第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
1	Test1024	KRSFinder：基于字节码的混淆对抗与污点传播分析系统
2	绿洲	ModelOasis——深度学习模型安全评估系统
3	注意到后门队	基于注意力的VIT后门防御平台
4	Forgery Buster	FakeX：AIGC图像检测与模型溯源平台
5	寒冰射手	ZombieHunter：基于二进制代码自动化分析的僵尸网络威胁狩猎系统
6	EthTrackers	基于交易的以太坊动态监测：新一代的恶意行为识别
7	我不熬夜	獬豸：AIGC文本风险检测与溯源系统
8	MFLW	面向决策树的高效zkSNARK系统
9	起名好难队	针对短视频平台的谣言视频检测系统
10	桥洞维修队	基于二值神经网络的联邦学习系统
11	无忧认证队	无忧认证——生物特征隐私保护的双因子认证
12	燃烧你的梦队	基于射频指纹注入技术的搭便车式隐蔽通信
13	只有队长不玩原神队	PassInfinity：基于可组合泛化知识的新型在线认证系统
14	零界智御	面向零信任安全的生成式威胁推断与验证系统
15	与发际线作队	secRAG——基于检索增强和越狱检测的安全搜索引擎
16	组一个队	BinLLM:基于大语言模型的二进制代码漏洞检测系统
17	临时组队	网络安全图谱及智能推演平台
18	锦忆梦	基于神经网络和量子加密的智能混合多模态加密系统
19	隐私守护小卫士	隐私卫士：端到端的可定制化流数据密文访问控制系统
20	挖不出漏洞队	面向低功耗蓝牙设备的漏洞挖掘系统
21	恋上虹膜在链上	链上虹膜——基于 Fabric 的虹膜加密认证系统
22	我来自混沌	基于混沌理论和并行计算的批量图像加密系统
23	Zeta	具有语义理解的敏感目标加密系统
24	这里没有二刺猿	结合LLM和属性图嵌入的二进制程序相似性检测软件
25	book思议队	金融安全守卫者-基于图神经网络的金融欺诈检测系统
26	信息安全作品赛参赛小队	智图锁：基于深度平衡离散哈希的选择性图像加密系统
27	代码写的都队	智驾护航——车联网安全卫士
28	东大双菜	天网：APT威胁情报集成与路径可视化分析系统
29	蒙的都队	密码之芯：轻量级密码安全性分析与检测系统
30	冻梨一队	智能合约漏洞检测
31	这是一个对	漏洞检测系统
32	车南联网	车联网“传真话”——抗攻击的语义通信安全系统
33	TEE之链	基于区块链的可信外包计算架构设计与实现
34	学网安什么都队	基于深度学习的以太坊智能合约漏洞检测
35	卷积矿物质队	非授权无人机智能侦测反制技术
36	冲就完了	WebInsight FusionMap: 动静全域网站测绘系统
37	我要迪斯尼队	M-RFF： 下一代移动通信射频指纹身份认证系统
38	手"指"灵活，I/Q更高	基于射频指纹识别的物联网设备认证系统
39	爱玩原神	PowerShell脚本高效解混淆及恶意代码检测工具
40	不知道叫什么队	基于语言大数据模型的 WEB API 隐藏端点发现与漏洞挖掘系统
41	信道防窃听小队	移动环境下基于ESP32嵌入式平台的对称无线信道密钥生成
42	你说的都队	基于Wi-Fi信号的人员感知与行为检测平台
43	生吃苹果	网络攻防数字孪生及态势推演平台
44	法网恢恢疏而不漏	LedgerShield——基于超级账本的去中心化可信网络验证系统
45	CV大师队	基于大语言模型的智能威胁情报提取系统
46	AI判官	当AI遇上侦探！面向AI生成内容的多模态检测系统
47	无声胜有生	对非线性特性信息攻防的超声波传感器智能设备
48	在南京	基于内生可解释性的深度网站指纹防御方法
49	一起握手队	基于水印嵌入的强安全密钥掌纹识别方法及实现
50	无人机通信队	面向无人机通信的无线信道密钥生成算法与系统

第十七届全国大学生信息安全竞赛——作品赛初赛团队名单

序号	团队名称	作品标题
51	地铺飞科队	DeepShield（深盾）：鲁棒人脸伪造检测系统
52	蓝猫龙骑团	声音保--面向通话软件的声音保护APP
53	我们一定队	妙眼-基于Diffusion的图像识别对抗样本净化系统
54	SuperQuantum	基于CV-QKD的量子安全视频通信系统
55	InfiniteFocus队	DiffMark：针对扩散模型的图像确权与溯源水印系统
56	我太想进步了	PinpointProbe：面向匿名通信网络的跨域小样本网站指纹识别系统 .docx
57	Book思议	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
58	淇猪去打猪	基于检索增强的通用大模型智能合约漏洞检测
59	VMKillers	VMForce：一种针对虚拟化混淆恶意软件的强制执行技术
60	哒哒哒	SecurePiNet:基于深度学习的便捷式网络流量监控与异常检测系统
61	一铭金人	复杂环境下基于树莓派的侦测与安全通信小车设计
62	秦岭山下	云端电子数据完整性审计系统
63	红心铸盾	基于同态加密的隐私保护人脸识别
64	畅通无组	基于RLWE的同态密码加速器设计与实现
65	大清早吃大青枣	基于函数生成的新型图像隐写算法
66	2的256次方	基于图像自然随机性的联邦取证分析系统
67	熔断大气层队	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
68	深藏blue~	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
69	车车特工队	可篡改定位与模糊补全的车载影像视频隐式表达水印系统
70	争渡	面向移动终端的敏感图像安全共享与云管理系统
71	aknb	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
72	墨迹追踪游骑兵	全息迷阵：基于协同跳变的动态目标防御系统
73	303小碗菜	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
74	book思一	护盾之径-基于链上联邦学习的战场车联网抗毁瘫轨迹研究
75	错误代码	无漏：基于混合推理的轻量级物联网漏洞防护系统
76	决信危机	链上链下协同的数据可信存储与安全共享方案
77	五角星光	基于双向情感与群体认识的网络暴力演化分析系统
78	万分信任	区块链驱动的一体化零信任安全防护平台
79	打虎队	玄武智卫——基于云边端协同的无人智能设备安全管控系统
80	海底小纵队	（k,n）视觉密码方案的跨载体实现
81	什么都对队	基于全同态加密的人脸识别系统
82	信息天才3.0	基于人脸识别的安全访客系统
83	密码尖兵	知识图谱驱动的分组密码智能分析系统
84	奋起上进	基于大模型RAG与Prompt的安全策略编排及智能响应系统
85	獬豸检测小分队	面向Android平台的应用隐私策略验证系统
86	制胜天眼	制胜天眼——基于可信联邦学习和行人重识别的跨域智能监控系统
87	谭何容易	时空蜜链：动态欺骗防御赋能的多步攻击诱捕系统
88	破晓之光	芯盾：面向硬件木马检测的硅前安全评测 EDA工具
89	低空尖兵	低空卫士：基于物理不可克隆函数的无人机双协同敌我识别系统
90	砺剑队	大规模高精度IP智能定位技术驱动的外部攻击面检测与展示系统
91	数安智囊团	DataTrading-基于联邦学习和区块链的智能数据招采平台
92	奇思妙想	MEPV3.0——密码协议形式化综合分析平台
93	芥末菜菜鸡	问卷安——基于本地化差分隐私的安全问卷系统
94	翔宇	热点事件中的情感分析与群体隐式立场挖掘系统
95	一路向前冲冲冲	基于白盒加密水印技术和Res2Net的声纹识别认证系统
96	NUEblue-ONE	基于SM4加密技术的侧信道防护系统的设计与实现
97	CyberGuardians	生成式签名——一种用于AI生成图像鉴别及来源确认的智能检测系统
98	Hack Titans	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
99	冲冲冲123	安全送达防护装置——基于R-GCN的物流异常检测与防护
100	吃葡萄不吐葡萄皮队	基于国密算法的分布式身份认证系统

第十七届全国大学生信息安全竞赛——作品赛初赛团队名单

序号	团队名称	作品标题
101	P1AY	基于区块链与国密算法的民航旅客积分服务平台
102	安全小分队	基于联盟链的PKI证书系统设计与实现
103	h0m0	商用密码应用安全性评估测试工具设计与实现
104	OK组合	基于Fabric的轻量级蠕虫计算防护系统
105	我们真厉害	流云护盾——基于SDN的LDos攻击检测与防御系统
106	踹一踹	跳变周期自适应的端信息跳变系统
107	DCCP	基于国产可信硬件和国密算法的机密计算平台
108	测测你的水印	Safemark:违法信息溯源场景下的大模型水印技术
109	碱基互补配队	LLM生成文本检测器
110	WMG	星鉴——支持多域多模型的中文机器生成文本检测系统
111	动态发展联盟	基于深度学习与多模态融合的虚假短视频综合检测系统
112	量子护网	融合量子密钥的 IPSec VPN 数据安全传输平台
113	风险引擎队	基于多维属性统计推断的身份认证风险识别响应系统
114	隐安推理	InferDPT：基于差分隐私的大语言模型安全推理框架
115	有志青年队	基于LLMs的智能合约漏洞检测：自动化断言与模糊测试的融合
116	联邦大队	基于后门水印的可溯源联邦模型多方授权系统
117	0o0o0oOCUR	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
118	ZZ施工队	面向第三方SDK的隐私透明度提升工具
119	提示词队	FRAUDGUARD: 基于大模型思维链的诈骗内容实时检测系统
120	阳光大学生	基于跨平台对比的移动应用隐私风险度量系统
121	顺其自然入队	基于隐私水印对大语言模型生成文本的辨识与确权
122	快乐星球队	面向移动应用生态复杂误导界面的检测对抗技术
123	WeAreRight	DataForge：面向产业数据共享的关键信息脱敏系统
124	试试就试试	ScanMal：跨平台恶意软件智能溯源与关联取证系统
125	哈基米队	Beyond：基于RoBERTa的NLP软件测试与安全性增强系统
126	FakeText	TextGuard-多线索自适应学习的文档图像伪造检测系统
127	scst	遗忘之盾：赋予用户数据被遗忘权与检测恶意用户行为的安全联邦遗忘系统
128	祖国的花朵	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
129	火炬坚果队	智联卫士—深度神经网络驱动的物联网恶意软件检测系统
130	哈哈哈哈哈	基于深度学习的关键电子数据识别分析工具
131	云曦249	基于机器学习和云沙箱的网络钓鱼攻击检测工具
132	云曦老油条	基于深度学习的PHP代码漏洞检测工具
133	wye邑卫安全	邑Scan-轻量化与全自动化web漏洞扫描平台
134	_NO_S3c_	克隆音频检测逃逸攻击系统
135	南极星	能源互联网安全智能巡检预警系统
136	网络巡警	基于DPDK的高速网络流量审计系统
137	啊队	基于持续学习的恶意软件检测系统
138	最危险的地方	DroneAuth:多无人机可扩展轻量高效身份认证机制
139	好想和你凑一队	基于最小中本系数的去中心化程度检测评估系统
140	早八睡不醒	可信机密虚拟机系统研制
141	坏运走开队	BlockSafeShield——基于智能合约生成的可扩展漏洞检测与防护系统
142	联联看	基于联邦学习的网络攻击智能感知系统
143	冲云霄	基于区块链和属性签名的分布式身份认证系统
144	安全智行守护者	基于深度学习与树莓派的危险行为智能感知系统
145	北城安星团队	基于suricata入侵检测实现的智感安全实训平台
146	智御	协同智盾漏洞扫描工具
147	智绘安全队	RGB可视化下的恶意代码深度探测
148	notshyshy	AlchemyShield：面向文生图模型的艺术风格保护系统
149	我不是大神	面向工业互联网不平衡入侵检测数据集的数据扩充系统
150	对对对对队	物联网时代的“瞒天过海”：智能家居恶意流量识别与防范策略

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
151	立大功旺旺队	PDLD：针对自适应敌手的可编程，去中心化链路洪泛防御
152	芯片又冒烟	MedInfo Shield——一种全流程医疗信息保障系统
153	二一队	PhasedDefender——面向联邦学习投毒攻击的分阶段可视化防御系统
154	得吃	基于社会背景的短视频平台新闻检测系统
155	车联网追踪者	路网卫士—车联网女巫攻击检测与溯源系统
156	那天与你邂逅的薇薇	面向异构环境的双网络联邦工控入侵检测系统
157	花园宝宝	应龙Armour --- 基于可信AI计算的智驾哨兵模式保护系统
158	玩原神玩的	影名单——动态且高效的匿名黑名单技术
159	林泉	基于流量数据的公有链交易分析
160	rebyK	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
161	理工神盾	以静制动：静态物联网稳健动态无线密钥生成系统
162	Hungry dragons	“轻隐”-基于对抗扰动迁移性的图像隐私保护方法
163	风卷残云队	基于时序图学习的Web 3.0混币交易地址关联框架
164	上春山	基于CNN的区块链网络异常检测系统
165	版权安全先锋队	IntelliTracer：生成式大模型版权保护与用户溯源服务
166	侧影轻语队	基于人工智能的密码芯片侧信道分析安全检测系统
167	牛仔裤乐队	Palette——基于流量群匿名化的实时指纹攻击防御系统
168	原神职业队	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
169	RSA_CCC	基于ISRSAC的多功能数字签名算法设计
170	DKYF33	掌密空间-基于国密算法的档案管理系统
171	起名字真难队	基于国密算法的区块链 医疗资源智能管理平台
172	Besti学研组	隐私卫——基于同态加密的双盲隐私保护服务系统
173	好队友更是好朋友	敏哨——基于华为ModelArts的敏感信息监测系统
174	七号小分队	基于嵌入式的噪声源随机性实时检测模块
175	明言密语	明言密语——基于树莓派的分组密码算法演示平台设计与实现
176	卷毛小分队	Puzz
177	取不出来名队	安医智训—基于动态安全多方计算的智慧诊疗平台
178	ZUC流的好快	ZUC高性能安全软件实现及应用
179	安疆儿女	安疆：针对恶意信号源的无人机移动测向与定位系统
180	战略投资部	鹰眼监察：非法无人机与飞控手的监管定位系统
181	DreamItPossible	安网驭行：融合性机器学习智能网联汽车入侵检测系统
182	ShardingTeapot	基于分片区块链的安全高效可扩展 6G AKA协议
183	赛博石榴	图影盾——基于语义和零水印的图片压缩保护系统
184	蒸蒸日上对不队	慧识——基于分布式身份的反诈骗身份识别系统
185	拿奖公布蟹黄堡秘方	医数通——基于分布式增量可验证计算的医疗数据交付方案
186	遥遥领先	迷影探漏——基于深度学习的模糊测试优化技术研究
187	超级凶队	基于门限属性基加密和分片区块链的医疗数据确权与跨域共享方案
188	网安第一小组	基于安全多方计算框架下gpt模型实现高效金融欺诈检测
189	wh1te	Proteus-基于格密码和属性基加密的无人机集群身份认证和密钥管理
190	基于DID身份的医疗信息共享方案	基于DID身份的医疗系统
191	Graphene	探赜索隐——面向政务数据安全的国密多方隐私计算平台
192	尚一队	KLGuard: 基于流量混淆的远程击键推测防御系统
193	我要成为密码学糕手	Kerberos——隐私保护的政务舆情监测系统
194	网络协议759	面向QUIC的请求伪造攻击仿真与防御验证系统
195	心算MD5	面向不可信服务器的基于模糊签名和隐私保护的身份认证系统
196	说点掏心窝子的话	基于GPS诱骗的无人机主动防御技术探索
197	补天小队	语纹声安——基于MFCC和小波的AI语音检测系统
198	怼对队	TurboSA：基于分片区块链和高效安全聚合的医疗大模型联邦学习系统
199	数链金安	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
200	安全大师	支持隐私保护的软件签名管理方案--基于零知识证明的全流程匿名化软件签名

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
201	首席救援对	零知识友好型哈希函数的算术电路实现与优化
202	小鲨鱼	安信探：基于通信传输协议的分布式违规设备检测与定位系统
203	我要当分子	GnnShin: Few-Shot场景下基于GNN的源码漏洞检测系统
204	西部牛仔	MalEye—基于掩码自编码器的恶意流量检测系统
205	AIGC真探社	真像只有一个——基于Inverse Diffusion的AI生成图像的鉴伪与溯源算法
206	GZteam	基于联盟链与联邦学习的医疗数据管理平台
207	Traveller	基于时间图模型的横向移动攻击检测与预测系统
208	我们最棒	基于区块链和代理重加密的文件访问控制系统
209	云境安枢	云境安枢——JavaScript安全加固应用平台
210	第一梯队	拍鉴通——基于区块链的蝴蝶乒乓球拍存证系统
211	重生之我在西安当兵马俑	AntiRec：基于可迁移通用对抗扰动的实时防语音识别隐私保护系统
212	CallCypher	CEPS-IoT：面向物联网终端的国产高性能集群通信代理
213	什么叫队	基于主机日志溯源图的网络威胁检测与预测系统
214	呼神护卫	基于区块链的车联网隐私保护认证机制的设计与实现
215	绝地求生	基于贝叶斯近似的高性能恶意隐写载体检测系统
216	昌平火箭	github敏感信息监控系统
217	代浩然说的都不队	面向云环境的流量传输管控系统
218	魔魔胡胡胡蘿蔔	基于以太坊智能合约的数字内容版权保护系统
219	从零开始的网安竞赛队	为了巩固提升国产操作系统中标麒麟安全性的预先漏洞检测平台
220	树上的鸟儿成双队	Web浏览器XSLeaks漏洞自动化检测系统
221	叫我第一名	基于随机森林和bilstm的恶意流量检测系统
222	世界需要OP	“极零”— 基于零信任的云计算资源细粒度动态防护系统
223	邻座的丁真同学偷偷用藏语向我表白	基于拟态主动防御的软件安全防护系统
224	欲买桂花同载酒	基于多特征融合的区块链异常交易检测与可视化分析系统
225	你说对就	基于联邦学习概念漂移下的网络加密公害流量识别终端
226	物联网同路人	信创环境下安全物联网边缘计算网关
227	管他对不对	基于深度学习的多种隐写算法的图像隐写检测与分析系统
228	惊天加密团	私语心声——基于同态加密的深度学习心理健康评估系统
229	布鲁内尔	TouchSec：基于触控手势的身份认证系统
230	香蕉味印度飞饼队	基于区块链和非交互式零知识证明的版权管理系统
231	宝宝说得队	基于遮挡增强步态识别的多模态智能安防系统
232	隐者无敌	基于社交网络图像的稳健隐蔽通信方法与系统
233	卷就队了	SecCredit-模型隐私保护的高性能小微企业信贷风险评估系统
234	初芽	云颜易容术
235	scc安全团队	基于语言无关特征和LLM融合的开源组件投毒检测
236	网络骑士	融合专家知识与大模型的软件漏洞检测系统
237	WasmGuard	WASanitizer：面向webassembly二进制的安全检测系统
238	无人机双向认证	基于步态识别的无人机送货双向认证系统
239	冲刺	链安卫士：软件供应链漏洞检测系统
240	红外步态视觉团队	热影步识——基于红外视频模态的步态识别
241	黑化肥挥发发灰会花飞队	多元语音攻击智能检测系统
242	鹰眼守护队	基于深度学习的伪造图像检测
243	CPSS	基于半监督学习的自更新物联网空间测绘平台
244	相亲相爱一家人队	基于差分隐私和剪枝的联邦学习框架
245	UltraGuard团队	基于近超声波干扰的智能音箱防窃听系统
246	NN又CC	安澜智鉴——基于二进制主动混淆与演化的未知恶意软件检测系统
247	明密文队	基于多领域自适应学习的谣言检测及交互平台
248	Cipher大模型	Cipher大模型
249	恩西西小队	融合毫米波感知的安全声纹认证系统
250	无敌飓风暴龙	基于有限状态机的QUIC协议指纹识别系统

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
251	芝士雪豹	多模态深度伪造检测与防护平台
252	隐视安全	基于区块链的防删除摄像头方案
253	威猛先生	大语言代码模型赋能开源物联网软件安全测试平台
254	CVE战士队	S2VulHub-信息精确的开源软件漏洞信息库系统
255	AVCrossGuard	AVCrossGuard：基于交叉注意力机制的多模态深度伪造检测系统
256	MDSAT团队	基于多维行为分析的Intelligent Web漏洞预测与渗透测试系统
257	CVE Hunter	基于对比迁移的物联网固件第三方组件漏洞分析
258	Shing吗	基于多维度特征融合的恶意代码检测系统
259	NCEPU305	链证溯源——基于区块链技术、零知识证明与可验证计算的智能无纸化供应链系统
260	PrivacyGuard	ERASER：面向多模态数据的隐私遗忘系统
261	Fast-Https	新型安全智能web服务器--高性能企业IT基础设施软件
262	网工之光	基于白盒SM4混合同态加密的数据库透明代理系统
263	网安小分队	“御语守界”：基于CodeBert的代码漏洞分析和修复建议平台
264	应龙祈盛队	ICDefender：面向工控网络的小样本生成与入侵检测系统
265	考试都队	面向智能模型效率后门的监测系统
266	ChainGuard	基于图表示学习的区块链交易安全保护系统
267	寻声聚力科技团队	寻声聚力——全方位舆情监测与态势感知系统
268	FRS_lab	人脸识别管家——安卓生态人脸识别中的隐私保护
269	CipherCrew队	基于深度语义特征遗传优化的指纹活性检测算法
270	π	“WIFI神探”-基于无线信道特征的盗版WIFI鉴定器
271	云图密语	云图密语
272	恶码侦探	恶码侦探——恶意软件分析与取证系统
273	智绘先锋团	智盾幻绘——基于对抗攻击的FPS游戏反AI作弊系统
274	对话守门人	面向垂直行业大语言模型的个性化隐私保护系统
275	忧郁的牙套	”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
276	大刘的小跟班	心脉密码
277	香蕉	国密盾
278	汪汪检测队	悟空智能--AI影像创作与智能伪造检测系统
279	安全第一	智聚安防——基于yolov5的人员聚集与闯入安全监测系统
280	植物人	基于DNA编码的高光谱遥感图像加密平台
281	丁真和他的队伍伙伴们	面向机器学习的后门攻击评测系统
282	南理工信息安全小分队	基于区块链的无人机认证系统
283	鸡块队	面向网络异常监测的DGA域名AI识别方法与系统
284	Matrix	基于Fate框架的隐私保护攻防系统
285	虚假内容安全检测队	FalconGuard-抗Deepfake和LLM增强的虚假内容检测系统
286	CAT	面向IoT设备的动静态混合自动化漏洞挖掘工具
287	Asuri	基于GDB的网络协议模糊测试方法研究与应用
288	climbers	在线社交媒体虚假信息检测与抑制原型系统
289	rm -rf /	面向WebAssembly的网络端深度学习模型防御技术
290	森林狼1队	物联网典型设备电子数据取证程序
291	WIRELESS	”网络安全哨兵“——基于大语言模型的恶意网站检测系统
292	NKU数据胶囊小队	智合——基于数据胶囊概念的自动化隐私合规检测系统
293	破防先锋队	ScopeChecker-超级应用API-Scope错位检测系统
294	Spy Terminators	GrangeeSense:基于格兰杰因果关系的隐藏物联网设备识别系统
295	密码都队	雾云存储场景下加密去重物联网数据的近似分析
296	啥都能解密	基于私钥攻击的RSA分类器
297	隐私安全了	基于安全多方计算的分布式差分隐私数据合成平台
298	人定胜天队	基于LLM的口令解释和评价系统
299	蛋仔派队	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
300	加蜜还是你说的队	基于蜜加密的口令管理器

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
301	黑铁小分队	Phoenix Guard-基于深度学习的可迁移轻量化工业互联网 IDS
302	梦通网安	改进深度伪造产物检测模型
303	科学特别调查队	基于人工智能的网络安全检查系统
304	nc2202小组	守护者 —— 个人用户的全方面保护专家
305	XP21	基于近似查询合成的DBMS的缺陷检测系统
306	网安队	慧眼识真：多模态媒体篡改的检测与定位技术 在防诈骗中的应用
307	XMU_WONDER	基于SM3的后量子数字签名系统
308	6Y	基于国密算法SM4的保留格式加密系统
309	UNhook	基于云服务器与内核技术的远程协同防泄露办公系统
310	匿网恢恢取证队	匿名安全和强追溯的分布式数字取证系统
311	来去无踪签名队	支持动态隐私溯源的分布式门限签名系统
312	e	基于对抗学习的深度伪造还原系统装置
313	LittleCiphers	基于同态加密的可搜索密文生物认证系统
314	LMC-AI Security	火眼金睛——AIGC时代全媒体深度伪造检测系统
315	音真探源	音真探源--语音深度伪造泛化性检测与算法溯源系统
316	明叶杰然	基于浅深层特征融合的合成音频水印系统
317	摸鱼小芬队	健康中国—基于PaddlePaddle的3D医疗数据解析平台
318	千里碧山队	安全面孔盾——人脸情绪识别加密系统
319	GEELY · NO1	自动化信息收集
320	四只眼	守护之盾：基于Linux的TCP网络安全通讯系统
321	农大保安团	农大保安团
322	啊对对	基于国产密码技术的个人密码管理系统
323	区块链守护者联盟	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
324	千秋印记	千秋印记，守护每一道契约
325	5000岁害怕暴力	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
326	SecureLight	“鉴恒锁隐”——基于安全网关的工控设备网络防护方案
327	安全摸鱼对对队	面向网络跟踪与恶意广告的手机 APP不良行为管控系统
328	规格严格不让及格	“传语报安”——基于声纹识别的实时身份验证系统
329	比奇堡的蟹堡王	面向防AI伪造的音频扰动与签名水印系统
330	Hit小分队	基于大语言模型的移动应用恶意隐私泄露评测系统
331	去吃肉夹馍	"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
332	重生之我在信安赛当暖男	“防诈视卫”——基于集成学习的生成式AI视频电诈识别系统
333	Py大星，我们一起去抓水母吧	“联邦药师”——基于博弈性选举机制的联邦学习辅助制药系统
334	Guardian队	GUARDIAN：基于集成对抗扰动与智能算法推荐的数字身份与艺术创作保护系统
335	大模型安全检测小组	“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
336	信安作品赛小分队	基于双机制联邦学习的异常流量检测系统
337	国奖小队	基于数字水印与SM2的在线链上图片交易与确权系统
338	凌晨四点	SecureSharing——面向价值观对齐和偏好对齐的社交推荐系统
339	HIT_巡遥千河	"Cybermark"——基于大模型水印技术的语言模型与数据产权的保护平台
340	天天开心	基于浏览器插件的有害内容监测技术研究
341	转只因队	基于可逆掩码网络的人脸隐私保护系统
342	懂懂	“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
343	电眼识器小分队	电眼识器——人工智能分解负荷的用电器感知系统
344	白手起家	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
345	网网队立大功	KGIGVDS-基于知识图谱的智慧电网可利用漏洞检测系统
346	不加生姜花椒香菜队	Hiaca-超大规模非法博彩网站捕捉及异常账户信息的自动化采集与分析系统
347	比特守护队	BCWatch：基于图表征学习的区块链异常交易检测系统
348	i人一队	基于图分析的CAN消息异常检测系统
349	幻想成为计科高手携雪豹驰骋理塘队	多模态协同的信息窃取行为识别与预警系统
350	信息安全，启动！	清朗网络——非法博彩App采集与分析系统

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
351	蓝多多	OTD-多源多端公共服务站点隐匿不良信息检测系统
352	天星之旅	基于知识图谱与大模型的车险诈骗智能判案系统
353	Del0n1x	基于PAS谓词聚合签名的在线评分系统
354	医疗星链组	基于委托计算的生物医疗数据分析智能体
355	逸一时误一时队	AutoSVT：极端天气下的自动驾驶预期功能安全测试平台
356	找不到人队	基于多元异构混合深度学习模型的软件缺陷预测框架
357	想不出名字队	面向推荐系统的异常内容检测与舆情管控系统
358	Kingdom-X	基于深度学习与区块链技术的网络内容监控系统
359	做的对不	面向社交媒体的在线多模态谣言检测系统
360	AI安全卫士	SafeChat：对抗LLM后门攻击的防御AI安全大模型
361	DTGL	ImGuardian——面向社交媒体的AI生成图像风险感知，评估与监测系统
362	GGBOND	航安达——空域监视与欺骗检测系统
363	MalScope	基于技战术与LCA算法的恶意代码功能二进制定位系统
364	学习使我快乐	GoShield-面向开源Go应用的自动漏洞修复系统
365	影卫士	影卫士——影评水军群体监测和意图识别系统
366	叫啥名呀	IdentityGuard:面向多模态身份信息的深度伪造主动防御平台
367	重生之我是蒟蒻	CopyCop：面向影视盗摄传播的自动感知与保护系统
368	OpenFort	OpenFort-面向开源软件安全的分析评估系统
369	神佑我楷洋	SmartRASP
370	SDKSpy开发团队	SDKSpy:面向软件供应链安全的SDK风险监测系统
371	VulnTrac	VulnTrac-基于大语言模型的仓库级代码脆弱性检测系统
372	泽言团队	泽言：面向人机协同的社交网络群体检测及意图识别系统
373	海底小纵队分队	基于DLP的移动端个人数据分类保护系统
374	DeepSentry	DeepSentry:面向实时通信诈骗的深度伪造检测防御系统
375	卧龙凤雏历险记	SChat：面向社交软件的隐私保护个性化推荐系统
376	夏天吃葡萄就队	GRAPES：生成式的基于强化学习的对抗性恶意软件检测系统
377	情比金坚铁三角队	NoEscape：洗钱行为识别与追踪溯源系统
378	LeakSpy	LeakSpy:数据贩卖平台主动感知与追溯系统
379	吗喽危险派对	VidTrace：面向AIGC新型威胁的短视频侵权行为检测与防护系统
380	评委老师说得都对	基于多维特征的Webshell检测系统
381	N4N	蒙小析-基于大模型智能体的鸿蒙恶意代码检测分析系统
382	202c	AntiTrolls—基于LLM和知识图谱的代理软件溯源与分析平台
383	蒟蒻信安	基于ATT&CK和D3FEND的跨域网络安全威胁防御智能决策系统
384	沉默的牛马	诊安全——基于CP-ABSE和变色龙哈希的电子病历系统
385	菜菜捞捞	基于SSA的恶意代码家族分类
386	熬夜冠军	“穹盾”——语义约束的多模态性格隐私保护系统
387	宇宙究极隐写战神队	“MediSCI”——面向远程医疗的新型可逆隐写增强系统
388	XJSS	基于提示词学习的存储型XSS攻击向量检测技术
389	高哥做的一定队	Aegis：以太坊实时交易检测预警系统
390	XU17	基于开源情报的Web后门检测系统
391	少年先疯队	SqliGPT：基于多智能体的SQL注入黑盒检测工具
392	IPv6达芬奇	IPv6网络高效资产属性发现测绘系统
393	0xMasterPro	大模型增强的漏洞监控程序自动生成技术
394	钧泽心镜	防伪守真--基于对抗样本的深度伪造主动防御系统
395	我说的都队	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
396	熬大夜	FortressHealth-PBFL: 强固隐私的联邦辅助诊断云平台
397	闯创一流	溯本求源：一种支持再分发行为追踪的数字作品安全共享系统
398	8月之约	基于大语言模型检索增强的在线实时智能问答技术
399	银河帕鲁队	移动应用流量识别与智能安全分析系统
400	三个臭皮匠和一个小莫奇	物联网设备web漏洞动态检测系统

第十七届全国大学生信息安全竞赛——作品赛初赛团队名单

序号	团队名称	作品标题
401	Lxlt	Profiler4DNS: 一种域名网络行为监测系统
402	银河WTF	基于DFA压缩算法的100Gbps实时网络安全检测系统
403	IVY	基于图模型的动态网络异常行为检测系统
404	12345	CE Guardian: 视频识别模型安全检测站
405	WebOK	净面——网站追踪实时检测与拦截系统
406	前面的区域以后再来探索队	前面的区域以后再来探索队
407	Jasmine	重明之眼——基于大模型和多模态的后门检测系统
408	发际线与我作队	实时可解释的网络入侵检测系统
409	Abit	基于射频指纹智能提取的nfc中继攻击检测系统
410	云海之上	网络安全防护系统自动化配置设计与实现
411	云海之巅	基于图谱特征分析的IP软核硬件木马检测系统
412	是风动	Akso：基于触发器提取与定向遗忘的神经网络模型后门识别与清除系统
413	the superego	基于异步机制的网络应用服务快速测量技术设计与实现
414	漏洞小分队	面向Web接口的物联网设备固件漏洞自动分析系统
415	智慧杂交版	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
416	天天向上	数字孪安--面向智能电网数字孪生的攻击检测系统
417	林克的左手	照衡——面向用户个人信息定制的离线口令生命周期管理工具
418	Team B	洞察之眼——LLM增强的网络协议模糊测试系统
419	青龙学习小组	火眼金睛——基于指针生成器网络的变体文本处理
420	有请下一队	SCrack——一句话Webshell高效后门密码破解系统
421	yellow道格	基于生成式文本隐写术的隐私通信保护工具
422	白泽RASP	白泽RASP：基于RASP的Web应用漏洞治理平台
423	会赢的对不队	擎源——面向信创软件的开源代码漏洞治理系统
424	白泽护航	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
425	发际线总是在和我作队	miniAuthX-小程序身份认证漏洞检测系统
426	智能卫士	基于图匹配网络的二进制软件漏洞检测系统
427	少年先锋队	按图索骥，追本溯源—数字图像来源取证系统
428	云脸小队	云脸-基于联邦学习的人脸认证系统
429	三点饮咖啡先	NoGPT-基于PPL和对数曲率的AI文本检测平台
430	信安就是心安	基于保护窗口的实时安全调度方法
431	动影追踪者	动影追踪者——视频来源鉴别系统
432	信息安全为您保驾护航	基于联邦学习的医疗数据隐私保护系统
433	干啥啥都队	一目了然——AI换脸检测系统
434	勇敢小精灵	PDFWhisper—基于PDF科学文献的隐蔽存储系统
435	伪影检测 护航未来	基于多注意力机制的深度伪造实时视频检测平台
436	密影	密影——基于超混沌系统和DNA编码的图像加密系统
437	Scr1w	NetVigil：基于网络流量的本地威胁情报系统
438	过了样例就算对	国密先锋——基于国产加密算法sm2与sm3的文件加密系统
439	田里务工队	国产大模型驱动的智能合约生成、检测及修复一体化平台
440	羽冠朝阳	Value-Zone：区块链驱动的数据可信确权及价值流通平台
441	win	“智巡护航”——基于yolo的智能安全巡检小车
442	卧龙凤雏	网络中基于sdn的DDOS防御系统
443	AAA	基于LLM的多模态网络异常检测系统
444	点击mod自动加载队	区块链数据要素公平交易系统
445	口算AES256	SecureShield：基于SDN的防火墙和入侵检测系统
446	不焦虑小分队	面向应急救援智能无人系统的安全跨域远程操控系统
447	不想再熬夜了	保护隐私的金融风险评估助手
448	抽空拿奖队	基于区块链的无人机安全物流配送系统
449	磐石队	基于多特征的音视频通话实时检测系统
450	以雷霆击碎黑暗	THOR：基于零信任的恶意二维码实时检测系统

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
451	这次我们不站队	图安–基于缩略图保持加密的图像资产服务云平台
452	四级必过队	基于区块链加密的慈善众筹平台
453	初来乍到队	链上非遗—基于区块链的非遗文创版权的多功能平台
454	啊对对对你说的都队	隐踪秘符：基于图像隐写的安全信息嵌入系统
455	安全飞行队	基于差分编码与块压缩的密文域可逆信息隐藏
456	区块链-哈基米队	基于FISCO BCOS的区块链投票平台
457	金科鸿宇	“图联芯界”-图像安全JKHY RISC-V架构后量子SoC处理器
458	AGCTF	基于GO语言的病毒检测系统
459	Attaching Muggle	基于SM4加密算法的黄河三角洲水陆生境监测系统
460	三枪加一炮	基于国密算法的禽畜养殖数据库安全策略研究与实现
461	四核多线程队	基于可信执行环境的数据同态加密传输方案
462	不给国一就睡觉	GM-Shield：基于SM9数字签名分布式可扩展零知识证明系统
463	安全护卫队	QueryGuard：安全高效数据库查询系统
464	你说的队	基于伪随机数生成器的轻量级门限签名方案
465	东里村大学代表队	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
466	脱贫不脱发队	面向联邦学习的 CKKS-RNS 同态算子芯片设计
467	超级胜利队	Zapper：简洁低交互的物联网设备互联认证协议
468	信息安全竞赛获奖队	“政链通”——基于后量子多签名的政务区块链系统
469	好运来队	医合差询：基于可验证差分隐私的医疗数据收集查询系统
470	智能安全与隐私保护团队	智能电网5G业务安全检测系统
471	7波胡杨队	探究云计算环境下的数据安全风险及应对策略
472	世界和平队	大数据环境下数据存储安全的解决方案
473	1111	基于深度学习的网络异常流量检测系统
474	ikun大队	混合式入侵检测系统（Hybrid Intrusion Detection System，HIDS）
475	蟹堡王的秘方守护团	基于多模态的抗声学侧信道攻击的故障检测
476	ToBeOne-Sec	CbWAF：基于CatBoost机器学习的WAF设计与实现
477	Honker_Team	网安智哨——数智网络威胁检测与分析一体化平台
478	守护者之盾	基于联邦学习的安卓恶意软件检测与分析系统
479	肝完信安凌晨三点南亭夜宵小队	肝完信安凌晨三点南亭夜宵小队
480	广东技术师范大学数字侦探	基于数字签名和SM4的证据录音器
481	洞见	洞见
482	我只是来混	基于开源系统软件-网络流量感知审计及运维自动化
483	启航队	文件保险柜
484	零点睡不着队	基于登陆注册后的集成跳转网站
485	智印守卫	溯防智印——支持溯防一体式版权保护的对抗水印系统
486	图像卫士	无痕加密——含有视觉语义的图像加密系统
487	水印侦探	追本溯源—面向大语言模型生成内容的水印版权保护系统
488	666大顺	基于flowprint的局域网APP加密流量自动化监测与识别
489	蕉太狼战队	RSA密钥加密解密系统
490	希望之队	基于映射匹配的异常流量检测系统
491	F426	HackerTrove————AI主动防御与演练平台
492	R@dar2024	基于后量子密码Kyber的通信系统
493	radar02	基于区块链技术的网络安全漏洞检测系统
494	R@dar02	基于虚拟蜜罐的主动防御系统
495	乎兮乎兮嘿嘿	PhishGuard-恶意电子邮件附件检测系统
496	GeekTrain	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
497	基因重组	网络巡逻者“web-scan”
498	信息加密小队	密语——智能手机隐私信息加密&解密App
499	紫玉清平	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
500	MeiDuiYao_	天山卫士—基于图对比和Snort的网络入侵检测系统

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
501	暗光卫士	ShadowGuard-基于多模型融合的黑暗环境下暴力行为检测系统
502	完美竞赛	基于JSP的WEB安全靶场
503	Union of ST	农产品溯源系统
504	AAAJNU	版权守航：数字创作版权保护平台
505	RushMe	SmartBitChain ：基于Bulletproof零知识证明的区块链
506	你好我们是一个队	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
507	暨大少年先疯队	“无隐”——基于自然语言处理与端口监控的隐私政策分析模型
508	签名嵌入小组	抗量子密码签名域情报传输系统的设计与实现
509	重在参与队	安全云存储中的密文数据去重与完整性审计
510	不会起名字队	Intrusion Insight—基于域适应的车联网络入侵检测系统
511	合约督察分队	智能合约督察天眼——基于深度学习的区块链智能合约安全检测系统
512	365天速通AI	语镜——面向可信LLM的安全风险检测与防御系统
513	byte	文心智安——基于文心一言的异常安全日志智能分析插件
514	江南皮革厂	IntelliFuzz-基于LLM的智能模糊测试系统
515	联邦学习	基于联邦学习的网络攻击检测
516	汪汪队	“Guardian”安防设备安全认证平台
517	命运石	基于联邦学习的恶意软件检测系统
518	蓬莱防火墙	周全-基于“ML”+“规则”双擎驱动的数据库防火墙-蓬莱防火墙
519	监督恶意url	恶意URL检测
520	检测大队	基于联邦学习的分布式拒绝服务攻击检测
521	进击的网络安全	基于联邦学习的网络攻击安全检测
522	专业团	信创环境下的云中心安防系统
523	叫啥好呢	智安联邦——基于增量联邦学习的流量攻击检测系统
524	基纽特战队	智警密传：基于DES-CBC加密的智慧家庭安防系统
525	起个名字吧	TouchSecureX：基于压感的指纹解锁
526	核心价值观非常队	智护府——基于YOLOv8的危险姿态识别系统
527	啥也不会，对不？	GuardExam - 自动化试卷安全管理与加密系统
528	麻瓜传媒	TrxLLM：面向区块链的图大模型交易风险检测系统
529	各安天命队	守护天空：基于深度学习的实时无人机网络协同入侵检测系统
530	我要上学	VoxTracer:基于变分可逆神经网络的说话人溯源系统
531	信安大赛您轻置玉足队	UnVoiceClone：面向生成式伪造语音欺骗的鲁棒主动防御系统
532	枫花雪月队	HeadSonic：基于骨传导耳机的高效安全身份认证系统
533	黑曼巴队	WiFi安防器：隐私保护的智能安全监测与防护系统
534	oGuardians	MetaGuard：保护通信元数据的匿名通信系统
535	AISec	天镜智盾：基于时序不一致性的恶意伪造检测系统
536	白泽驰骋之ddl战队	PrivTuner：基于联邦学习的语言模型隐私保护个性化微调系统
537	歪比巴丨丶	HateSentry——基于大模型的多模态网络仇恨检测系统
538	麦门永存队	闻声识脸：基于声信号的3D动态人脸认证系统
539	时代科研团	隐秘追踪：基于记忆水印的图像版权保护系统
540	云边协同数据创新小组	基于云边协同的可信数据去重平台
541	东厢月	FaceShield-基于可逆神经网络的DeepFake溯源追踪系统
542	你才是挑战者	微动识真：基于跨模态匹配机制的人脸活体检测系统
543	FuzzLLM	FuzzLLM-基于模糊测试思想的大模型越狱攻击漏洞评估框架
544	%TEMP%	基于不经意访问的多域告警记录安全共享
545	MC方块人求生	TELEPATH：基于Minecraft的隐蔽通信系统
546	freegait	FreeGait：基于无约束步态识别的身份认证系统
547	PnP-IRDM	PnP-IRDM:一种可即插即用的SRS对抗样本防御插件
548	glhf	洞观：TLS中间人威胁检测及防御系统
549	西天取经	脉动声息——基于声学传感的智能用户认证系统
550	干饭不想排队	“声行逐迹”--基于深度学习的智能声纹识别侦察系统

第十七届全国大学生信息安全竞赛——作品赛初赛团队名单

序号	团队名称	作品标题
551	翻斗花园75号	视界领航——基于AI视觉与安全加密技术的智慧助盲新篇章
552	关关过关关队	ChronoElderChain——基于Fabric区块链的时间银行智慧养老系统
553	队不队	数智守护者——打破数据孤岛安全解决方案
554	sky dragon队	安全哨兵——基于多模态学习的智能检测系统
555	芳姐小分队	心室守护—医学数据全生命周期隐私保护解决方案
556	海洋信安队	基于机器学习和文本挖掘的水上通航安全漏洞分析系统
557	信息安全护盾团队	基于区块链技术的医疗数据安全护盾系统
558	白鲸安行	白鲸安行—自动驾驶安全决策控制与防御系统
559	一切归于虚无，万事皆是徒劳	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
560	漏洞知识小课堂	基于知识图谱的漏洞检测与教学系统
561	凝聚队	MalwareCipher：面向加密流量的智能恶意检测系统研究与实现
562	江大智盾	基于Bert和时域卷积网络的智能合约漏洞检测系统
563	少年侦探队	基于概念漂移识别的网络入侵检测系统
564	很爱学信安	“智联安行”—基于机器学习的智能网联汽车安全通信系统
565	末影之眼队	基于足迹，工作量证明和信誉值联合的车联网女巫攻击检测技术
566	我真的想不出来	幽影停泊—基于国密的ZK-AVP远程泊车导引系统
567	链上物流	基于区块链的加密物流管理系统
568	添砖JAVA	永安-面向智能网联汽车的差分隐私联邦智检系统
569	数据守护者队	政务加密链——数据共享与信息检索隐私保护系统
570	Trackers	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
571	一举成名队	保信护池--基于联邦学习的电池SOH估计中的隐私数据保护
572	沙卡拉卡	基于NLP的智能合约漏洞检测系统
573	喵喵队	车轨隐私盾
574	GG博	轨迹定制—基于同态加密和属性基加密的个人隐时空私轨迹保护系统
575	漏洞猎手	FFGNN-VDS：基于特征融合和图神经网络的漏洞检测系统
576	JSNU雪冰城	R盾—协议秘密泄露漏洞检测工具
577	星期四疯狂列队	虚假人工智能生成内容态势感知与预警系统
578	真的假的？我打信安！？	觅踪-基于生成对抗网络的隐语识别系统
579	冲刺一下	基于区块链的警用无人机加密数据安全存证系统
580	神盾安全	守护者——基于网络爬虫的恶意URL检测系统
581	隐私电网先锋队	面向V2G网络支持匿名支付的隐私认证系统
582	一加一大于二	SC Trace——基于区块链的供应链信息管理与溯源一体化系统
583	指望另一队	恶意流量分析系统
584	B	隐秘——自定义数据加密系统
585	蒸蒸日上	基于混沌算法的文件保护与产权溯源平台
586	苦猴伟	插件化Java中间件漏洞扫描器
587	SpecialRain	破军：面向多功能安全测试的网络威胁探测系统
588	梦火	基于Paillier的时控性同态加密电子投票系统
589	前量子队	寻密--基于MLP的通用密码算法识别推荐方案
590	密码admin	基于流处理PSI与yolov8的智慧医疗监测系统
591	龙子湖一高	基于隐私计算技术的虚拟社交空间
592	加油队	安全防护及报警装置
593	亮剑队	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
594	361安全卫士	基于随机神经网络的数据隐私保护的分布式训练系统
595	随便组的队	基于无透镜成像的人脸识别系统
596	嗡嗡嗡	基于量子噪声流的微波光子内生安全系统
597	N友小趴菜	DecoupleGuard——基于良性特征解耦的可靠后门防御系统
598	汪汪队睡大觉	SPARSE：融合语义跟踪与路径分析的高级持续性攻击溯源系统
599	根本躺不平	融合大模型的恶意流量检测诊断系统
600	StingerHorizon	APTSentinel：融合上下文语义特征与注意力机制的轻量级 APT检测系统

第十七届全国大学生信息安全竞赛——作品赛初赛团队名单

序号	团队名称	作品标题
601	Stinger	RISKCOG：下一代移动设备用户隐式实时认证系统
602	内核哨兵	K-Sentinel：基于内核日志的安全监管平台
603	AAAAA队	面向医疗数据的隐私保护数据分类算法的设计与实现
604	随便什么队	国密算法演示平台的设计与实现
605	杭州三小只	基于秘密共享的医疗数据保护平台的设计与实现
606	Wyking	分布式环境中基于国密算法的代理重加密系统设计与实现
607	山居	基于TF-IDF特征选择与LightGBM分类的Web攻击智能识别系统
608	Leo	基于国密 SM4 算法的文件加密应用
609	双枪帅哥	基于RAG模型的本地网络安全知识库AI助手
610	HybridGuard	HybridGuard：面向机器人操作系统的分布式隐私保护方案
611	网安小队	融密：深度学习分析隐写系统
612	爱迪生小组	勒索病毒的检测及文件还原系统
613	鹰眼迅查	基于特征图建模和胶囊网络的恶意软件分析系统
614	小雨点滴答答	真相守卫——面向Deepfake的多模态融合检测系统
615	我说的都怼	链盾——基于区块链和属性加密的出生证明存证系统
616	网事如风	基于全同态加密和AIGC的智能医疗数据处理平台
617	灵动小队	融合个人信息与口令重用的口令验证系统
618	守护世界	守护视界--基于信创环境的智能网络监测与响应系统
619	送你一朵小红花	基于零信任与区块链的IoT设备安全管控平台
620	一一一队	基于去中心化CP-ABE的公开可验证乐观公平交换协议
621	11408酱	“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
622	爱喝果粒橙	ProtoGuard:工控协议的安全哨兵
623	天选6队	“链锁产权”基于区块链技术的知识产权保护系统
624	啦啦队	基于头部姿态估计技术实现反AI换脸系统
625	中午吃什么	基于SM2&SM3算法的特权账号管理系统
626	计网不挂科	基于同态加密的联邦学习图像识别系统
627	炸鸡队	农信链溯源系统
628	枫行奋进	基于国密算法的数据库防篡改系统
629	信安第一梯队	密钥云——基于昇腾AI服务器的属性基加密的作业管理系统
630	瑞智安邦	“瑞智安邦”——基于视频大数据的人群综合治安风险监测与防范平台
631	TO SEE透视车防团队	TO SEE透视车防
632	急急国王队	基于yolov9的智能网联汽车图像脱敏系统
633	代码肯定都队	基于改进残差网络的网络入侵检测系统
634	OLY	MC2FDetector-基于多通道特征融合的软件缺陷检测
635	恒心无畏队	“智”洞商机——面向商业数据分析与辅助决策的隐私计算平台
636	四分之三保研队	锦衣暗卫-大模型越狱漏洞防御系统
637	智信队	基于帧级注意力的跨语种深度伪造音频检测系统
638	唯一指定获奖选手	区块链异常账户识别系统
639	隐私医疗链盟	链医联邦：隐私保护的多机构鲁棒医疗数据联邦分析系统
640	三木一叶	面向数据异构和数据安全的城市监控体系架构
641	VigilantBytes	基于程序控制流特征的控制流完整性机制研究
642	懒说配听，炎之拿瓦	基于卷积神经网络的恶意代码API特征提取与检测系统
643	md5撞击中	基于集成学习与深度神经网络的PE恶意代码检测系统
644	天生赢家	GuardNTRU：基于NTRU的后量子抗性区块链安全交易系统
645	ai超级无敌宇宙强队	基于“区块链+联邦学习”的智能舆情分析系统
646	湖南农大蝰蛇信息安全实验室	流智图灵——融合RoBERTa-MiniLM和知识图谱的流量分析系统
647	蝰蛇实验室	基于Docker的高效智能网络安全竞赛演练平台
648	蝰蛇信息安全实验室	GenAIDetector——基于自然语言处理的AI虚假文本检测综合平台
649	Sec4AI	字里乾坤——AIGC文本多比特水印方法
650	MYSEC	基于硬件虚拟化技术的windows应用程序加壳保护系统

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
651	大吉大利	基于卷积神经网络的图像篡改嫌疑检测与自适应水印工具
652	只要学不死，就往死里学	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
653	安链先锋	基于国密算法的校园卡区块链存证系统
654	四个臭皮匠	面向AVR架构MCU的功耗侧信道泄漏安全检测
655	作品就跑了	量子密钥管理
656	你几时起了我未用镜花水月的错觉？	Hypnotist-一款动态加密和主动防御的软件保护引擎
657	隧视	隧视——基于可解释机器学习的恶意DoH隧道检测系统
658	F4	Hideout——联邦学习中多维自适应后门攻击框架演示系统
659	天下英雄当真如过江之鲫	混沌之盾：面向敏感目标的区域图像加密算法
660	不会cv队	基于数字孪生的物联网安全测试与监测平台
661	Finder	智慧公交——基于RFID及人脸识别的信息加密系统
662	睡大觉测绘队	基于无人机搭载边缘端的网络资产定位与测绘技术
663	星辉	万维聚真——多源网络空间测绘可信聚合系统
664	量子幼稚园	具有可调参数的确定性量子搜索算法求解 SAT问题
665	墨水精灵	“墨水精灵”-透过酸碱探索防伪奥秘
666	Pearlsky3	GLM-3模型中的恶意提示词注入与对抗研究
667	阿兰维克	eVAult：基于IPFS与区块链的健康信息加密存储和AI预测系统
668	尽显锋芒	基于深度学习的安卓恶意软件检测平台
669	统一青梅	来源于网络
670	保卫者	VeriPIR: 面向数据外包的可验证隐私信息检索
671	胜文	面向社交平台的多模态深度伪造检测系统
672	勇往直前	基于Transformer和可靠零知识证明的多模态深度伪造检测系统
673	烤鱼和干锅都	ModelForSSDLC：面向安全软件生命周期的软件成分安全评估方法模型
674	Eurus	Fed Privacy Shield
675	YulinSec	SPLM:大模型与主动免疫赋能的V2G安全预警平台
676	链上汪汪队	可验证的隐私保护糖尿病视网膜病变预测联邦学习系统
677	为网安添砖java队	智溯御网—基于SCNN-LLAMA的网络入侵检测系统
678	我请问对不队	基于函数秘密共享的高效电子投票方案
679	同学会	AppScope——智能化安卓应用安全分析平台
680	唐人街	Sphinx——基于触摸振动信号的用户认证系统
681	以太链盟	碳链宝-安全可溯源的全流程碳市场管理平台
682	小葵花向阳队	ShadowVote：基于区块链的完全匿名自计票投票系统
683	样本过了就算队	医保卫士-基于多模型融合的医疗保险欺诈识别监测系统
684	深藏blue	基于声学特征的无人机检测和识别系统
685	取名这么难	基于前缀引导的强化安全代码自动生成系统 —SafeCoder
686	全都队	基于不经意键值存储的两方外包隐私集合交集基数计算系统
687	夜未央	隐影卫士——基于图像隐写的版权保护
688	Viking	ByzantineVK---基于鞅理论的抗投毒拜占庭鲁棒联邦学习平台
689	认证不队	基于设备声纹的双因素认证系统
690	为了地球的安全	“边城”——面向复杂对抗环境的多维密态数据采集与统计系统
691	哇哇珠峰	MyDataBase:隐私保护的安全可验证外包数据库
692	火柴人守护者	火柴人守护者—基于NPU加速的边缘隐私保护智能监控系统
693	安保大队	STS-AI网络安全平台
694	什么都队	蜜罐管理系统
695	想不到	网络嗅探系统
696	kinght	GoWAFer - 基于Golang的轻量化Web应用防火墙
697	一个人哭	面向对抗样本攻击的智能汽车行驶安全检测及防御系统
698	网安安保分队	安枢-BGP源认证内生安全防御系统
699	H0rizon	AMS2E：面向医联体的医疗数据安全共享系统
700	果宝特攻队	基于动态检测的未授权漏洞扫描

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
701	你在跟我作队	Django Vuln Hunter：高效漏洞侦测平台
702	西北请我去喝风	企网安全一体化设计
703	宝宝巴士	轻量级ARP欺骗防御与精准溯源实时监控系统
704	ATS	基于可编程交换机的DDoS缓解系统
705	试一试对不队	试一试SDN
706	小王想获奖	态势感知智慧平台
707	荆楚大队	基于SDN环境的DDoS多功能缓释系统
708	ERROR0	基于SDN的攻击感知与均衡调度系统
709	重生之我是牢大	一种基于区块链的数据安全共享系统
710	Jay	荷鲁斯之眼—基于Bi-RNN的恶意代码视觉静态检测系统
711	Vans如意	基于物理网络的分布式加密系统
712	JK	全流量驱动的Web漏洞智能挖掘及验证系统
713	车盾	车盾——智能网联汽车入侵检测系统
714	波利多罗斯	"狴犴"——基于图神经网络的硬件木马检测系统
715	赛博卫士	基于国密算法的无人集群安全通信系统
716	Autogen—CTF	基于大语言模型的CTF自动化测试竞技场
717	阿巴阿巴	基于非对称加密的无人机安全通信系统
718	我和专家站一队	芯盾智防：基于机器学习的鲁棒性硬件木马检测系统
719	3.12MB	视觉乌贼——融合判断与混淆的工业视觉安全检测双重防御机制
720	考的全队	大模型驱动的海量文本敏感信息检测技术研究
721	冲冲冲🤛	基于国密算法和生物特征认证的安全智能锁钥系统
722	啥也不会	基于数字孪生网络的安全策略优化与验证技术研究
723	WirelessHunters	智耳：智能无线网络安全监测与主动对抗系统
724	萝卜老鸭汤	御鹰——对抗传感器攻击的自主定位系统
725	ABC队	一种轻量化的隐私保护人脸认证系统
726	西瓜网络安全队	云密宝盒-云计算下密态数据安全交换与共享的领航者
727	nobug	基于区块链的艺术品数字资产知识产权系统
728	海底小队	基于联邦学习的艺术品推荐系统
729	捕风捉音	高性能声纹识别平台
730	你说的到底对不队	“一步止谣”——基于多模态的虚假信息检测系统
731	事已至此，先吃饭吧	基于区块链的服务器日志记录系统
732	miniFlyteam	链筑安全-Fabric联盟链驱动的房产交易防护平台
733	风雨云集	混合列优化AES算法的云数据安全化应用
734	威胁猎手hreatHunters	一种SDN控制器DDoS攻击的检测方法及防御系统
735	冒犯性语言检测小队	网暴终结者—基于预训练模型的中文冒犯性语言检测
736	微光	网络哨兵——基于溯源图的APT攻击检测
737	奥德彪	针对云计算自动扩容Yo-Yo攻击的防御方案
738	Flyteam	基于SM9的优化和DNA加密技术的图片加密算法
739	radio飞机	基于软件无线电框架的WiFi的Python分析
740	快乐干饭早点睡觉	基于LLM的漏洞检测和蜜罐防护系统
741	检测小队	AIGC检测平台
742	XoX	信宝阁：基于同态交换水印与链上零知识的数字藏品可信平台
743	摸鱼如喝水	TrapWeaver-基于大语言模型和行为检测的主机入侵检测 /防御系统
744	黑飞不起来队	“天网”低空卫士——察打一体的低空智联网管控系统
745	v我50鸡翅分你一队	LightFakeDet——基于知识蒸馏的轻量化人脸鉴伪系统
746	CodeBrain	CppHawkEye:基于知识图谱的智能化C++供应链开源漏洞检测系统
747	北雷村车管所	PriPark: 隐私保护的车位信息群智感知平台
748	蜡笔要小心队	Invisible Cloak——结果模式隐藏的多模式密态数据检索系统
749	四大名捕	“明察秋毫”：基于多元数据联邦学习的反诈人脸鉴伪系统
750	AI-AntS	P-Oracle: 基于机器学习的协议安全性自动化分析平台

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
751	我和Y神一个队	Anti-ransomware:基于机器学习和细粒度访问控制的勒索软件检测与防御系统
752	凌晨四点练习落地水	Safe-charge：基于区块链技术的充电桩交易系统
753	我没意见	IoT Guardian—面向IoT设备的多因子容错认证平台
754	Vanguard	RKEGuardian：自适应跳频技术增强的RKE安全通信系统
755	少年先疯疯疯队	AuthLink：跨移动应用认证安全风险检测系统
756	万源生万德	TKACG-APT攻击检测与溯源系统
757	Lumio	MPCTensorLib——面向深度神经网络的轻量级安全多方计算平台
758	我要迪士尼队	安疫——基于隐私保护和抗攻击的传染病溯源预警系统
759	架云卫士	SkySecure——面向“云网端”架构的无人机集群安全控制系统
760	貌影辨识	貌影辨识
761	没有ads的泥头车小队	LawTester——针对交通法规的自动驾驶安全测试系统
762	网信小队	面向云网端架构的无人系统安全语义通信
763	EIGuard	EIGuard: 边缘智能场景下侧信道安全分析与加固系统
764	歌者	信链：基于可编辑区块链的数据监管平台
765	春招被拒八次想考研	SafePilot：基于对抗性驾驶策略的自动驾驶系统安全性检测平台
766	数据库武林盟主	TrustVault：基于ARM TrustZone的嵌入式加密数据库解决方案
767	图书馆五楼风很大	基于国密算法的加密图像双认证系统
768	一路向东	智链安全—基于区块链与人工智能的身份认证系统
769	sec	SEC——基于Tiny ML的零信任移动端程序设计
770	守望	守望漏洞检测及验证工具
771	老秦人攻打提瓦特	昆仑枢机--主动式零信任内网监测系统
772	东方树叶	Tokenpass—基于国密SM2的分布式匿名身份认证系统
773	这次一定队	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
774	道里夷易	基于5G网络的轻量级多用户认证与优化系统
775	创新小队	基于BB-PRF的匿名投票问卷系统
776	四季平安	基于进程匹配的学生上机管理系统
777	Cipher-security	BSIMS-IIoT:基于区块链的安全IIoT智能管理系统
778	海底大纵队	基于国密算法和同态加密的安全人脸识别系统
779	玛卡巴卡队	智护·固件安全织梦者
780	好了是贵蜜对不队	Spissatus—云存储环境下基于全同态加密的图像检索平台
781	UFO	基于极大周期序列的安全S盒生成系统
782	食堂不排队	基于门限环签名的抗量子攻击电子投票系统
783	TG	基于加密图像的大容量可逆数据隐藏系统
784	QR	基于加密二维码的快递隐私保护系统
785	Default	“能源卫士”网络攻击环境下新能源预测安全监控系统
786	我将点燃大海	基于 Logistic Regression 逻辑回归原理的刷单检测模型
787	BlueDreamer	基于大语言模型纠错的不良短消息识别系统
788	勇往直前队	基于超像素排序与自适应多预测器的可逆数据隐藏算法
789	LastFlag	网络安全信息检测系统
790	云边协同	云治安-基于云边协同和深度学习的被动WIFI跟踪检测系统
791	CreWin	“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
792	仰望星空	“指纹无痕”：基于零知识证明与区块链的隐匿指纹认证系统
793	仟行团队	灵眸—基于多通道并行检测的综合图像鉴伪系统
794	Megablue	基于R-LWE的车联网抗量子聚合签名方案
795	WhiteCat	基于知识图谱的工业互联网异常监测系统的设计与实现
796	agl	CTF加解密工具
797	打深渊凑不起一个人队	智信先锋——基于RepVGG-SimAM的多特征卷积图不良信息监测系统
798	青年先锋队	智飞卫士-实时无人机GPS欺诈检测系统
799	冠军侯队	深度强化学习安全测试系统
800	打入决赛就算成功	基于区块链的隐私保护群组密钥管理与服务推送系统

第十七届全国大学生信息安全竞赛——作品赛初赛团队名单

序号	团队名称	作品标题
801	E3p101t-Y	反诈先锋---基于机器学习的诈骗网站检测提示系统
802	Explorer	针对XSS的拦截系统
803	南山小纵队	BDHunter：基于多元技术集成的后门攻击检测方案
804	摆烂宝宝巴士	基于ChaCha20的伪随机数生成算法和验证码生成器
805	RCX²_win	金智FinGuard—基于Paillier的金融数据安全多方计算系统
806	匿颜守护者	PRO-Face：跨场景人脸视频隐私保护系统
807	TechGuard	CyberSecure MedTrack
808	欢宜香小队	基于多层路由的分布式匿名网络通信系统
809	IS安防大队	车行智安-面向隐私保护的车联网安全防御系统
810	慧眼识人	基于联邦学习与差分隐私技术的人脸识别安全系统
811	wk	高安全的文件存储系统
812	网络守护者	网络安全之旅：网络守护者的使命
813	带饼队	浏览器个人信息保护
814	信息安全竞赛队	基于SQL的风险检测系统
815	乘风破浪队	学生信息安全管理系统
816	不忘初心	数据安全人人有责
817	比特安全卫士	数据盾牌：智能防御系统
818	都行的队伍	关于web安全的攻防测试
819	科技创新队	基于机器学习的网络安全入侵检测系统
820	信息安全有我们	基于网络安全的实验探索与实践
821	509	系统安全
822	521队	文件传输
823	长理队伍168	加密文件传输工具
824	Yz_S3c_Encrypt	基于四维忆阻超混沌系统和DNA加密的图像加密算法
825	千人千面	PCP：基于隐私保护的高效的人脸识别系统
826	勇敢向前冲	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
827	对对队	星络之盾——构建企业虚拟专用网络的信息安全堡垒
828	一定拿奖队	Matlab图形版权战：数字水印技术的趣味攻防
829	少年先疯队1	智盾——多维协同的网络安全检测与管理体系
830	深藏-Blue队	Cybersecurity-基于ACL的跨地域网络通信系统
831	创意联盟	基于安全区域划分的医院网络信息安全加固系统设计与实施
832	Ginkgo	基于多层感知器与击键动力学的用户识别系统
833	阿浩小先生	基于Java的数据之间加密和解密
834	感觉就很队	WeVote:基于区块链的自统计加权投票系统
835	德尔塔	企业内网资产暴露风险检测
836	集美大学队伍	RSA文书加密防篡改
837	发量王者	Bingo Cloud：基于ADMHF的云存储加密数据去重与同步系统
838	独行侠	网络流量检测系统
839	钥匙翘翘队	迹码寻——基于图片识别的字迹甄别系统
840	程序只要能跑啥都队	漏洞智探——基于LLM的软件漏洞检测系统
841	幺幺叁236分队	威检智盾——基于图神经网络与溯源图构建的APT检测系统
842	Search	基于隐私保护的联邦框架赋能城市电网安全
843	怪兽小分队	隐图-基于图片隐写的信息加密系统
844	黑科技	树莓派网络安全智能检测机器人
845	松北队	基于混沌方法的图片加密系统
846	大怪兽	数字图像加密系统
847	R600	网络数据安全加密技术
848	防伪先锋	基于YOLOV5人脸反欺诈检测研究
849	SkyMirror	基于异构图嵌入的恶意软件检测与分类
850	赛博保安	暗流慧鉴——基于流量分析的Tor恶意软件检测

第十七届全国大学生信息安全竞赛 ——作品赛初赛团队名单

序号	团队名称	作品标题
851	404！	金锁密盾阁--基于全方位密码学的信息安全密码学利器
852	接下来即将赶到赛场的是三只小趴菜	PPTP--基于单一暴露点的跨域内网渗透测试平台