2021年第六届全国密码技术竞赛决赛入围作品（共123个）

（A类作品22个）								
序号	团队名称	所属学校	作品名称	作品编号	作品类型	领队老师	指导老师	团队学生
1	才轩队	北京电子科技学院	SM9算法在电力领域的应用—硬件高性能实现及侧信道防护	CACR2021YFRIZC	软件设计	张艳硕	张艳硕	唐子越，兰毅达，杨守森
2	绿园可达鸭	北京航空航天大学	电力大数据隐私计算	CACR2021X36SR5	软件设计	高莹	姚燕青	周磊，王英东，滕达
3	nno密码小分队	北京邮电大学	电力大数据隐私计算	CACR2021T7MD32	软件设计	朱洪亮	李祺	韦程瀚，袁希旺，米嘉欣
4	寻密	北京邮电大学	某类有限域上本原多项式搜索工具	CACR20215DMKI9	软件设计	朱洪亮	毕经国	李锦凯，黄广，董英杰
5	LGY	北京邮电大学	基于hash算法的较小文件高强度加密	CACR20218WVS9W	软件设计	朱洪亮	李祺	袁乙灵，弓雪妍，梁宇轩
6	为了被念到时可以霸屏很久才把队名	北京邮电大学	SM2的倍点运算快速实现	CACR2021PULYBM	工程实践	朱洪亮	李祺	赵键锦，向柏澄，徐益彰
7	斜刘海_遮住右眼角的忧伤	合肥工业大学	基于hash算法的较小文件高强度加密	CACR2021XVL9V8	软件设计	朱晓玲	朱晓玲	苏悦，梁雨霄，江晓锐
8	非专业密码队	河南理工大学	S盒及压缩函数的密码学性质检测	CACR20213P7JO1	软件设计	汤永利	闫玺玺	尤俊茹，付岩岩，刘飞扬
9	富强民主文明和谐队	河南理工大学	某类有限域上本原多项式搜索工具	CACR2021RZDQS2	软件设计	汤永利	张静	郎永康，陈晴晴，王瀚博
10	三只黄鹂	河南理工大学	基于hash算法的分组数据加密软件	CACR2021VK3I1P	软件设计	汤永利	孟慧	李佳昕，任利娜，李英
11	火布偶	华中科技大学	某类有限域上本原多项式搜索工具	CACR20216HQ73L	软件设计	骆婷	汤学明	蒋源，刘万奇，张焱柯
12	没有灵感所以你说的都队	华中科技大学	S盒及压缩函数的密码学性质检测	CACR2021HDJBXR	软件设计	骆婷	骆婷	周雅洁，赵浩然，徐鹏
13	我做的全都对	华中科技大学	电力领域物联终端密码算法软件设计实现	CACR202167PSV6	软件设计	骆婷	徐鹏	甘伟盟，刘宇宇，杨一帆
14	乘风破浪队	华中科技大学	ECDSA签名私钥恢复	CACR2021U49127	工程实践	骆婷	徐鹏	汪兆祥，王洋，张家华
15	借点月光	华中科技大学	基于hash算法的较小文件高强度加密	CACR202113TOGO	软件设计	骆婷	骆婷	赵常鹏，宋感恩，吴方舟
16	写的都队	南京理工大学	基于hash算法的分组数据加密软件	CACR20214MTIW9	软件设计	许春根	黄婵颖	刘禄，王子超，刘乐远
17	说什么都对	青岛大学	ECDSA签名私钥恢复	CACR2021LWSJ7K	工程实践	陈飞	李增鹏	高菲，李金凤，邓旭东
18	正中信息密码技术应用一队	山东正中信息技术股份有限公司	SM2的倍点运算快速实现	CACR2021QZBKN8	工程实践	郭峰	付勇	房立蕾，王明玺，郑雷雷
19	喵喵喵喵喵喵	西安电子科技大学	电力大数据隐私计算	CACR2021Y8S3RQ	软件设计	张宁	张宁	徐升，向海川，蒋昊
20	邦邦两拳	西安电子科技大学	S盒及压缩函数的密码学性质检测	CACR2021ZRMR2G	软件设计	张宁	王子龙	李汀，王亚龙，王申奥
21	xd_3l	西安电子科技大学	基于hash算法的分组数据加密软件	CACR2021K23RYY	软件设计	张宁	张宁	林文耀，刘灏，刘谭仁
22	还没想好	西安邮电大学	ECDSA签名私钥恢复	CACR2021PT6VBQ	工程实践	郭瑞	秦宝东	张皓玉，陈倩倩，何岩
（B类作品101个）								
序号	团队名称	所属学校	作品名称	作品编号	作品类型	领队老师	指导老师	团队学生
1	刚之队	北方工业大学	基于区块链技术的电子保函管理系统	CACR2021JTCFQP	软件设计	何云华	徐刚	崔宇，覃江海，余奕盈
2	要做全做队	北方工业大学	基于区块链和国密X3DH的加密通信系统	CACR2021SEPI83	软件设计	何云华	王宝成	李化鹏，王莉荣，黄曦
3	ncutwcw	北方工业大学	基于国密算法与QR码的体育用品鉴别系统	CACR2021SZ2QCL	软件设计	何云华	王宝成	陈霄，王琛，吴志庆
4	团队2号	北方工业大学	生物特征模板融合区块链的智能家居隐私保护	CACR2021HWZL7Q	其他	何云华	李琛	沈沂亭，白孟函，范晓轩
5	二三五队	北方工业大学	基于跨链可信度计算的充电桩公平计价策略	CACR2021P8G8PZ	理论课题	何云华	何云华	王爽，肖棚玥，罗明顺
6	7AE0	北京电子科技学院	基于国密算法的新型智慧医疗资源管理系统	CACR20217RRTIY	软件设计	张艳硕	张艳硕	李泽昊，刘新宇，李烨龙
7	密码猜不队	北京电子科技学院	基于国密算法的智能公益基金管理系统	CACR20218YHC1I	软件设计	张艳硕	张艳硕	贝世之，严嘉钰，杨坤
8	重金求发	北京电子科技学院	基于全同态加密的人脸密文识别系统	CACR202136G4IB	软件设计	张艳硕	杨亚涛	李兆夫，陈柏维，崔克政
9	假面骑士01	北京电子科技学院	基于国密算法的新型云存储双重加密系统设计	CACR2021CZS5SL	软件设计	张艳硕	张艳硕	朱轩锐，张宇鹏，戚少波
10	阿巴阿巴队	北京电子科技学院	伽罗瓦域下本原多项式搜索工具的设计与实现	CACR2021NOWJUP	软件设计	张艳硕	王志强	王文彬，黄济森，于欣月
11	三等一	北京电子科技学院	基于SM3的新型智慧金融信息服务系统	CACR2021DF6G4L	软件设计	张艳硕	张艳硕	常万里，初凯旋，戴君熹
12	旺柴队	北京电子科技学院	全同态密码算法的FPGA快速实现	CACR2021OLD7OL	软件设计	张艳硕	杨亚涛	王在舟，潘威宏，邱雁峰

13	吃饱躺好	北京电子科技学院	基于国密算法的多场景文件传输系统	CACR2021KJEB39	软件设计	张艳硕	王志强	田野，杨永健，刘道瞳
14	密竞才子	北京电子科技学院	对称密码算法部件安全性能测试	CACR2021QCA8GP	软件设计	张艳硕	李艳俊	张潇，张俊怡，刘继荣
15	AliceBob	北京航空航天大学	票据隐私保护的公平自统计电子投票系统	CACR20217QQYMX	软件设计	高莹	孙钰	李慧琳，张凌越，刘霏霏
16	蓝田炸鱼	北京航空航天大学	面向电力数据的隐私集合求交方案	CACR2021MRNF79	软件设计	高莹	高莹	熊科宇，马杰，方翌佳
17	到底对不队	北京航空航天大学	白盒SM4算法的安全性分析与设计	CACR2021WU1G4T	理论课题	高莹	郭华	朱浩，刘怀远，陈俊鑫
18	左轮庸医	北京航空航天大学	抗恶意敌手的通用隐私计算协议	CACR20218U8JEX	软件设计	高莹	张宗洋	潘豪文，夏铭远，刘淮
19	电弧星	北京航空航天大学	uBlock的快速实现	CACR20213R1IZJ	软件设计	高莹	郭华	王瑜，唐泽林，林觉睿
20	轻量级战队	北京航空航天大学	轻量级MDS矩阵的快速搜索和优化	CACR2021RTHDJH	工程实践	高莹	高莹	漆小静，李宗润，贾梓潇
21	进取号	北京航空航天大学	SM2算法非定点标量乘法软件高速实现	CACR2021FH8PYN	程序编制	高莹	高莹	王菁菁，漆林，姜一凡
22	超能陆战队	北京航空航天大学	面向动态委员会的可主动更新秘密分享	CACR2021DZMYFB	理论课题	高莹	张宗洋	孔至立，刘佳睿，林学承
23	0D4Y	北京航空航天大学	支持高效搜索和计算的加密数据库设计与实现	CACR20217EJVEK	工程实践	高莹	高莹	卢洛芳子，罗元超，丘健锴
24	江南天安TASS	北京江南天安科技有限公司	基于hash算法的较小文件高强度加密	CACR2021155LGT	软件设计	张玉安	张玉安	马晓艳，张钊，李雪雁
25	看山还山	北京交通大学	电力领域物联终端密码算法软件设计实现	CACR2021J3CON6	软件设计	黎琳	王健	李鹏，王凯崙，赵阳阳
26	bistu队	北京信息科技大学	基于报文哈希链的签名认证系统	CACR2021D7Z1X1	软件设计	任亚唯	蒋文保	刘颖慧，韩明轩，叶帅
27	莫妮卡火锅	北京印刷学院	基于ZUC与CRT的门限交换加密水印系统	CACR2021ELWJL8	软件设计	游福成	丁海洋	李芸伟，陈维启，赵培越
28	刷大一分队	北京印刷学院	基于ElGamal的同态密文检索系统	CACR2021DUYAY7	软件设计	游福成	李子臣	惠世豪，侯建，邵航
29	Zer0T	北京邮电大学	基于访问策略隐藏的零信任架构设计与实现	CACR2021AMIU5R	软件设计	朱洪亮	徐洁	吴雨勋，朱乃桄，王思远
30	CryptoMan_415	北京邮电大学	基于秘密共享的数字货币钱包的设计与实现	CACR2021CLMMAW	软件设计	朱洪亮	石瑞生	张晨宇，宋雨宸，田传用
31	阿巴阿巴	电子科技大学	某类有限域上本原多项式搜索工具	CACR20214WYP9I	软件设计	李洪伟	聂旭云	谭盾，何亚非，代迪
32	ET	东华大学	典型分组密码标准破译分析软件的设计与实现	CACR2021KG1FBF	软件设计	李玮	李玮	张金煜，张雨希，李嘉耀
33	ET_	东华大学	新型故障分析技术的软件设计与检测实现	CACR2021RCUVTU	软件设计	李玮	李玮	蔡天培，刘春，朱晓铭
34	BulletProof	东南大学	基于无线信道特征的安全密钥协商方案	CACR2021J6LTSX	理论课题	陈立全	宋宇波	郑天宇，马文豪，林建东
35	Alohomora	东南大学	适用于物联网签名认证的混沌哈希算法设计	CACR2021UH6BUL	理论课题	陈立全	陈立全	曹楷林，王宇，朱宇航
36	随机配队	福建师范大学	安全高效的国产泛指定验证者签名证明设计	CACR20211R3HTT	软件设计	林超	林超	蒲浪，陈修远，丰梦琪
37	IDEAL	复旦大学	Aigis-ake密钥交换协议的高效实现	CACR20212QIQ25	工程实践	赵运磊	赵运磊	刘羽，梁志闯，何峰
38	Alpha_and_Omega	复旦大学	格基密钥封装算法优化与软硬件高效实现	CACR2021Y7WAJM	工程实践	赵运磊	赵运磊	郑婕妤，赵一凡，沈诗羽
39	富婆三人组	广州大学	某类有限域上本原多项式搜索工具	CACR2021HAOXEF	软件设计	周权	张晓磊	梁文欣，史瑜壁，胡淼
40	进击的凯撒	桂林电子科技大学	5G物联区块链共享租赁平台	CACR2021IJW91I	软件设计	武小年	丁勇	李静怡，答乐梅，曹亚南
41	郑州烩面	国网河南省电力公司电力科学研究院	基于国密算法的电力物联网RFID认证方案	CACR2021FWEMT9	工程实践	吕卓	吕卓	李鸣岩，伦迪，陈萌萌
42	crypto_team1	哈尔滨工业大学（深圳）	基于TFHE的多密钥全同态机器学习工具集	CACR2021UETXHE	程序编制	蒋琳	蒋琳	段灏，谭泽玖，王泓潇
43	干饭且用盆	海南大学	面向智能家居的密码分析与防护	CACR20216668LQ	工程实践	欧嵬	欧嵬	高硕，张睿劼，史晨辉
44	好想天天睡大觉	海南大学	车联网环境中智能充电桩的密码分析与防御	CACR2021ZNK53D	工程实践	欧嵬	欧嵬	王启超，刘毅寒，李培荣
45	差不多队	海南大学	基于国密的电子签章系统在疫情防控中的应用	CACR2021A548C3	软件设计	欧嵬	岳秋玲	朱亚玲，曾墨轩，翁方宸
46	LovelyCabbage	杭州电子科技大学	基于同态加密的数据库隐私保护方案设计实现	CACR2021UWKSNK	软件设计	游林	胡耿然	陈旭泓，陈睿齐，姚乐
47	未名战队	杭州师范大学	支持细粒度控制文件分享的加密云盘	CACR20217FJLTQ	软件设计	刘雪娇	王圣宝	周鑫，王杨波，郑超逸
48	Random	河南师范大学	基于区块链的多方协作僵尸网络检测	CACR20213B8J5J	软件设计	张恩	张恩	秦磊勇，陈宛桢，王吉祥
49	黑龙江大学密码技术竞赛1队	黑龙江大学	基于属性基和区块链的电力数据隐私保护系统	CACR2021PI4JEL	软件设计	张可佳	李菊雁	王琦，祝小毓，乔芷琪
50	我们队名很长你忍一下队	湖北大学	SM4算法软件快速实现	CACR20211ZO4Z8	工程实践	曾祥勇	向泽军	徐润擎，刘勇，陈思维
51	HUBUer	湖北大学	低异或门数MDS矩阵的实现和快速搜索	CACR20218LU8S6	软件设计	曾祥勇	曾祥勇	洪春雷，徐锐，王石
52	504小队1号	湖北工业大学	轻量级公平会议地点确定位置服务隐私计算	CACR2021BP39I6	软件设计	阮鸥	沈华	李博轮，尹寻，李继强
53	锁好门	华南师范大学	SM2/4算法白盒实现自动化分析工具	CACR2021W9RGQA	工程实践	龚征	龚征	汤宇锋，邓伟杰，邓童夏
54	哦哦好的	暨南大学	基于hash算法的分组数据加密软件	CACR2021N87WAX	软件设计	赖俊祚	赖俊祚	宋贝贝，朱易明，黄连冠

55	没有bug队	江苏大学	车联网中无中心身份认证及密文检索系统设计	CACR2021VAKN3Q	软件设计	韩牟	韩牟	危李霞，王诗佳，王定轩
56	图灵三人组	江苏大学	车内网络中一次一密属性基通信系统设计	CACR20215Q64DW	软件设计	韩牟	韩牟	吴帅，朱梦丽，程彭洲
57	涅槃小队	江苏科技大学	基于对话加密的临时会话系统	CACR2021JNXLBF	软件设计	李会格	李会格	吴宇航，吴昊，杜亮
58	IS	金陵科技学院	基于物理不可克隆函数的车联网安全通信系统	CACR2021A5VODK	软件设计	柳亚男	柳亚男	孙腾，刘浩源，王欣
59	安全小能手	兰州理工大学	基于优化混沌映射的图像加密算法设计与实现	CACR2021OJ88MF	软件设计	郭显	郭显	王怡暄，陈玲，仲邦财
60	无名之辈	南京理工大学	适用于医疗影像的隐私保护联邦学习系统	CACR2021PL65XH	软件设计	许春根	付安民	王尚，戴值洋，赵家雪
61	不知道叫什么	南京理工大学	基于FPGA的同态加密算法的快速实现	CACR2021NBUWH7	硬件制作	许春根	窦本年	徐承志，杨蒙蔚，陶洪耀
62	没有密码	南京理工大学	加强数据隐私保护的安全人脸识别系统	CACR2021MZL18H	软件设计	许春根	黄婵颖	许全义，李伟琦，蒋浩
63	ANDXOR	南京师范大学	S盒及压缩函数的密码学性质检测工具箱	CACR202164YGZN	软件设计	陆阳	孙银霞	李进，李盈盈，王苇苇
64	题目都会做	南京信息工程大学	SM2的倍点运算快速实现	CACR2021LCC5PT	工程实践	展翔	袁程胜	翟浩达，陶英健，杨威
65	格兰芬多	南京邮电大学	隐私保护的Covid-19密接者追踪系统	CACR2021JSOKSO	软件设计	王志伟	王志伟	肖华，刘驰，李星宇
66	Halycon	南开大学	ECC数乘加速在零知识证明系统中的应用	CACR2021IR5MJG	软件设计	刘哲理	苏明	文周之，杨浩然，蒋泽恩
67	Dedup	南开大学	基于多密钥NTRU的加密去重系统	CACR2021AP7NVH	软件设计	刘哲理	贾春福	谢子瑜，葛晓炜，黄艺璇
68	密码小组1	青岛科技大学	基于零知识证明的轻量级环签名	CACR2021ULM9GM	理论课题	王玲玲	王玲玲	曹中达，周朋，赵雪芹
69	青藏密码先锋	青海大学	隐私保护的可信精准就医推荐模型	CACR2021G6GK9L	软件设计	谢永	谢永	曹海艳，翟浩楠，苏醒
70	WLT_hooray	武汉大学	基于SIMD指令集的SM2算法优化实现	CACR2021VB7L49	软件设计	何德彪	彭聪	韦薇，童亦雯，刘钰琳
71	旅行者	武汉大学	SM2数字签名私钥的恢复	CACR2021B6EADA	工程实践	何德彪	何德彪	朱郭诚，朱鑫杰，白野
72	NullPointerException	武汉大学	基于SM2的环签名高速实现及其应用	CACR2021QRIDTS	软件设计	何德彪	彭聪	黄俊，郑航城，雷斗威
73	Cry_战队	西安电子科技大学	分布式环境下基于SM9的轻量级身份认证	CACR2021FM3CK5	软件设计	张宁	李学俊	徐斐，赵清扬，刘涛
74	怎么都做不队	西安电子科技大学	云加密图像可验证检索系统设计	CACR2021YMBFF1	软件设计	张宁	王剑锋	苏媛媛，王汇轩，刘喜超
75	no_Error	西安电子科技大学	基于国密的选择性身份认证系统	CACR20219WV2VC	软件设计	张宁	王鹤	詹美杰，马慧，杨泽霖
76	嘤嘤嘤	西安电子科技大学	基于SM3的多熵源真随机数生成器	CACR20219Z6JX8	硬件制作	张宁	苏锐丹	胡夏南，吴灿，董梦迪
77	对对对对队	西安电子科技大学	国密SM2算法高吞吐量优化与实现	CACR2021XTHBWR	软件设计	张宁	朱辉	刘兴东，李临风，黄煜坤
78	我们一定好好学密码学	西安电子科技大学	基于SGX的动态密文数据库可信检索系统	CACR2021YLWE6J	软件设计	张宁	王剑锋	雍辛为，安淑贞，吴姣姣
79	咕咕咕	西安电子科技大学	基于国密优化RISC-V核的IoT应用	CACR2021DH73AV	硬件制作	张宁	张宁	蒋凯安，刘优然，秦研
80	别碰我的私钥	西安邮电大学	基于SM3和对称信息隐藏的图像自认证系统	CACR2021YUBZJM	软件设计	郭瑞	任方	修海燕，郝艳莉，于明宇
81	PT	西安邮电大学	基于国密算法的区块链电子投票选举系统	CACR2021TW3AO8	软件设计	郭瑞	郭瑞	徐磊，魏鑫，陈丽
82	XUPTcrypto1	西安邮电大学	基于DPSI-CA的隐私保护接触追踪系统	CACR2021AEC4LT	软件设计	郭瑞	赵艳琦	杨耿，尚利蓉，杜田
83	天生有范	长沙理工大学	基于弱可链接性环签名的匿名检举系统	CACR2021E9YNMX	软件设计	张煌	张煌	赵玎娜，宋坪容，陈宇翔
84	ESC队	浙江工商大学	基于区块链的防摄屏数字水印系统	CACR2021L74MRS	软件设计	洪海波	朱东海	曹娟，刘力帆，阮傲琦
85	郑县小民	郑州大学	基于同态加密和差分隐私的联邦学习方案设计	CACR2021DMXM1B	软件设计	李妍	王志华	张哲源，郑方冰，刘睿恒
86	FLXG大胜利	中国科学技术大学	基于混沌映射的置乱技术的密码学性质检测	CACR2021J2DJJA	软件设计	李卫海	李卫海	张浩繁，郑济中，童宇
87	0error0warning	中国科学院信息工程研究所	基于国密算法的足熵软件随机数发生器	CACR20212MSVC7	软件设计	马原	马原	杜铭枢，韩东池，顾伟嵩
88	3W战队	中国科学院信息工程研究所	国密算法的同态实现	CACR2021L93JMP	软件设计	马原	贾仃仃	李智豪，王睿达，魏本强
89	ZLNCAUC	中国民航大学	基于国密和区块链的GNSS导航电文认证	CACR2021ISPA29	工程实践	吴志军	吴志军	张媛，梁铖，聂嘉
90	123	中国人民解放军战略支援部队信息工程大学	密码协议的形式化安全分析平台	CACR2021D492TU	软件设计	陆思奇	陆思奇	李兆轩，韩庆迪，苗旭阳
91	我们整好了	中国人民解放军战略支援部队信息工程大学	基于概率型视觉密码的医学图像隐私保护系统	CACR2021GVLG38	工程实践	陆思奇	付正欣	郑为福，王子阳，黄航璎
92	冲进决赛圈	中国人民解放军战略支援部队信息工程大学	基于视觉密码的医疗隐私保护系统	CACR2021XDLFCV	软件设计	陆思奇	胡浩	刘子涵，周逸群，刘桂林

93	lcw零零后	中国人民解放军战略支援部队信息工程大学	基于FPGA的轻量级SM2算法硬件实现	CACR20219JSWHE	硬件制作	陆思奇	房礼国	柳兴邹，王朝丙，曹康乾
94	专业团队	中国人民解放军战略支援部队信息工程大学	轻量级分组密码关键组件安全性评估软件	CACR2021ZHIQO3	软件设计	陆思奇	任炯炯	马璋君，许子昂，刘嘉硕
95	英特纳雄耐尔就一定要实现	中国人民解放军战略支援部队信息工程大学	基于区块链的多方共识自媒体监管系统	CACR2021HVUOG7	软件设计	陆思奇	胡浩	段小琼，李振东，李飞扬
96	信星	中国人民解放军战略支援部队信息工程大学	隐私保护的人脸识别系统设计与实现	CACR2021HOQQYM	软件设计	陆思奇	赵秀凤	姜迎畅，李俊杰，李嘉豪
97	求锦鲤	中国人民解放军战略支援部队信息工程大学	基于深度学习的密码算法模拟与实现	CACR20212PI9VB	工程实践	陆思奇	任炯炯	万靖国，朱明亮，蔡柳佳
98	密联二分队	中山大学	基于区块链的公平对称可搜索加密实现	CACR2021Z3ISFQ	工程实践	田海博	张方国	梁岫琪，叶婉，陈建彰
99	白客队	中央财经大学	序列密码的分析	CACR202156GUT4	软件设计	段美姣	武霞	娄健越，胡成韬，潘守飞
100	九头蛇万岁	重庆交通大学	面向电力领域的基于国密算法的联邦学习框架	CACR20217WWZZA	软件设计	米波	米波	匡航冬，马浩宇，翁渊
101	三个顶俩	重庆邮电大学	支持Top-k查询的LBS数据隐私保护	CACR20211YW3DP	软件设计	周由胜	刘媛妮	何沅霖，张浩冬，陈裕杰