内容检测系统	三等奖
GuardNTRU: 基于NTRU的后量子抗性区块链安全交易系统	三等奖
隐私卫士: 端到端的可定制化流数据密文访问控制系统	三等奖
面向社交平台的多模态深度伪造检测系统	三等奖
基于联盟链与联邦学习的医疗数据管理平台	三等奖
智飞卫士-实时无人机GPS欺诈检测系统	三等奖
基于区块链和代理重加密的文件访问控制系统	三等奖
智链安居: 基于区块链的环签名与门限ElGamal加密信息治理平台	三等奖
UnVoiceClone: 面向生成式伪造语音欺骗的鲁棒主动防御系统	三等奖
Intrusion Insight—基于域适应的车联网入侵检测系统	三等奖
IntelliFuzz-基于LLM的智能模糊测试系统	三等奖
面向第三方SDK的隐私透明度提升工具	三等奖
基于保护窗口的实时安全调度方法	三等奖
面向机器学习的 CKKS-RNS 同态算子芯片设计	三等奖
真相守卫——面向Deepfake的多模态融合检测系统	三等奖
基于LLM的漏洞检测和蜜罐防护系统	三等奖
基于贝叶斯近似的高性能恶意隐写载体检测系统	三等奖
TextGuard-多线索自适应学习的文档图像伪造检测系统	三等奖
基于国产可信硬件和国密算法的机密计算平台	三等奖
基于非接触式掌纹识别的移动端大规模人群身份认证系统	三等奖
BCWatch: 基于图表征学习的区块链异常交易检测系统	三等奖
面向Web3.0恶意交易的高效地址关联系统	三等奖
M-RFF: 下一代移动通信射频指纹身份认证系统	三等奖
基于无透镜成像的人脸识别系统	三等奖
灵眸—基于多通道并行检测的综合图像鉴伪系统	三等奖
基于编码树的频率隐藏保序加密方案及其在密态数据库中的应用实践	三等奖
BinLLM:基于大语言模型的二进制代码漏洞检测系统	三等奖

作品名称	奖项级别
基于图像自然随机性特征的联邦取证分析系统	三等奖
面向IoT设备的动静态混合自动化漏洞挖掘工具	三等奖
CbWAF: 基于CatBoost机器学习的WAF设计与实现	三等奖
“轻隐”-基于对抗扰动迁移性的图像隐私保护方法	三等奖
当AI遇上侦探! 面向AI生成内容的多模态检测系统	三等奖
BlockSafeShield——基于智能合约生成的可扩展漏洞检测与防护系统	三等奖
GnnShin: Few-Shot场景下基于GNN的源码漏洞检测系统	三等奖
基于改进 YOLOv9 的智能网联汽车图像脱敏系统	三等奖
基于联盟链的PKI证书系统设计与实现	三等奖
基于近似查询合成的DBMS的缺陷检测系统	三等奖
基于持续学习的恶意软件检测系统	三等奖
当伊芙来敲门——后量子密码算法的侧信道辅助的选择密文攻击	三等奖
Taint-Fuzz:基于混合分析的二进制算法复杂性漏洞自动化挖掘系统	三等奖
“智语护航”——基于红队测试与算术安全校准的大模型防护体系	三等奖
“智能护盾”: 基于黑盒水印和图像感知哈希的DNN版权保护与溯源系统	三等奖
SecCredit-模型隐私保护的高性能小微企业信贷风险评估系统	三等奖
云治安-基于云边协同和深度学习的被动WIFI跟踪检测系统	三等奖
工业互联网口令盒子——基于SM3算法的批量动态强口令生成与管理系统	三等奖
恶码侦探——恶意软件分析与取证系统	三等奖
基于秘密共享的医疗数据保护平台的设计与实现	三等奖
基于噪声残差和平均光流模式的深度视频修复被动取证系统	三等奖
动影追踪者——视频来源鉴别系统	三等奖
后门寻踪-面向恶意软件检测深度神经网络的后门攻击漏洞挖掘	三等奖
擎源——面向信创软件的开源代码漏洞治理系统	三等奖
“御语守界”: 基于CodeBert的代码漏洞分析和修复建议平台	三等奖
基于生成式文本隐写术的隐私通信保护工具	三等奖
基于伪随机数生成器的轻量级门限签名方案	三等奖
政务加密链——数据共享与信息检索隐私保护系统	三等奖
PhasedDefender——面向联邦学习投毒攻击的分阶段可视化防御系统	三等奖
云图密语--基于理想缩略图保持加密的图像共享平台	三等奖
基于帧级注意力的跨语种深度伪造音频检测系统	三等奖
ProtoGuard:工控协议的安全哨兵	三等奖
基于嵌入式的噪声源随机性实时检测模块	三等奖
态势感知智慧平台	三等奖

优胜奖 (138项)

作品名称	奖项级别
基于语言无关特征和LLM融合的开源组件投毒检测	优胜奖
基于物理网络的分布式加密系统	优胜奖

作品名称	奖项级别
多模态融合的信息窃取行为分析与预警系统	优胜奖
EtherGuardian: 以太坊匿名账户智能追踪与链上交易监管系统研究与实现	优胜奖
网络安全图谱及智能推演平台	优胜奖
音真探源--语音深度伪造泛化性检测与算法溯源系统	优胜奖
TKACG-APT攻击检测与溯源系统	优胜奖
基于DFA压缩算法的100Gbps实时网络安全检测系统	优胜奖
GoShield-面向开源Go应用的自动漏洞修复系统	优胜奖
“智联安行”—基于机器学习的智能网联汽车安全通信系统	优胜奖
基于联邦学习概念漂移下的网络加密公害流量识别终端	优胜奖
Sphinx——基于触摸振动信号的用户认证系统	优胜奖
心室守护—医学数据全生命周期隐私保护解决方案	优胜奖
基于时间图模型的横向移动攻击检测与预测系统	优胜奖
基于双机制联邦学习的网络异常流量检测系统	优胜奖
漏洞智探——基于LLM的软件漏洞检测系统	优胜奖
AMALA: 一种基于拉格朗日四平方和定理的分组密码加密算法设计与应用	优胜奖
基于人脸识别的安全访客系统	优胜奖
OTD-多源多端公共服务站点隐匿不良信息检测系统	优胜奖
“极零”—基于零信任的云计算资源细粒度动态防护系统	优胜奖
基于可信执行环境的数据同态加密传输方案	优胜奖
OpenFort-面向开源软件安全的分析评估系统	优胜奖
“指纹无痕”: 基于零知识证明与区块链的隐匿指纹认证系统	优胜奖
基于区块链的隐私保护群组密钥管理与服务推送系统	优胜奖
基于加密图像的大容量可逆数据隐藏系统	优胜奖
基于后量子密码Kyber的通信系统	优胜奖
基于CV-QKD的量子安全视频通信系统	优胜奖
基于RLWE的同态密码加速器设计与实现	优胜奖
基于浅深层特征融合的合成音频水印系统	优胜奖
Aegis: 以太坊实时交易检测预警系统	优胜奖
AutoSVT: 极端天气下的自动驾驶预期功能安全测试平台	优胜奖
MC2F—基于多通道特征融合的缺陷检测系统	优胜奖
ScanMal: 跨平台恶意软件智能溯源与关联取证系统	优胜奖
THOR: 基于零信任的恶意二维码实时检测系统	优胜奖
基于白盒SM4混合同态加密的数据库透明代理系统	优胜奖
基于白盒加密水印技术和Res2Net的声纹识别认证系统	优胜奖
全流量驱动的Web漏洞智能挖掘及验证系统	优胜奖
守望漏洞检测及验证工具	优胜奖
獬豸: AIGC文本风险检测与溯源系统	优胜奖
基于检索增强的通用大模型智能合约漏洞检测	优胜奖
智信先锋——基于RepVGG-SimAM的多特征卷积图不良信息监测系统	优胜奖

作品名称	奖项级别
DataForge: 面向产业数据共享的关键信息脱敏系统	优胜奖
PDFWhisper—基于PDF科学文献的隐蔽存储系统	优胜奖
MalwareCipher: 面向加密流量的智能恶意检测系统研究与实现	优胜奖
“智链共联，医溯未来”——基于属性基加密的医疗数据细粒度协作共享方案	优胜奖
基于二值神经网络的联邦学习系统	优胜奖
链医联邦: 隐私保护的多机构鲁棒医疗数据联邦分析系统	优胜奖
面向数据异构和数据安全的城市监控体系架构	优胜奖
DermAI——结合Vision Mamba与跨域知识迁移的隐私保护皮肤疾病智能识别系统	优胜奖
基于蜜加密的口令管理器	优胜奖
面向网络异常监测的DGA域名AI识别方法与系统	优胜奖
Zapper: 简洁低交互的物联网设备互联认证协议	优胜奖
基于射频指纹识别的物联网设备认证系统	优胜奖
基于同态加密的可搜索密文生物认证系统	优胜奖
基于安全多方计算的分布式差分隐私数据合成平台	优胜奖
基于数字水印与SM2的在线链上图片交易与确权系统	优胜奖
基于区块链技术的医疗安全护盾系统	优胜奖
TouchSec: 基于触控手势的身份认证系统	优胜奖
白泽RASP: 基于RASP的Web应用漏洞治理平台	优胜奖
车行智安-面向隐私保护的车联网安全防御系统	优胜奖
智链安全—基于区块链与人工智能的身份认证系统	优胜奖
克隆音频检测逃逸攻击系统	优胜奖
保护隐私的金融风险评估助手	优胜奖
基于图分析的CAN消息异常检测系统	优胜奖
局部内容感知图像数字水印工具: 盗摄攻击下图像的版权保护和追溯	优胜奖
基于联邦学习的网络攻击检测	优胜奖
可信机密虚拟机系统研制	优胜奖
路网卫士—车联网女巫攻击检测与溯源系统	优胜奖
基于Paillier的时控性同态加密电子投票系统	优胜奖
TouchSecureX: 基于压感的指纹解锁	优胜奖
基于量子噪声流的微波光子内生安全系统	优胜奖
PassLLM—基于 LLM 的口令强度评价和解释系统	优胜奖
协同智盾漏洞扫描工具	优胜奖
HybridGuard: 面向机器人操作系统的分布式隐私保护方案	优胜奖
基于多特征融合的区块链异常检测与可视化分析系统	优胜奖
金智FinGuard—基于Paillier的金融数据安全多方计算系统	优胜奖
文心智安——基于文心一言的异常安全日志智能分析插件	优胜奖
基于深度语义特征遗传优化的指纹活性检测算法	优胜奖
云密宝盒-云计算下密态数据安全交换与共享的领航者	优胜奖
助力大语言模型的隐私感知样本生成工具 - 基于自适应梯度剪切的隐私保护样本生成系统	优胜奖

作品名称	奖项级别
基于云服务器与内核技术的远程协同防泄露办公系统	优胜奖
基于函数生成的新型图像隐写算法	优胜奖
智图锁：基于深度平衡离散哈希的选择性图像加密系统	优胜奖
安智守望--基于信创环境的智能安全监测与响应系统	优胜奖
基于水印嵌入的强安全密钥掌纹识别方法及实现	优胜奖
基于区块链和非交互式零知识证明的版权管理系统	优胜奖
商用密码应用安全性评估工具设计与实现	优胜奖
基于隐私保护的联邦框架赋能城市电网安全	优胜奖
面向医疗数据的隐私保护数据分类算法的设计与实现	优胜奖
智联卫士—深度神经网络驱动的物联网恶意软件检测系统	优胜奖
勒索病毒的检测及文件还原系统	优胜奖
面向推荐系统的异常内容检测与舆情管控系统	优胜奖
融合大模型的恶意流量检测诊断系统	优胜奖
基于社会背景的短视频平台新闻检测系统	优胜奖
基于R-LWE的车联网抗量子聚合签名方案	优胜奖
基于图匹配网络的二进制软件漏洞检测系统	优胜奖
千秋印记，守护每一道契约	优胜奖
基于大语言模型和容器投毒检测技术的个性化网络靶场平台	优胜奖
ShadowGuard-基于多模型融合的黑暗环境下暴力行为检测系统	优胜奖
物联网时代的“瞒天过海”：智能家居恶意流量识别策略	优胜奖
SecurePiNet: 基于深度学习的便捷式网络流量监控与异常检测系统	优胜奖
基于蜜罐的攻击溯源系统	优胜奖
保信护池--基于联邦学习的电池SOH安全保障	优胜奖
ChronoElderChain——基于Fabric区块链的时间银行智慧养老系统	优胜奖
基于多元异构混合深度学习模型的软件缺陷预测框架	优胜奖
PPTP--基于单一暴露点的跨域内网渗透测试平台	优胜奖
具有可调参数的确定性量子搜索算法求解 SAT 问题	优胜奖
Phoenix Guard-基于深度学习的可迁移轻量化工业互联网 IDS	优胜奖
基于进程匹配的学生上机管理系统	优胜奖
安枢-BGP源认证内生安全防御系统	优胜奖
RISKCOG: 下一代设备用户隐式实时认证系统	优胜奖
MedInfo Shield——一种全流程医疗信息保障系统	优胜奖
国密盾	优胜奖
跳变周期自适应的端信息跳变系统	优胜奖
网络哨兵——基于溯源图的APT攻击检测	优胜奖
农信链溯源系统	优胜奖
基于国密算法的校园卡区块链存证系统	优胜奖
面向AVR架构MCU的功耗侧信道泄漏安全检测	优胜奖
混沌之盾：面向敏感目标的区域图像加密算法	优胜奖

作品名称	奖项级别
“图联芯界”-图像安全JKHY RISC-V架构后量子SoC处理器	优胜奖
银鹰系统——基于人工智能的网络安全检查系统 (SES)	优胜奖
隐秘——自定义数据加密系统	优胜奖
敏哨——基于华为ModelArts的敏感信息监测系统	优胜奖
智慧公交——基于RFID及人脸识别的信息加密系统	优胜奖
基于Fate框架的隐私保护攻防系统	优胜奖
取巧图便——基于区块链与数据算法驱动的智能合约身份认证系统	优胜奖
基于YOLOV5人脸反欺诈检测研究	优胜奖
混合列优化AES算法的云数据安全化应用	优胜奖
基于5G网络的轻量级多用户认证系统	优胜奖
清朗网络——非法博彩App采集与分析系统	优胜奖
“智链认证”——基于区块链和属性基加密的分布式身份认证系统	优胜奖
STS-AI网络安全平台	优胜奖
SafeChat: 对抗LLM后门攻击的防御AI安全大模型	优胜奖
基于机器学习和云沙箱的网络钓鱼攻击检测工具	优胜奖
基于RAG模型的本地网络安全知识库 AI助手	优胜奖
链上非遗——基于区块链的非遗文创版权的多功能平台	优胜奖
轻量级ARP欺骗防御与精准溯源实时监控系統	优胜奖
混合式入侵检测系统	优胜奖

第十七届全国大学生信息安全竞赛作品赛组委会

西北工业大学网络空间安全学院

