附件2

全国密码算法设计竞赛公钥加密算法第二轮入选名单

|  |  |  |  |
| --- | --- | --- | --- |
| 排名 | 算法名称 | 第一设计者 | 参与设计者 |
| 1 | LAC.PKE | 路献辉（中国科学院信息工程研究所信息安全国家重点实验室） | 刘亚敏（中国科学院信息工程研究所信息安全国家重点实验室）贾仃仃（中国科学院信息工程研究所信息安全国家重点实验室）薛海洋（中国科学院信息工程研究所信息安全国家重点实验室）贺婧楠（中国科学院信息工程研究所信息安全国家重点实验室）张振飞（Algorand）李宝（中国科学院信息工程研究所信息安全国家重点实验室）王鲲鹏（中国科学院信息工程研究所信息安全国家重点实验室） |
| 2 | Aigis-enc | 张江（密码科学技术国家重点实验室） | 郁昱（上海交通大学）范淑琴（密码科学技术国家重点实验室）张振峰（中国科学院软件研究所）杨糠（密码科学技术国家重点实验室） |
| 3 | AKCN-MLWE | 赵运磊（复旦大学） | 程蕾晓（复旦大学）金正中（复旦大学）巩博儒（复旦大学）吴洪祥（银联商务股份有限公司）隋光烨（上海扈民区块链科技有限公司）张振峰（中国科学院软件研究所） |
| 4 | Piglet-1 | 王丽萍（中国科学院信息工程研究所） | 彭力强（中国科学院信息工程研究所）蔡家豪（中国科学院信息工程研究所）戚艳红（中国科学院信息工程研究所） |
| 5 | TALE | 潘彦斌（中国科学院数学与系统科学研究院） | 李昊宇（中国科学院数学与系统科学研究院）谢天元（中国科学院数学与系统科学研究院）刘珍（中国科学院数学与系统科学研究院）杨照民（中国科学院数学与系统科学研究院）朱熠铭（中国科学院数学与系统科学研究院） |
| 6 | AKCN-E8 | 赵运磊（复旦大学） | 刘哲（南京航空航天大学）金正中（复旦大学）巩博儒（复旦大学）隋光烨（上海扈民区块链科技有限公司）刘伟超（银联商务股份有限公司）文黎明（银联商务股份有限公司） |
| 7 | SCloud | 郑中翔（清华大学） | 王安宇（中国科学院信息工程研究所）樊海宁（清华大学）赵春欢（清华大学）刘超（山东大学）张雪（清华大学） |

全国密码算法设计竞赛数字签名算法第二轮入选名单

|  |  |  |  |
| --- | --- | --- | --- |
| 排名 | 算法名称 | 第一设计者 | 参与设计者 |
| 1 | Aigis-sig | 张江（密码科学技术国家重点实验室） | 郁昱（上海交通大学）范淑琴（密码科学技术国家重点实验室）张振峰（中国科学院软件研究所）杨糠（密码科学技术国家重点实验室） |
| 2 | 木兰 | 赵运磊（复旦大学） | 巩博儒（复旦大学）程蕾晓（复旦大学）文黎明（银联商务股份有限公司）谢群松（银联商务股份有限公司）陈如钢（上海扈民区块链科技有限公司）任思溟（银联商务股份有限公司）吴洪祥（银联商务股份有限公司） |
| 3 | FatSeal | 潘彦斌（中国科学院数学与系统科学研究院） | 李昊宇（中国科学院数学与系统科学研究院）谢天元（中国科学院数学与系统科学研究院）刘珍（中国科学院数学与系统科学研究院）杨照民（中国科学院数学与系统科学研究院）朱熠铭（中国科学院数学与系统科学研究院） |
| 4 | PKP-DSS | 林东岱（中国科学院信息工程研究所） | J.-C.Faugère(CryptoNext,INRIA and Sorbonne University）X.HAN（Orange Labs,France）E.Kousaa（University of Versailles）G.Macario-Rat（Orange Labs）J.Patarin（University of Versailles,CNRS）L.Perret（CryptoNext,Sorbonne University and INRIA） |

 全国密码算法设计竞赛密钥交换算法第二轮入选名单

|  |  |  |  |
| --- | --- | --- | --- |
| 排名 | 算法名称 | 第一设计者 | 参与设计者 |
|  | SIAKE | 薛海洋（中国科学院信息工程研究所信息安全国家重点实验室） | 路献辉（中国科学院信息工程研究所）王鲲鹏（中国科学院信息工程研究所）田松（中国科学院信息工程研究所）徐秀（中国科学院信息工程研究所）贺婧楠（中国科学院信息工程研究所）李宝（中国科学院信息工程研究所） |
|  | SKCN-MLWE | 赵运磊（复旦大学） | 程蕾晓（复旦大学）金正中（复旦大学）巩博儒（复旦大学）吴洪祥（银联商务股份有限公司）隋光烨（上海扈民区块链科技有限公司）张振峰（中国科学院软件研究所） |
|  | LAC.KEX | 路献辉（中国科学院信息工程研究所信息安全国家重点实验室） | 刘亚敏（中国科学院信息工程研究所信息安全国家重点实验室）贾仃仃（中国科学院信息工程研究所信息安全国家重点实验室）薛海洋（中国科学院信息工程研究所信息安全国家重点实验室）贺婧楠（中国科学院信息工程研究所信息安全国家重点实验室）张振飞（Algorand）李宝（中国科学院信息工程研究所信息安全国家重点实验室）王鲲鹏（中国科学院信息工程研究所信息安全国家重点实验室） |