

序号	作品标题	团队名称
1	基于有限状态机的 QUIC 协议指纹识别系统	无敌飓风暴龙
2	基于语言无关特征和 LLM 融合的开源组件投毒检测	scc 安全团队
3	基于前缀引导的强化安全代码自动生成系统—SafeCoder	取名这么难
4	大模型驱动的海量文本敏感信息检测技术研究	考的全队
5	基于 GPS 诱骗的无人机主动防御技术探索	说点掏心窝子的话
6	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	数链金安
7	芯盾智防：基于机器学习的鲁棒性硬件木马检测系统	我和专家站一队
8	MyDataBase:隐私保护的安全可验证外包数据库	哇哇珠峰
9	基于物理网络的分布式加密系统	Vans 如意
10	LeakSpy:数据贩卖平台主动感知与追溯系统	LeakSpy
11	基于随机神经网络的数据隐私保护的分布式训练系统	361 安全卫士
12	智盾幻绘——基于对抗攻击的 FPS 游戏反 AI 作弊系统	智绘先锋团
13	基于双向情感与群体认识的网络暴力演化分析系统	五角星光
14	智安联邦——基于增量联邦学习的流量攻击检测系统	叫啥好呢
15	HateSentry——基于大模型的多模态网络仇恨检测系统	歪比巴 、
16	多模态协同的信息窃取行为识别与预警系统	幻想成为计科高手携雪豹驰骋理塘队
17	玄武智卫——基于云边端协同的无人智能设备安全管控系统	打虎队
18	基于大模型 RAG 与 Prompt 的安全策略编排及智能响应系统	奋起上进
19	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	Trackers
20	网络安全图谱及智能推演平台	临时组队
21	音真探源--语音深度伪造泛化性检测与算法溯源系统	音真探源
22	脉动声息——基于声学传感的智能用户认证系统	西天取经
23	信链：基于可编辑区块链的数据监管平台	歌者
24	基于后门水印的可溯源联邦模型多方授权系统	联邦大队

25	寻声聚力——全方位舆情监测与态势感知系统	寻声聚力科技团队
26	AuthLink: 跨移动应用认证安全风险检测系统	少年先疯疯疯队
27	TKACG-APT 攻击检测与溯源系统	万源生万德
28	基于对比迁移的物联网固件第三方组件漏洞分析	CVE Hunter
29	EIGuard: 边缘智能场景下侧信道安全分析与加固系统	EIGuard
30	ImGuardian——面向社交媒体的 AI 生成图像风险感知, 评估与监测系统	DTGL
31	基于深度学习的以太坊智能合约漏洞检测	学网安什么都队
32	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	我说的都队
33	芯盾: 面向硬件木马检测的硅前安全评测 EDA 工具	破晓之光
34	基于 DFA 压缩算法的 100Gbps 实时网络安全检测系统	银河 WTF
35	MPCTensorLib——面向深度神经网络的轻量级安全多方计算平台	Lumio
36	面向 QUIC 的请求伪造攻击仿真与防御验证系统	网络协议 759
37	面向社交媒体的在线多模态谣言检测系统	做的对不
38	基于国密算法和生物特征认证的安全智能锁钥系统	冲冲冲🐶
39	AntiTrolls——基于 LLM 和知识图谱的代理软件溯源与分析平台	202c
40	安疆: 针对恶意信号源的无人机移动测向与定位系统	安疆儿女
41	GoShield-面向开源 Go 应用的自动漏洞修复系统	学习使我快乐
42	“MediSCI”——面向远程医疗的新型可逆隐写增强系统	宇宙究极隐写战神队
43	P-Oracle: 基于机器学习的协议安全性自动化分析平台	AI-AntS
44	周全-基于“ML”+“规则”双擎驱动的数据库防火墙-蓬莱防火墙	蓬莱防火墙
45	TrustVault: 基于 ARM TrustZone 的嵌入式加密数据库解决方案	数据库武林盟主
46	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	一切归于虚无, 万事皆是徒劳
47	SPARSE: 融合语义跟踪与路径分析的高级持续性攻击溯源系统	汪汪队睡大觉
48	“传语报安”——基于声纹识别的实时身份验证系统	规格严格不让及格
49	“智联安行”——基于机器学习的智能网联汽车安全通信系统	很爱学信安

50	基于步态识别的无人机送货双向认证系统	无人机双向认证
51	基于特征图建模和胶囊网络的恶意软件分析系统	鹰眼迅查
52	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	智慧杂交版
53	基于联邦学习概念漂移下的网络加密公害流量识别终端	你说对就
54	Sphinx——基于触摸振动信号的用户认证系统	唐人街
55	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	熔断大气层队
56	心室守护—医学数据全生命周期隐私保护解决方案	芳姐小分队
57	御鹰——对抗传感器攻击的自主定位系统	萝卜老鸭汤
58	FakeX: AIGC 图像检测与模型溯源平台	Forgery Buster
59	VoxTracer:基于变分可逆神经网络的说话人溯源系统	我要上学
60	泽言: 面向人机协同的社交网络群体检测及意图识别系统	泽言团队
61	WASanitizer: 面向 webassembly 二进制的安全检测系统	WasmGuard
62	HeadSonic: 基于骨传导耳机的高效安全身份认证系统	枫花雪月队
63	以静制动: 静态物联网稳健动态无线密钥生成系统	理工神盾
64	基于时间图模型的横向移动攻击检测与预测系统	Traveller
65	PRO-Face: 跨场景人脸视频隐私保护系统	匿颜守护者
66	RKEGuardian: 自适应跳频技术增强的 RKE 安全通信系统	Vanguard
67	妙眼-基于 Diffusion 的图像识别对抗样本净化系统	我们一定队
68	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	Hack Titans
69	DiffMark: 针对扩散模型的图像确权与溯源水印系统	InfiniteFocus 队
70	信创环境下的云中心安防系统	专业团
71	净面——网站追踪实时检测与拦截系统	WebOK
72	基于双机制联邦学习的异常流量检测系统	信安作品赛小分队
73	重明之眼——基于大模型和多模态的后门检测系统	Jasmine
74	问卷安——基于本地化差分隐私的安全问卷系统	芥末菜菜鸡

75	漏洞智探——基于 LLM 的软件漏洞检测系统	程序只要能跑啥都队
76	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	紫玉清平
77	基于开源情报的 Web 后门检测系统	XU17
78	ScopeChecker-超级应用 API-Scope 错位检测系统	破防先锋队
79	基于人脸识别的安全访客系统	信息天才 3.0
80	FortressHealth-PBFL: 强固隐私的联邦辅助诊断云平台	熬大夜
81	DeepSentry:面向实时通信诈骗的深度伪造检测防御系统	DeepSentry
82	溯防智印——支持溯防一体式版权保护的对抗水印系统	智印守卫
83	云端电子数据完整性审计系统	秦岭山下
84	PCP: 基于隐私保护的高效的人脸识别系统	千人千面
85	OTD-多源多端公共服务站点隐匿不良信息检测系统	蓝多多
86	基于国密算法和同态加密的安全人脸识别系统	海底大纵队
87	PrivTuner: 基于联邦学习的语言模型隐私保护个性化微调系统	白泽驰骋之 ddl 战队
88	Beyond: 基于 RoBERTa 的 NLP 软件测试与安全性增强系统	哈基米队
89	VidTrace: 面向 AIGC 新型威胁的短视频侵权行为检测与防护系统	吗喽危险派对
90	“极零”——基于零信任的云计算资源细粒度动态防护系统	世界需要 OP
91	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	aknb
92	基于注意力的 VIT 后门防御平台	注意到后门队
93	面向防 AI 伪造的音频扰动与签名水印系统	比奇堡的蟹堡王
94	基于可信执行环境的数据同态加密传输方案	四核多线程队
95	鹰眼监察: 非法无人机与飞控手的监管定位系统	战略投资部
96	OpenFort-面向开源软件安全的分析评估系统	OpenFort
97	Fed Privacy Shield	Eurus
98	SPLM:大模型与主动免疫赋能的 V2G 安全预警平台	YulinSec

99	链安卫士：软件供应链漏洞检测系统	冲刺
100	多元语音攻击智能检测系统	黑化肥挥发发灰会花飞队
101	“指纹无痕”：基于零知识证明与区块链的隐匿指纹认证系统	仰望星空
102	在线社交媒体虚假信息检测与抑制原型系统	climbers
103	融合个人信息与口令重用的口令验证系统	灵动小队
104	深度强化学习安全测试系统	冠军侯队
105	基于区块链的隐私保护群组密钥管理与服务推送系统	打入决赛就算成功
106	ByzantineVK---基于鞅理论的抗投毒拜占庭鲁棒联邦学习平台	Viking
107	“边城”——面向复杂对抗环境的多维密态数据采集与统计系统	为了地球的安全
108	基于加密图像的大容量可逆数据隐藏系统	TG
109	基于后量子密码 Kyber 的通信系统	R@dar2024
110	基于随机森林和 bilstm 的恶意流量检测系统	叫我第一名
111	VMForce：一种针对虚拟化混淆恶意软件的强制执行技术	VMKillers
112	面向应急救援智能无人系统的安全跨域远程操控系统	不焦虑小分队
113	面向低功耗蓝牙设备的漏洞挖掘系统	挖不出漏洞队
114	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	303 小碗菜
115	支持动态隐私溯源的分布式门限签名系统	来去无踪签名队
116	GrangeeSense:基于格兰杰因果关系的隐藏物联网设备识别系统	Spy Terminators
117	幽影停泊—基于国密的 ZK-AVP 远程泊车导引系统	我真的想不出来
118	基于 Wi-Fi 信号的人员感知与行为检测平台	你说的都队
119	基于隐私水印对大语言模型生成文本的辨识与确权	顺其自然入队
120	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	白泽护航
121	IntelliTracer：生成式大模型版权保护与用户溯源服务	版权安全先锋队
122	火眼金睛——AIGC 时代全媒体深度伪造检测系统	LMC-AI Security
123	“Guardian”安防设备安全认证平台	汪汪队

124	基于 CV-QKD 的量子安全视频通信系统	SuperQuantum
125	基于同态加密的隐私保护人脸识别	红心铸盾
126	基于 RLWE 的同态密码加速器设计与实现	畅通无组
127	大语言代码模型赋能开源物联网软件安全测试平台	威猛先生
128	字里乾坤——AIGC 文本多比特水印方法	Sec4AI
129	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	深藏 blue~
130	面向异构环境的双网络联邦工控入侵检测系统	那天与你邂逅的薇薇
131	基于浅深层特征融合的合成音频水印系统	明叶杰然
132	FalconGuard-抗 Deepfake 和 LLM 增强的虚假内容检测系统	虚假内容安全检测队
133	GuardNTRU: 基于 NTRU 的后量子抗性区块链安全交易系统	天生赢家
134	基于社交网络图像的稳健隐蔽通信方法与系统	隐者无敌
135	隐私卫士: 端到端的可定制化流数据密文访问控制系统	隐私守护小卫士
136	语镜——面向可信 LLM 的安全风险检测与防御系统	365 天速通 AI
137	基于 SM4 加密技术的侧信道防护系统的设计与实现	NUEblue-ONE
138	面向社交平台的多模态深度伪造检测系统	胜文
139	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	0o0o0oOCUR
140	Aegis: 以太坊实时交易检测预警系统	高哥做的一定队
141	基于联盟链与联邦学习的医疗数据管理平台	GZteam
142	AutoSVT: 极端天气下的自动驾驶预期功能安全测试平台	逸一时误一时队
143	智飞卫士-实时无人机 GPS 欺诈检测系统	青年先锋队
144	WebInsight FusionMap: 动静全域网站测绘系统	冲就完了
145	医数通——基于分布式增量可验证计算的医疗数据交付方案	拿奖公布蟹黄堡秘方
146	基于区块链和代理重加密的文件访问控制系统	我们最棒
147	天镜智盾: 基于时序不一致性的恶意伪造检测系统	AIsec
148	MC2FDetector-基于多通道特征融合的软件缺陷检测	OLY

149	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	区块链守护者联盟
150	ScanMal：跨平台恶意软件智能溯源与关联取证系统	试试就试试
151	融合量子密钥的 IPSec VPN 数据安全传输平台	量子护网
152	DecoupleGuard——基于良性特征解耦的可靠后门防御系统	N 友小趴菜
153	THOR：基于零信任的恶意二维码实时检测系统	以雷霆击碎黑暗
154	基于白盒 SM4 混合同态加密的数据库透明代理系统	网工之光
155	基于白盒加密水印技术和 Res2Net 的声纹识别认证系统	一路向前冲冲冲
156	全流量驱动的 Web 漏洞智能挖掘及验证系统	JK
157	守望漏洞检测及验证工具	守望
158	"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	去吃肉夹馍
159	DeepShield（深盾）：鲁棒人脸伪造检测系统	地铺飞科队
160	UnVoiceClone：面向生成式伪造语音欺骗的鲁棒主动防御系统	信安大赛您轻置玉足队
161	匿名安全和强追溯的分布式数字取证系统	匿网恢恢取证队
162	獬豸：AIGC 文本风险检测与溯源系统	我不熬夜
163	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	信道防窃听小队
164	基于检索增强的通用大模型智能合约漏洞检测	淇猪去打猪
165	智信先锋——基于 RepVGG-SimAM 的多特征卷积图不良信息监测系统	打深渊凑不起一个人队
166	Intrusion Insight——基于域适应的车联网入侵检测系统	不会起名字队
167	DataForge：面向产业数据共享的关键信息脱敏系统	WeAreRight
168	PDFWhisper——基于 PDF 科学文献的隐蔽存储系统	勇敢小精灵
169	FreeGait：基于无约束步态识别的身份认证系统	freegait
170	ZUC 高性能安全软件实现及应用	ZUC 流的好快
171	安网驭行：融合性机器学习智能网联汽车入侵检测系统	DreamItPossible
172	MalwareCipher：面向加密流量的智能恶意检测系统研究与实现	凝聚队
173	“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	CreWin

174	智合——基于数据胶囊概念的自动化隐私合规检测系统	NKU 数据胶囊小队
175	IntelliFuzz-基于 LLM 的智能模糊测试系统	江南皮革厂
176	面向第三方 SDK 的隐私透明度提升工具	ZZ 施工队
177	基于保护窗口的实时安全调度方法	信安就是心安
178	面向联邦学习的 CKKS-RNS 同态算子芯片设计	脱贫不脱发队
179	真相守卫——面向 Deepfake 的多模态融合检测系统	小雨点滴答答
180	基于二值神经网络的联邦学习系统	桥洞维修队
181	链医联邦：隐私保护的多机构鲁棒医疗数据联邦分析系统	隐私医疗链盟
182	面向数据异构和数据安全的城市监控体系架构	三木一叶
183	基于 LLM 的漏洞检测和蜜罐防护系统	快乐干饭早点睡觉
184	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	Book 思议
185	基于大语言模型纠错的不良短消息识别系统	BlueDreamer
186	miniAuthX-小程序身份认证漏洞检测系统	发际线总是在和我作队
187	基于蜜加密的口令管理器	加蜜还是你说的队
188	基于贝叶斯近似的高性能恶意隐写载体检测系统	绝地求生
189	火眼金睛——基于指针生成器网络的变体文本处理	青龙学习小组
190	面向网络异常监测的 DGA 域名 AI 识别方法与系统	鸡块队
191	TextGuard-多线索自适应学习的文档图像伪造检测系统	FakeText
192	Zapper：简洁低交互的物联网设备互联认证协议	超级胜利队
193	基于国产可信硬件和国密算法的机密计算平台	DCCP
194	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	白手起家
195	“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	忧郁的牙套
196	BCWatch：基于图表征学习的区块链异常交易检测系统	比特守护队
197	基于时序图学习的 Web 3.0 混币交易地址关联框架	风卷残云队
198	M-RFF：下一代移动通信射频指纹身份认证系统	我要迪斯尼队

199	基于射频指纹识别的物联网设备认证系统	手"指"灵活, I/Q 更高
200	针对短视频平台的谣言视频检测系统	起名好难队
201	ERASER: 面向多模态数据的隐私遗忘系统	PrivacyGuard
202	雾云存储中密文物联网数据的去重存储与近似分析	密码都队
203	基于无透镜成像的人脸识别系统	随便组的队
204	基于同态加密的可搜索密文生物认证系统	LittleCiphers
205	灵眸—基于多通道并行检测的综合图像鉴伪系统	仟行团队
206	基于安全多方计算的分布式差分隐私数据合成平台	隐私安全了
207	面向零信任安全的生成式威胁推断与验证系统	零界智御
208	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	蛋仔派队
209	BinLLM:基于大语言模型的二进制代码漏洞检测系统	组一个队
210	基于深度学习与多模态融合的虚假短视频综合检测系统	动态发展联盟
211	基于图像自然随机性的联邦取证分析系统	2 的 256 次方
212	基于数字水印与 SM2 的在线链上图片交易与确权系统	国奖小队
213	基于区块链技术的医疗数据安全护盾系统	信息安全护盾团队
214	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	是风动
215	TouchSec: 基于触控手势的身份认证系统	布鲁内尔
216	面向 IoT 设备的动静态混合自动化漏洞挖掘工具	CAT
217	CbWAF: 基于 CatBoost 机器学习的 WAF 设计与实现	ToBeOne-Sec
218	白泽 RASP: 基于 RASP 的 Web 应用漏洞治理平台	白泽 RASP
219	AlchemyShield: 面向文生图模型的艺术风格保护系统	notshyshy
220	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	5000 岁害怕暴力
221	车行智安-面向隐私保护的车联网安全防御系统	IS 安防大队
222	面向 Web 接口的物联网设备固件漏洞自动分析系统	漏洞小分队
223	真像只有一个——基于 Inverse Diffusion 的 AI 生成图像的鉴伪与溯源算法	AIGC 真探社

224	“轻隐”-基于对抗扰动迁移性的图像隐私保护方法	Hungry dragons
225	当 AI 遇上侦探！面向 AI 生成内容的多模态检测系统	AI 判官
226	BlockSafeShield——基于智能合约生成的可扩展漏洞检测与防护系统	坏运走开队
227	GnnShin: Few-Shot 场景下基于 GNN 的源码漏洞检测系统	我要当分子
228	智链安全—基于区块链与人工智能的身份认证系统	一路向东
229	克隆音频检测逃逸攻击系统	_NO_S3c_
230	"猖狂"——基于图神经网络的硬件木马检测系统	波利多罗斯
231	保护隐私的金融风险评估助手	不想再熬夜了
232	基于图分析的 CAN 消息异常检测系统	i 人一队
233	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	你好我们是一个队
234	基于联邦学习的网络攻击检测	联邦学习
235	可信机密虚拟机系统研制	早八睡不醒
236	WeVote:基于区块链的自统计加权投票系统	感觉就很队
237	基于 yolov9 的智能网联汽车图像脱敏系统	急急国王队
238	PassInfinity: 基于可组合泛化知识的新型在线认证系统	只有队长不玩原神队
239	路网卫士—车联网女巫攻击检测与溯源系统	车联网追踪者
240	基于 Paillier 的时控性同态加密电子投票系统	梦火
241	TouchSecureX: 基于压感的指纹解锁	起个名字吧
242	基于量子噪声流的微波光子内生安全系统	嗡嗡嗡
243	基于联盟链的 PKI 证书系统设计与实现	安全小分队
244	智耳：智能无线网络安全监测与主动对抗系统	WirelessHunters
245	基于 LLM 的口令解释和评价系统	人定胜天队
246	协同智盾漏洞扫描工具	智御
247	基于近似查询合成的 DBMS 的缺陷检测系统	XP21
248	HybridGuard: 面向机器人操作系统的分布式隐私保护方案	HybridGuard

249	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	欲买桂花同载酒
250	基于概念漂移识别的网络入侵检测系统	少年侦探队
251	基于持续学习的恶意软件检测系统	啊队
252	金智 FinGuard—基于 Paillier 的金融数据安全多方计算系统	RCX ² _win
253	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	rebyK
254	文心智安——基于文心一言的异常安全日志智能分析插件	byte
255	ICDefender: 面向工控网络的小样本生成与入侵检测系统	应龙祈盛队
256	基于深度语义特征遗传优化的指纹活性检测算法	CipherCrew 队
257	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	东里村大学代表队
258	云密宝盒-云计算下密态数据安全交换与共享的领航者	西瓜网络安全队
259	Palette——基于流量群匿名化的实时指纹攻击防御系统	牛仔裤乐队
260	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	原神职业队
261	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	亮剑队
262	国产大模型驱动的智能合约生成、检测及修复一体化平台	田里务工队
263	基于云服务器与内核技术的远程协同防泄露办公系统	UNhook
264	“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	大模型安全检测小组
265	面向 WebAssembly 的网络端深度学习模型防御技术	rm -rf /
266	星鉴——支持多域多模型的中文机器生成文本检测系统	WMG
267	基于函数生成的新型图像隐写算法	大清早吃大青枣
268	智图锁：基于深度平衡离散哈希的选择性图像加密系统	信息安全作品赛参赛小队
269	守护视界--基于信创环境的智能网络监测与响应系统	守护世界
270	基于水印嵌入的强安全密钥掌纹识别方法及实现	一起握手队
271	“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	11408 酱
272	SecCredit-模型隐私保护的高性能小微企业信贷风险评估系统	卷就队了

273	“窥盗”——基于高低频分离和隐私边缘隐藏的手机文件防窥系统	懂懂
274	基于区块链和非交互式零知识证明的版权管理系统	香蕉味印度飞饼队
275	商用密码应用安全性评估测试工具设计与实现	h0m0
276	基于隐私保护的联邦框架赋能城市电网安全	Search
277	KRSFinder: 基于字节码的混淆对抗与污点传播分析系统	Test1024
278	云治安-基于云边协同和深度学习的被动 WIFI 跟踪检测系统	云边协同
279	面向医疗数据的隐私保护数据分类算法的设计与实现	AAAAA 队
280	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	这次一定队
281	智联卫士—深度神经网络驱动的物联网恶意软件检测系统	火炬坚果队
282	勒索病毒的检测及文件还原系统	爱迪生小组
283	面向推荐系统的异常内容检测与舆情管控系统	想不出名字队
284	融合大模型的恶意流量检测诊断系统	根本躺不平
285	密码之芯：轻量级密码安全性分析与检测系统	蒙的都队
286	面向机器学习的后门攻击评测系统	丁真和他的队伍伙伴们
287	追本溯源—面向大语言模型生成内容的水印版权保护系统	水印侦探
288	基于社会背景的短视频平台新闻检测系统	得吃
289	恶码侦探——恶意软件分析与取证系统	恶码侦探
290	基于秘密共享的医疗数据保护平台的设计与实现	杭州三小只
291	基于 R-LWE 的车联网抗量子聚合签名方案	Megablue
292	基于图匹配网络的二进制软件漏洞检测系统	智能卫士
293	千秋印记，守护每一道契约	千秋印记
294	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	GeekTrain
295	ShadowGuard-基于多模型融合的黑暗环境下暴力行为检测系统	暗光卫士
296	隧视——基于可解释机器学习的恶意 DoH 隧道检测系统	隧视
297	面向 V2G 网络支持匿名支付的隐私认证系统	隐私电网先锋队

298	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	对对对对队
299	“网络安全哨兵”——基于大语言模型的恶意网站检测系统	WIRELESS
300	LLM 生成文本检测器	碱基互补配队
301	SecurePiNet:基于深度学习的便捷式网络流量监控与异常检测系统	哒哒哒
302	蜜罐管理系统	什么都队
303	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	只要学不死，就往死里学
304	保保护池--基于联邦学习的电池 SOH 估计中的隐私数据保护	一举成名队
305	ChronoElderChain——基于 Fabric 区块链的时间银行智慧养老系统	关关过关关队
306	动影追踪者——视频来源鉴别系统	动影追踪者
307	基于多元异构混合深度学习模型的软件缺陷预测框架	找不到人队
308	PPTP--基于单一暴露点的跨域内网渗透测试平台	接下来即将赶到赛场的是三只小趴菜
309	具有可调参数的确定性量子搜索算法求解 SAT 问题	量子幼稚园
310	基于遮挡增强步态识别的多模态智能安防系统	宝宝说得队
311	Phoenix Guard-基于深度学习的可迁移轻量化工业互联网 IDS	黑铁小分队
312	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	祖国的花朵
313	基于图表示学习的区块链交易安全保护系统	ChainGuard
314	擎源——面向信创软件的开源代码漏洞治理系统	会赢的对不队
315	基于进程匹配的学生上机管理系统	四季平安
316	安枢-BGP 源认证内生安全防御系统	网安安保分队
317	RISKCOG：下一代移动设备用户隐式实时认证系统	Stinger
318	NoGPT-基于 PPL 和对数曲率的 AI 文本检测平台	三点饮咖啡先
319	MedInfo Shield——一种全流程医疗信息保障系统	芯片又冒烟
320	声音保--面向通话软件的声音保护 APP	蓝猫龙骑团
321	“WIFI 神探”-基于无线信道特征的盗版 WIFI 鉴定器	π
322	国密盾	香蕉

323	跳变周期自适应的端信息跳变系统	踹一踹
324	网络哨兵——基于溯源图的 APT 攻击检测	微光
325	农信链溯源系统	炸鸡队
326	基于国密算法的校园卡区块链存证系统	安链先锋
327	面向 AVR 架构 MCU 的功耗侧信道泄漏安全检测	四个臭皮匠
328	混沌之盾：面向敏感目标的区域图像加密算法	天下英雄当真如过江之鲫
329	“御语守界”：基于 CodeBert 的代码漏洞分析和修复建议平台	网安小分队
330	“图联芯界”-图像安全 JKHY RISC-V 架构后量子 SoC 处理器	金科鸿宇
331	基于人工智能的网络安全检查系统	科学特别调查队
332	隐秘——自定义数据加密系统	B
333	敏哨——基于华为 ModelArts 的敏感信息监测系统	好队友更是好朋友
334	智慧公交——基于 RFID 及人脸识别的信息加密系统	Finder
335	基于生成式文本隐写术的隐私通信保护工具	yellow 道格
336	基于 Fate 框架的隐私保护攻防系统	Matrix
337	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	勇敢向前冲
338	基于 YOLOV5 人脸反欺诈检测研究	防伪先锋
339	混合列优化 AES 算法的云数据安全化应用	风雨云集
340	基于 5G 网络的轻量级多用户认证与优化系统	道里夷易
341	基于伪随机数生成器的轻量级门限签名方案	你说的队
342	晴朗网络——非法博彩 App 采集与分析系统	信息安全，启动！
343	基于区块链和属性签名的分布式身份认证系统	冲云霄
344	STS-AI 网络安全平台	安保大队
345	政务加密链——数据共享与信息检索隐私保护系统	数据守护者队
346	PhasedDefender——面向联邦学习投毒攻击的分阶段可视化防御系统	二一队
347	云图密语--基于理想缩略图保持加密的图像共享平台	云图密语

348	来源于网络	统一青梅
349	基于数字孪生的物联网安全测试与监测平台	不会 cv 队
350	PinpointProbe: 面向匿名通信网络的跨域小样本网站指纹识别系统	我太想进步了
351	基于帧级注意力的跨语种深度伪造音频检测系统	智信队
352	SafeChat: 对抗 LLM 后门攻击的防御 AI 安全大模型	AI 安全卫士
353	ProtoGuard:工控协议的安全哨兵	爱喝果粒橙
354	基于嵌入式的噪声源随机性实时检测模块	七号小分队
355	基于机器学习和云沙箱的网络钓鱼攻击检测工具	云曦 249
356	基于 RAG 模型的本地网络安全知识库 AI 助手	双枪帅哥
357	链上非遗—基于区块链的非遗文创版权的多功能平台	初来乍到队
358	态势感知智慧平台	小王想获奖
359	轻量级 ARP 欺骗防御与精准溯源实时监控系統	宝宝巴士
360	混合式入侵检测系统	ikun 大队