

在路上 ON THE ROAD



WAPI产业联盟公众号



金蛇添福

2025

CHINESE
NEW YEAR



理事成员：

中国移动通信集团公司
中国电信集团有限公司
中国联合网络通信集团有限公司
国家密码管理局商用密码检测中心
国家无线电监测中心检测中心
西电捷通公司
北大方正集团有限公司
北京中电华大电子设计有限责任公司
中电科普天科技股份有限公司
深圳市明华澳汉智能卡有限公司
北京数字认证股份有限公司

WAPI产业联盟

理事长：曹军
秘书长：张璐璐

《在路上 On The Road》编辑部

主 编：张璐璐
编 辑：周园 刘剑昕
王立华 陈博

美术编辑：周园

WAPI产业联盟秘书处

会员服务部 标准化部 市场与产业部
测试实验室 综合管理部

联络单位

ISO/IEC JTC 1/SC 6中国对口委员会
工业和信息化部宽带无线IP标准工作组

联系方式

地 址：北京海淀区知春路27号量子芯座1608室
邮 编：100191
电 话：010-82351181
传 真：010-82351181 ext.1901
邮 箱：wapi@wapia.org zhouy@wapia.org
网 站：<http://www.wapia.org.cn>
公众号：



WAPI产业联盟公众号

新春致禧 Happy Chinese New Year

05 WAPI产业联盟恭贺新春

媒体聚焦 Media Focus

06 新华社：中国将牵头制定抗量子攻击的通信网络安全协议设计指南

09 通信世界等：首批三款低功耗模组通过WAPI协议基础要素测评

特别报道 Special Report

11 第一观察：抓科技创新，总书记反复强调“迫切”

联盟关注 Alliance Concerns

14 新华时评：中央经济工作会议 | 坚持以质取胜和发挥规模效应相结合

WAPI 问答 WAPI FAQ

15 WAPI 问答（系列连载）第十二部分（PART 12）

产经要闻 Industrial & Economic News

21 习近平：努力建设一支强大的现代化信息支援部队推动我军网络信息体系建设跨越发展

21 丁薛祥：推动构建网络空间命运共同体迈向新阶段

22 中共中央办公厅 国务院办公厅：保障新型城市基础设施网络和数据安全

22 金壮龙：全面深化改革，有效应对重大风险挑战

23 中国人民银行等七部门：落实科技自立自强战略，加强数据和网络安全防护

23 尹力：推动北京国际科技创新中心建设迈向更高水平

联盟工作 Alliance Work

- 24 WAPI产业联盟参加“红色之旅·走进怀柔第一党支部纪念馆”主题党日活动
- 25 WAPI产业联盟参加“关爱生命 救在身边 党员先行”应急救护知识培训主题党日活动
- 26 WAPI产业联盟发布《关于安全无线局域网高质量发展的通告》
- 29 无线网络安全标准化委员会2024年第四次主任委员会议（总第11次）顺利召开
- 30 第三届无线网络安全标准化委员会第五次会议成功召开
- 33 南网数网科技“电鸿”系列低功耗WAPI模组 通过联盟测评
- 34 智开科技WAPI系列产品通过联盟测试

成员与市场 Member & Marketing

- 35 南网超高压公司在国内率先实现所辖站点WAPI无线局域网全覆盖
- 36 国网冀北唐山供电公司创新应用WAPI技术 实现低压分布式光伏直采直控
- 37 宁夏首次在750千伏变电站应用蓄电池远程核容养护系统 探索并入沙湖WAPI网络
- 38 国家电网命名20支国际标准化创新团队
- 40 华信傲天携手伟仕佳杰 制造业数字化转型新篇章
- 40 华为参加2024年通信新技术暨配电通信技术专题交流论坛
- 41 高通发布骁龙8至尊版移动平台 支持WAPI
- 41 MTK发布天玑9400移动芯片 支持WAPI
- 42 西电捷通、中兴微、华为等联盟会员在2024年数据通信标准化会上分享标准情况
- 43 谨慎采购美国芯片 中国互联网协会等四协会发声

产业技术论坛 Industry & Technology Forum

- 45 面向量子时代安全需求的WAPI 2.0技术标准体系

尊敬的专家、领导、业界同仁：

日月其迈，时盛岁新，又是一年春来到。籍此贺卡，呈递我们的惦念，祝您和家人：春祺夏安，秋绥冬禧！也向您汇报WAPI标准产业共同体持续保障网络基础连接安全的进展和成绩。

2024年，产业链上下游围绕“以应用促发展，共建高质量安全无线局域网”，扎实推进WAPI建设。为电力、国防等诸多行业提供了安全稳定、高速可靠的通信方式，支撑了新型行业系统构建，促进了传统行业赋能，增进了劳动者福祉。伴随应用场景的不断丰富，更多厂商加入WAPI产业，让标准链、产业链、供应链持续壮大。190余项国际国家行业团体标准，持续发挥基础引领作用，新一届标委会正面向量子时代的网络安全布局谋篇。联盟公共服务平台，为关键基础技术、产品、测评、网络系统建设等提供高效支撑保障，本年度通过联盟测试测评的WAPI新产品已近百款。

网络安全是网络强国建设的坚实保障。新的一年，希望继续和您一起努力拼搏，为筑牢国家网络安全屏障作出积极贡献！

WAPI产业联盟（中关村无线网络安全产业联盟）

无线网络安全标准化委员会

工业和信息化部宽带无线IP标准工作组

ISO/IEC JTC1/SC6国内技术对口单位

无线网络安全技术国家工程研究中心

甲辰年岁末

电贺新春

新华社：

中国将牵头制定抗量子攻击的通信网络安全协议设计指南

【编者按】当前全球标准组织和各国均在开展行动，应对量子计算机带来的安全挑战。日前中国专家在瑞典斯德哥尔摩举行的ISO/IEC JTC1/SC6（系统间远程通信和信息交换）会议上，就如何设计抗量子攻击的通信网络安全协议提交提案并获会议一致通过，将由中国专家牵头推进制定协议设计指南。这一举措，将为全球通信网络向后量子密码迁移提供引导。对此，新华社、新华网、中新社、人民网、光明网、中国经济网、中国法院网、中国证券报等媒体发布报道。

以下是新华社的报道：



新华社北京10月28日电（记者刘羽佳）记者日前从WAPI产业联盟获悉，近日在瑞典斯德哥尔摩举行的ISO/IEC JTC1/SC6（系统间远程通信和信息交换）会议上，中国专家就如何设计抗量子攻击的通信网络安全协议提交提案并获会议一致通过，会议决议成立预备工作项目，由中国专家牵头推进制定协议设计指南。量子

时代到来后，现有通信网络安全协议变得不再安全。此次我国针对协议设计问题提交提案，将促进全球数据通信系统更平稳地从传统密码算法时代过渡到后量子密码算法时代，避免量子计算机给现有使用传统公钥密码体系的通信系统带来较大安全威胁。据介绍，随着量子计算的发展，全球基于传统密码算法的通信协议和系统皆面临颠覆性挑战。虽然可商用量子计算机的发布尚无确切时间表，但其给全球网络空间带来的挑战已经切实存在，目前已有攻击者开始收集和存储一些重要数据，留待未来使用量子计算机进行破解以获取重要信息。“为此全球标准组织和各国均在推进行动计划，应对量子计算机带来的安全挑战。本次中国专家提交的国际提案，旨在为全球通信网络向后量子密码迁移提供引导。”WAPI产业联盟秘书长张璐璐表示。据悉，WAPI产业联盟参加了提案论证，西电捷通公司是提案的主要技术贡献者。西电捷通公司总经理曹军表示，西电捷通公司数年前就开始研究抗量子攻击的网络安全协议，此次正式提交国际提案，是在向后量子时代迁移的历史进程中，中国科技创新力量为构建共享共治的网络空间命运共同体做出的贡献。记者从2024量子科技标准与产业化大会了解到，西电捷通公司等中国企业已经在无线局域网领域开展了抗量子攻击的通信安全协议设计实践，发布了具有抗量子攻击能力的新一代WAPI技术。

部分媒体新闻链接：

新华社：<https://h.xinhuanet.com/vh512/share/12253322?d=134da84&channel=weixin&time=1730104976429>

新华网：<http://www1.xinhuanet.com/20241028/5d10f8bc8f9241f6b5cd0fee2cbb8708/c.html>

中新社：<https://www.chinanews.com.cn/cj/2024/10-28/10309480.shtml>

人民网：<http://finance.people.com.cn/n1/2024/1028/c1004-40348899.html>

光明网：https://tech.gmw.cn/2024-10/28/content_37641759.htm

中国经济网：http://tech.ce.cn/news/202410/29/t20241029_39184033.shtml

中国证券报：https://cs.com.cn/xwzx/hg/202410/t20241028_6449528.html

证券时报：<http://www.stcn.com/article/detail/1374549.html>

国际时报网：<http://news.cwan.com/pandian/2024/1028/98589.html>

环球传媒网：<http://joke.lygmedia.com/joke/20241028/28292723.html>

澎湃新闻：https://www.thepaper.cn/newsDetail_forward_291676

中国工信新闻网：https://www.cnii.com.cn/tx/202410/t20241028_611406.html

中经头条：<https://mp.weixin.qq.com/s/TwY7j-sw9ybT7ToIyxVDbg>

中国法院网：<https://www.chinacourt.org/article/detail/2024/10/id/8169380.shtml>

正义网：https://news.jcrb.com/jsxw/2024/202410/t20241028_6702033.html

中工网：<https://www.workercn.cn/c/2024-10-28/8379996.shtml>

西藏网信办：https://wxb.xzdw.gov.cn/wlaq/aqdt/202410/t20241029_520999.html

通信世界: <http://www.cww.net.cn/article?id=594941>

网易: <https://www.163.com/dy/article/JFJKUL1F05346RC6.html?spss=dy-author>

凤凰科技: <https://tech.ifeng.com/c/8e39Zx72TCH>

千龙网: <https://china.qianlong.com/2024/1028/8365499.shtml>

新浪财经: <https://finance.sina.com.cn/jjxw/2024-10-29/doc-incuehuh2221045.shtml>

京报网: <https://news.bjd.com.cn/2024/10/28/10950035.shtml>

上海证券报: <https://www.cnstock.com/commonDetail/294182>

东方财富网: <https://finance.eastmoney.com/a/202410283219588136.html>

太平洋财富网: <http://www.pcfortune.com.cn/news/yuanchuang/2024/1028/197169.html>

重庆日报: https://epaper.cqrb.cn/cqrb/2024-10/29/009/content_rb-338587.htm

扬子晚报: <https://www.yangtse.com/zncontent/4106109.html>

河北新闻网: https://world.hebnews.cn/2024-10/28/content_9254158.htm

齐鲁网: <http://news.iqilu.com/china/gedi/2024/1028/5734631.shtml>

长江网: http://news.cjn.cn/bsy/gjxw_19789/202410/t5021796.htm

东南网: http://news.fjnen.com/2024-10/28/content_31765885.htm

云南网: <https://news.yunnan.cn/system/2024/10/28/033281836.shtml>

胡杨网: http://www.huyangnet.cn/content/2024-10/28/content_1927798.html

广西新闻网: <http://www.gxnews.com.cn/staticpages/20241028/newgx671fa186-21659660.shtml>

西安网: <https://news.xiancity.cn/system/2024/10/28/031167198.shtml>

哈尔滨新闻网: <https://www.my399.com/p/387762.html>

齐鲁壹点网: <https://www.ql1d.com/general/25001688.html>

兰州新闻网: https://www.lzbs.com.cn/gnnews/2024-10/29/content_506546134.htm

滁州网: <http://www.chuzhou.cn/2024/1028/500474.shtml>

环渤海新闻网: https://news.huanboha inews.com.cn/2024-10/28/content_50378635.html

高陵经济网: <http://www.glxcb.cn/jiaoyu/2024/1028/248372.html>

福建网络广播电视台: <https://www.fjtv.net/folder331/2024-10-28/6231135.html>

今报在线: <http://shipin.jinbaonet.com/shipin/2024/1028/2000170499.html>

通信世界等：

首批三款低功耗模组通过WAPI协议基础要素测评

【编者按】2024年12月4日，北京联盛德微电子有限责任公司型号为WM6180的低功耗WAPI模组和南方电网数字电网科技（广东）有限公司型号为SWKJ-DH-H001、SWKJ-DH-L001的低功耗电鸿WAPI通信模组，首批通过WAPI协议基础要素测评。通信世界、中国信息化周报、信息主管网、飞象网等媒体对此进行了报道。

以下是通信世界的报道：



日前记者从WAPI产业联盟获悉，北京联盛德微电子有限责任公司型号为WM6180的低功耗WAPI模组和南方电网数字电网科技（广东）有限公司型号为SWKJ-DH-H001、SWKJ-DH-L001的低功耗电鸿WAPI通信模组，首批通过WAPI协议基础要素测评。

随着WAPI广泛服务各行各业，传感器、手持终端等类业务终端产品，大多通过集成低功耗WAPI模组快速具备WAPI功能。但据反馈，目前市场上有一部分低功耗WAPI模组以及集成了低功耗WAPI模组的终端产品，没有采用具有符合国家密码主管部门批准算法能力的安全芯片对密钥进行安全存储和执行密码运算（包括国家密码管理局第7号公告发布的无线局域网专用商密算法ECDSA、ECDH、SHA-256，以及通用商密算法SM2/3/4）。这种风险与WAPI安全协议技术本身无关，属于产品工程实现层面的问题。但存在密钥泄露的安全风险，易导致“非法设备获得合法身份”，影响用户整体方案的安全性。



WAPI产业联盟对此高度重视，并根据市场用户安全管理需求，启动了针对低功耗WAPI模组以及集成了低功耗WAPI模组的终端产品的WAPI协议基础要素测评能力建设与服务，用于检验产品是否采用了具有符合国家密码主管部门批准算法能力的安全芯片对密钥进行安全存储和执行密码运算。从产品工程实现层面，防范安全风险。

在管理规范方面，WAPI测试实验室依据GB/T19001-2016 idt ISO 9001:2015国际质量管理体系要求，制定了严格的测评服务业务规范和管理流程。在测评实施方面，与模组厂商、芯片厂商、检测机构等进行了充分沟通与论证，形成了科学全面的测评方法。

自2024年8月服务启动以来，产业市场反响热烈，多家厂商咨询并提交了测评申请。

部分媒体新闻链接：

通信世界：<http://www.cww.net.cn/article?id=595623>

中国信息化周报/信息主管网：www.cio360.net/show-598-103907-1.html

飞象网：<http://www.cctime.com/html/2024-11-25/1697221.htm>

第一观察：

抓科技创新，总书记反复强调“迫切”

国际在线

2024年11月5日，习近平总书记考察武汉产业创新发展研究院，了解推进科技创新的举措。

我们通过梳理发现，党的二十大之后，习近平总书记考察广东、河北、内蒙古、上海等20多个省份，都谈到了科技创新。就在上个月，总书记刚刚察看安徽省重大科技创新成果集中展示。

不只是地方考察。从今年中央政治局首次集体学习到全国两会看望政协科技界委员，再到中央深改委会议，全国科技大会、国家科学技术奖励大会、两院院士大会……习近平总书记密集调研、部署。

2035年建成科技强国。正如总书记所强调的：“实现中华民族伟大复兴时不我待，要进一步增强科技创新的紧迫性”“通过创新引领和驱动发展已经成为我国发展的迫切要求”“必须进一步增强紧迫感，进一步加大科技创新力度”。

快马加鞭、不进则退的紧迫感，源于对时与势的深刻判断。

向外看，“当今世界正经历百年未有之大变局，科技创新是其中一个关键变量”“围绕科技制高点的竞争空前激烈”。同时，来自外部的打压遏制随时可能升级，“脱钩断链”“小院高墙”风险加剧，迫切需要加快高水平科技自立自强，从而把握历史主动、发展主动。

向内看，中国式现代化之路行进到关键节点，产业转型升级、新旧动能转换爬坡过坎，抓住这一轮科技革命和产业变革带来生产力跃升机遇，将推动我国科技和产业发展由“跟随者”向“引领者”转变。

科技创新在推动高质量发展、推进中国式现代化中的位势和作用更加突出。以高水平科技自立自强的“强劲筋骨”支撑民族复兴伟业，是迫切要求，是必然选择。

“对科技创新和产业创新融合提出了更为迫切的需求”——

2013年、2018年、2022年、2024年，习近平总书记多次赴武汉考察，始终关切科技创新、科技自立自强、科技成果转化等问题。

这一次，在武汉产业创新发展研究院，总书记的一番话意涵深刻：“实现高水平科技自立自强、发展新质生产力，对科技创新和产业创新融合提出了更为迫切的需求。”

推进现代化建设，要靠科技强国、产业强国。从科技到产业，成果转化是将科技创新优势转化为经济发展动力的重要和必然途径。

一次次科技和产业革命，带来一次次生产力提升。推进中国式现代化，必须形成高度发达的生产力。依托我国产业基础优势和超大规模市场优势，以关键核心技术突破推动产业向中高端攀升，产业创新就能更高水平、更富效率，新质生产力就更发达，发展就更高质量。

在今年全国两会上，一名政协委员谈到“我国企业专利转化还有较大空间。创新链与产业链‘相望难相见’，是阻碍新质生产力形成的卡点”的现实困境。

对此，总书记指明破解之道：“特别是企业自身直接研发形成成果转化，院校和企业形成共同体，这样的趋势、方向是对的，要快马加鞭，把激励、促进政策进一步抓好。”

在6月召开的全国科技大会、国家科学技术奖励大会、两院院士大会上，总书记阐明推动科技创新和产业创新深度融合的路径，“融合的基础是增加高质量科技供给”“融合的关键是强化企业科技创新主体地位”“融合的途径是促进科技成果转化应用”。

总书记此次在武汉产业创新发展研究院，察看科技创新供应链平台成功案例展示，具有很强的针对性。而“武创院”就是一家新型研发机构，链接高校院所、龙头企业、投资机构等创新资源，助推高校院所的研发成果与企业需求精准匹配、高效落地，着力破解成果转化“最后一公里”难题。

总书记提出这一“迫切”要求，为科技创新和产业创新融合发展、加大科技成果转化应用力度按下了快进键。

“加强基础研究，是实现高水平科技自立自强的迫切要求”——

当前，国际科技竞争向基础前沿前移。加强基础研究、从源头和底层解决关键技术问题，是应对国际科技竞争、实现高水平自立自强的迫切需要。

总书记曾指出：“基础研究处于从研究到应用、再到生产的科研链条起始端，地基打得牢，科技事业大厦才能建得高。”基础研究的突破、核心技术的攻关，往往能够带来生产力的深刻变革和社会的巨大进步。

在河北了解药品研发生产情况，强调“加强基础研究和科技创新能力建设”；中央政治局就量子科技研究和应用前景举行集体学习时，强调“量子科技发展取决于基础理论研究的突破”；此次在武汉，强调“加强关键核心技术研发攻关”。

面对国内外发展新形势，只有把科技的命脉牢牢掌握在自己手中，破解“卡脖子”问题，才能以自身发展的独立性、自主性、安全性应对形势变化的不确定性。

“推进自主创新，最紧迫的是要破除体制机制障碍”——

习近平总书记曾指出，“科技领域是最需要不断改革的领域”“科技创新、制度创新要协同发挥作用，两个轮子一起转”“推进科技创新，必须破除体制机制障碍”。

当前，我国科技创新能力不断提升，但在科技成果转化、知识产权保护、科研评价体系等方面仍存在一些体制机制问题，导致创新资源配置不均衡、创新主体活力不足、创新成果转化效率偏低等，影响和制约着科技创新的整体效能和新质生产力的发展。

从党和国家机构改革组建中央科技委员会，到党的二十届三中全会提出构建支持全面创新体制机制，对深化科技体制改革作出一系列重要部署。深化科技体制改革、提升国家创新体系整体效能的统筹部署不断提速。

此次在武汉，总书记强调“围绕重点产业强化创新链产业链资金链人才链融合”“构建大中小企业协同创新机制，提升科技成果转化水平”。

“融合”“协同”“机制”……这些关键词道出解决转化问题，就要通过深化改革，疏解科技创新链条上不顺不畅体制机制关卡，打通从科技强到产业强、经济强、国家强的通道，形成科技创新和产业创新深度融合的局面。

创新是一个系统工程，创新链、产业链、资金链、政策链相互交织、相互支撑。科技创新和制度创新“双轮驱动”，以形成支持全面创新的基础制度，最大程度调动创新主体的积极性，最大限度解放和激发科技作为第一生产力所蕴藏的巨大潜能。

当前，正处于进一步打造生产力优势的重要关头。面对风起云涌的科技革命、产业变革，发展的机遇稍纵即逝。

推动科技创新，习近平总书记提出“迫切”要求，就是要把握机遇，不可等待观望，当有只争朝夕的劲头；要锚定重点，洞察创新本质，看准了就抓紧干。这也是习近平总书记一贯谋事业的战略眼光、抓工作的科学方法。

新华时评：

中央经济工作会议 | 坚持以质取胜和发挥规模效应相结合

新华社

新华社北京12月19日电（记者李延霞）近日举行的中央经济工作会议提出，必须统筹好提升质量和做大总量的关系，夯实中国式现代化的物质基础。这一重要论述对做好经济工作导向鲜明、意义重大。

质量和总量，是经济发展中最重要的关系之一。当前，我国正处在加快转型升级、推进高质量发展的关键阶段，必须辩证认识、科学统筹质量和总量的关系，坚持以质取胜和发挥规模效应相结合，把质的有效提升和量的合理增长统一于高质量发展的全过程。

坚持以质取胜和发挥规模效应相结合，是时代所需、现实所需。中国式现代化对经济发展的质量、结构、规模都有很高要求。当前形势下，稳就业、防风险、惠民生，有效应对外部环境变化，都需要保持一定的经济增速，要牢牢围绕经济建设这个中心，以量的积累稳住经济发展基本盘。同时，面对新的使命任务和新的环境，要紧紧锚定高质量发展这个首要任务，完整准确全面贯彻新发展理念，加快构建新发展格局，坚持以质取胜，不断塑造竞争新优势。

坚持以质取胜和发挥规模效应相结合，我们有基础有条件有潜力。作为超大规模经济体，我国拥有巨大的经济体量、市场容量和产业配套能力，要用好超大规模市场优势和丰富的应用场景，发挥好科技创新引领作用，促进科技创新和产业创新深度融合，培育更多世界一流企业和领先技术，推动我国经济发展“质”“量”齐升、行稳致远。

坚持以质取胜和发挥规模效应相结合，需要坚持系统集成、协同配合，打出有力有效的政策“组合拳”。首次实施“更加积极的财政政策”、货币政策14年来首次转向“适度宽松”、全方位扩大国内需求、以科技创新引领新质生产力发展……会议部署的一系列举措，既着力稳定预期、激发活力，稳定经济增长，又着眼长远发展，通过深化改革释放发展潜力，提高发展质量，充分体现了对“质”与“量”的科学统筹。

统筹好经济发展中质量与总量的关系，必须贯穿于全面建设社会主义现代化国家全过程。坚持不懈、久久为功，不断实现更高质量、更有效率、更加公平、更可持续、更为安全的发展，将推动中国经济航船乘风破浪行稳致远。

WAPI 问答（系列连载）

在WAPI服务各行各业及关键信息基础设施建设的过程中，联盟总结了一些市场用户的常见问题。同时，我们注意到百度百科、搜狗百科、互动百科、维基百科中文版等对WAPI技术、标准、产业及演进历程的描述存在不准确或某些错误。为帮助大家更加客观、准确地了解WAPI，推出WAPI问答（系列连载）。

WAPI问答（系列连载）覆盖WAPI技术、标准、产品、应用、检测评估、联盟与会员等方面内容，并定期更新。文件中涉及的数据与内容，均源自公开信息。

咨询请联系：staff@wapia.org

第十二部分（PART 12）

■ 1. 问：面向量子时代，WAPI技术标准体系将如何演进和发展？在为无线局域网络提供抗量子攻击能力方面，进展如何？

答：自2003年WAPI 1.0技术标准体系形成迄今，八十余项国家、行业、团体标准陆续得到发布，标准体系不断完善，联盟测试实验室的产品和系统测试项目，已演进四个版本，持续支撑产业创新发展。

随着量子技术逐步取得突破及商业化进展的加快，使用传统密码算法的网络安全协议体系面临重大挑战，迫切需要形成新一代WLAN安全技术标准体系。因此WAPI 2.0技术标准体系的演进目标是：面向量子时代安全需求，提供抗量子攻击能力，并在身份保护、防范离线字典攻击等方面提供更高安全性，支持快速切换、确保承载的多媒体业务传输具备更高质量。2021年12月28日，WAPI产业联盟、无线网络安全标准化委员会发布了T/WAPIA 046《无线局域网安全技术规范》，这是WAPI 2.0技术标准体系的第一项标准。

T/WAPIA 046在安全性、隐私保护、应对量子计算攻击威胁和防范离线字典攻击等方面，对现有WAPI 1.0技术标准体系进行了升级与增强，主要包括：

- （1）升级采用面向量子安全的安全协议方案缓解量子威胁，降低WLAN通信系统数据“当前存储，以后破解”风险；
- （2）新增支持身份保护功能，在保障通信安全的同时保护用户隐私；
- （3）新增支持快速切换机制，满足音视频等流媒体业务无中断传输；
- （4）升级支持防范离线字典攻击，提供可靠前向安全性（PFS），防范窃听者暴力破解获得密码和通

信数据；

(5) 全面适配通用国密算法，提供更高强度安全。

同时，T/WAPIA 046兼容WAPI 1.0技术标准体系，为实际部署中提供了向新安全方案的有序过渡，适应了平滑演进、兼容互通的产业需求。

■ 2. 问：目前已经发布的基于WAPI的无线局域网技术标准有80多项，从技术演进角度看，分为几个标准体系？

答：《中共中央关于进一步全面深化改革、推进中国式现代化的决定》将进一步推动WAPI技术标准体系的建设和应用。

《决定》中22处提到“标准”，尤其是在以下两方面，将直接影响和激励WAPI技术标准体系的完善和应用：

(1) 构建全国统一大市场。推动市场基础制度规则统一、市场监管公平统一、市场设施高标准联通。WAPI产业联盟组织制定的团体标准是形成“高质量安全无线局域网”的关键基础，是对政府发布标准（国家标准、行业标准）的重要补充，并已在产品研发、检验检测、认证认可、产业应用等环节得到了广泛采信和实施，对规范、引导、服务市场起到重要作用。下一步，联盟将进一步深入完善标准体系，促进标准实施，服务于构建全国统一大市场。

(2) 完善流通体制，加快发展物联网，健全一体衔接的流通规则和标准，降低全社会物流成本。WAPI产业联盟组织创新提出的无线网络安全技术标准体系中，包含了射频识别（RFID）和近场通信（NFC）等物联网传感层安全协议，填补了我国在该领域研究的空白，已被发布为7项ISO/IEC国际标准、3项欧洲ECMA标准、9项国家/军用标准、5项行业标准，上述标准的实施将得到进一步深化。上述标准具体情况，可联系联盟标准化部：lmbz@wapia.org。

■ 3. 问：T/WAPIA 046《无线局域网安全技术规范》的实施情况如何？

答：T/WAPIA 046实施正稳步进行中。2025年上半年内将有多家联盟成员发布符合T/WAPIA 046标准的STA、AP/AC、AS等系列产品，联盟测试实验室2024年内将正式接受配套产品标准符合性委托测试，并出具测试报告。

值得关注的是，T/WAPIA 046适配了通用商密算法SM2和SM3，并持续使用SM4，对WAPI 1.0技术标准体系中WLAN安全协议内容进行了扩展，增加了适配后的机制选项，包括新增WAI2协议、快速切换机制等，在

密码算法强度、身份保护、抗离线字典攻击和应对量子计算攻击等安全性方面有显著增强，使WLAN设备持续满足合规要求、支持形成可信赖WLAN网络和服务，适用于更高安全要求的应用环境，将有效应对量子时代的新安全威胁。在实际部署方面，T/WAPIA 046兼容WAPI 1.0技术标准体系，满足实际部署中WAPI 1.0向WAPI 2.0技术标准体系的有序过渡，适应了平滑演进、兼容互通的产业需求。

T/WAPIA 046发布实施后，因其结合和兼顾了面向量子时代安全和使用通用商密算法的需求，得到业界的关注和响应。多厂商多类别产品开发、联盟测试平台能力建设，稳步推进。同时，联盟不间断地收集和响应产业应用实施过程中成员单位和业界各方提出的意见、建议，持续追求在不降低安全性的前提下，进一步减少技术演进升级的投入，将芯片等硬件系统升级的工作减至最少，在满足合规性需求的前提下，进一步保护投资。例如：标委会已针对T/WAPIA 046中WAI2协议封装及以太类型字段标识的改进，通过修改单项目立项，正在制定中。

根据联盟产业调研，实施T/WAPIA 046的典型方式是采用软件升级方式（作为软件补丁部署在WAPI 1.0标准符合性设备上），按照目前计划，未来半年内将有多个联盟成员单位发布STA、AP/AC、AS等系列符合T/WAPIA 046的产品，为行业和产业应用提供合规、兼顾面向量子时代安全和通用商密算法应用需求的产品和网络系统解决方案。联盟测试实验室已经过整备和样本测试，2024年内将正式接受成员单位的产品标准符合性委托测试，并出具测试报告，供业界采用。同时联盟将继续做好和产业、行业决策机构以及采购政策的衔接，使产业、行业能及时采用合规、具有更高安全性、面向量子时代安全需求的产品，支持保障网络服务的安全性。

■ 4. 问：在WAPI 1.0和WAPI 2.0两种技术标准体系中，安全服务可以在同一网络SSID内启用么？

答：不可以。

在产品测试和示范应用中，存在同一网络SSID内，不同版本WAPI机制并存，以及同一版本机制中证书鉴别和预共享密钥鉴别混用的情况。由于预共享密钥鉴别面临的安全管理风险较大、仅适用于满足短时间临时组网的需求，与证书鉴别机制安全性差异大，以及不同版本WAPI机制的安全等级不同，为防止降维攻击，联盟建议：应用中应避免不同版本WAPI机制，以及同一版本机制中证书鉴别和预共享密钥鉴别在同一网络中同时启用服务的做法。

■ 5. 问：在WAPI 1.0技术标准体系基础上，直接将密码算法替换为SM2/3。这种做法是否合规，为什么？

答：这种做法不合规。

目前业界存在“在现有WAPI 1.0技术标准体系的基础上，在产品开发中直接替换原有WLAN专用商密算

法、使用通用商密算法”的做法。这种做法，不是现有标准体系支持的合规方式，以这种方式开发的产品，不具备技术标准体系演进形成的新的安全能力。

WAPI产业联盟在2024年11月14日发布的《关于安全无线局域网高质量发展的通告》中，对此已做了警示和剖析。详见联盟官网http://www.wapia.org.cn/yaowen/detail_342490.shtml。

■ 6. 问：联盟2024年8月推出的WAPI协议基础要素测评服务具体指什么？解决什么问题？测试对象是什么？

答：WAPI协议基础要素测评服务用于：检验被测产品是否采用了具有符合国家密码主管部门批准算法能力的安全芯片，对密钥进行安全存储、执行密码运算，以及让密钥产生、密码运算、密钥销毁等与WAPI协议实现紧密相关的基础要素工作，是否在安全芯片内部完成，保证了“密钥不出安全芯片”的原则。

目前WAPI协议基础要素测评服务对象主要是：低功耗WAPI模组，以及集成了低功耗WAPI模组的终端产品。

■ 7. 问：为什么WAPI协议基础要素测评主要针对低功耗WAPI模组？

答：低功耗WAPI模组以单片机（MCU）为核心单元，算力和资源受限，这类产品无法像运行Windows、Linux、Android等操作系统的产品那样具备一定的软件安全防护能力。如果低功耗WAPI模组不采用硬件安全芯片存储密钥、执行密码运算，软件存储、执行运算的密钥就很容易被非法获取，会导致“非法设备获取合法身份”，由此带来安全风险。

因此需要通过WAPI协议基础要素测评，检验低功耗WAPI模组是否采用了具有符合国家密码主管部门批准算法能力的安全芯片，对密钥进行安全存储、执行密码运算。

■ 8. 问：厂商为什么要参加WAPI协议基础要素测评？

答：随着WAPI在各行业广泛应用，传感器、手持终端等类业务终端产品，大多通过集成低功耗WAPI模组快速具备了WAPI功能。但市场上有一部分低功耗WAPI模组以及集成了低功耗WAPI模组的终端产品，它们没有采用具有符合国家密码主管部门批准算法能力（包括国家密码管理局第7号公告发布的无线局域网专用商密算法ECDSA、ECDH的指定椭圆曲线和参数，SHA-256，以及通用商密算法SM2/3/4）的安全芯片对密钥进行安全存储和执行密码运算，因此存在密钥泄露的安全风险，易导致“非法设备获得合法身份”。这种风险与WAPI安全协议技术本身无关，属于产品工程实现层面的问题，但却会影响用户整体使用方案的安全性，给行

业网络带来安全风险。

厂商参与WAPI协议基础要素测评，可以验证产品是否采用了具有符合国家密码主管部门批准算法能力的安全芯片对密钥进行安全存储、执行密码运算，避免密钥泄露、非法设备获得合法身份等安全风险，也为行业网络选用产品提供了参考和依据。

■ 9. 问：正在修订的《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》系列团体标准，项目目标是什么？

答：2021年，系列团体标准T/WAPIA 045《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》获得发布。该系列标准规范了实体鉴别与密钥管理的融合技术，基于国家/国际标准规范的三元对等安全架构，具备身份保护能力、抗字典攻击能力等，促进了网络安全连接技术在有线局域网、无线局域网、近场通信、射频识别、移动通信、TCP/IP等基础通信网络中的规模部署和应用实施。

量子计算、区块链等新技术的快速发展和演进，对现有的鉴别与密钥管理技术体系提出了新挑战和新需求。针对上述，无线网络安全标准化委员会于2024年11月13日立项了《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》系列标准（修订），该项目欢迎所有联盟成员单位、标委会委员和社会公众积极参与。

■ 10. 问：正在制定的团体标准《信息安全技术 数字证书管理 第3部分：证书颁发》和团体标准《信息安全技术 数字证书管理 第4部分：证书撤销》，其项目目标是什么？

答：2024年8月14日，无线网络安全标准化委员会批准《信息安全技术 数字证书管理 第3部分：证书颁发》和《信息安全技术 数字证书管理 第4部分：证书撤销》立项，该2项标准将规范WAPI证书颁发和撤销技术，旨在减少因证书管理不当而引发的安全风险，提高网络通信的安全性和稳定性。

其中，《信息安全技术 数字证书管理 第3部分：证书颁发》将规范证书在线颁发、自动更新的技术实现，通过自动化管理流程，实现证书到期前的自动检测、生成、分发和更新，保障在自动更新过程中数据的完整性和机密性。

《信息安全技术 数字证书管理 第4部分：证书撤销》将确保无线局域网中的证书撤销机制能够有效组织被撤销证书的继续使用，防止未授权访问、数据泄露等安全威胁；通过减少撤销过程中的计算量和传输开销，提高撤销效率；保障WAPI证书撤销机制能够与其他安全协议和标准兼容，促进不同设备和系统间的互操作性，为安全无线局域网提供更灵活和广泛的安全支持。

■ 11. 问：国家标准委印发的《团体标准组织综合绩效评价指标体系》和企业有什么关系？企业关注哪些具体要求和指标？

答：2024年8月14日，国家标准化管理委员会印发《团体标准组织综合绩效评价指标体系》，旨在深入贯彻落实《国家标准化发展纲要》，发挥市场对团体标准的优胜劣汰作用，促进“制定好、管理好、应用好”团体标准。《指标体系》从组织管理能力、专业技术能力、标准编制能力、推广应用能力4个维度提出了具体要求。其中对企业参与团体标准工作提出了具体要求，建议企业关注和落实相关工作。包括：

（1）在“2.3参编单位相关技术创新成果”中，鼓励制定含有标准必要专利的团体标准，鼓励科研成果、新产品、新技术、新服务转化为团体标准；

（2）在“4.5.3市场应用”中，鼓励在招投标文件或商业合同中实施应用团体标准；鼓励企业依据团体标准进行生产经营活动时，在“企业标准信息公共服务平台<https://www.qybz.org.cn>”上公开执行团体标准的相关信息；

（3）在“4.5.6合格评定应用”中，鼓励在检验检测、评价、认证认可中应用团体标准。



习近平：

努力建设一支强大的现代化信息支援部队 推动我军网络信息体系建设跨越发展

2024年12月4日，中共中央总书记、国家主席、中央军委主席习近平视察信息支援部队发表重要讲话时强调，要贯彻新时代强军思想，贯彻新时代军事战略方针，强化使命担当，勇于创新突破，夯实部队基础，努力建设一支强大的现代化信息支援部队，推动我军网络信息体系建设跨越发展。

习近平强调，要坚持解放思想、实事求是、与时俱进，加强统筹谋划，创新发展模式，积极探索实践，扎实做好网络信息体系建设各项工作。要聚焦能打仗、打胜仗，优化信息服务保障方式，蹄疾步稳推进网络信息公共服务平台建设，融合利用好各类数据信息，高度重视网络信息安全防护，加快融入体系、驱动体系、赋能体系，引领指挥模式创新、作战方式转变。要持续推进改革任务落实，建立健全工作运行机制，配套完善相关法规制度，打造共建共用共享良好生态，提高网络信息体系建设质量和效益。

丁薛祥：

推动构建网络空间命运共同体迈向新阶段

2024年11月20日，中共中央政治局常委、国务院副总理丁薛祥在2024年世界互联网大会乌镇峰会开幕式上强调，当前互联网、大数据、云计算、人工智能、区块链等技术不断取得突破，正在全面赋能经济社会发展，但数字鸿沟仍在扩大，网络安全形势更加严峻。国际社会比以往任何时候都更加需要携起手来，推动构建网络空间命运共同体迈向新阶段，建设更加美好的“数字未来”。

丁薛祥提出四点建议：一是完善全球治理，实现网络空间命运与共。坚持真正的多边主义，尊重各国网络主权，构建更加公平合理、开放包容、安全稳定、富有生机活力的网络空间。二是加强协同创新，推动网络信息技术加快发展。积极拓展人工智能、大数据、区块链等领域合作，推进基础研究和前沿技术联合攻关。三是强化公平普惠，促进互联网发展成果全球共享。四是坚持依法依规，提升网络安全防护水平。深化网络空间安全合作，强化技术向善，妥善应对人工智能等科技发展带来的规则冲突、社会风险、伦理挑战。

中共中央办公厅 国务院办公厅： 保障新型城市基础设施网络和数据安全

2024年12月5日，中共中央办公厅、国务院办公厅印发《关于推进新型城市基础设施建设打造韧性城市的意见》指出，要保障新型城市基础设施的网络和数据安全。要严格落实网络和数据安全法律法规和政策标准，强化信息基础设施、传感设备和智慧应用安全管控，推进安全可控技术和产品应用，加强对重要数据资源的安全保障。要强化网络枢纽、数据中心等信息基础设施抗毁韧性，建立健全网络和数据安全应急体系，加强网络和数据安全监测、通报预警和信息共享，全面提高新型城市基础设施安全风险抵御能力。

金壮龙： 全面深化改革，有效应对重大风险挑战

2024年11月16日，工业和信息化部党组书记、部长金壮龙在《求是》杂志发表署名文章《进一步全面深化改革 为推进新型工业化注入强大动力》中指出，发展和安全是一体之两翼、驱动之双轮，需要统筹兼顾、同步推进。当前，世界百年未有之大变局加速演进，全球产业发展格局深刻调整，逆全球化思潮抬头，单边主义、保护主义明显上升，来自外部的打压遏制不断升级，我国工业和信息化发展进入战略机遇和风险挑战并存、不确定难预料因素增多的时期，各种“黑天鹅”、“灰犀牛”事件随时可能发生。有效应对这些风险挑战，必须进一步全面深化改革，大力加强制度建设，提升行业治理现代化水平，用完善的制度防范化解风险、有效应对挑战，推动新型工业化走深走实、行稳致远。

中国人民银行等七部门： 落实科技自立自强战略，加强数据和网络安全防护

2024年11月27日，中国人民银行、国家发展改革委、工业和信息化部、金融监管总局、中国证监会、国家数据局、国家外汇局等七部门联合印发《推动数字金融高质量发展行动方案》指出，要落实科技自立自强战略，持续提升科技核心系统自主可控能力。要加强数据和网络安全防护，强化数据安全的商用密码保护，加强基础、共性安全支撑。

尹力： 推动北京国际科技创新中心建设迈向更高水平

2024年11月19日，北京市委书记尹力在北京市科技大会暨科学技术奖励大会上指出，要更加深刻认识建设国际科技创新中心是党中央赋予北京的战略任务、科技创新是推动发展方式转变的关键所在、科技现代化是北京率先基本实现社会主义现代化的有力支撑，锚定到2035年全面建成国际科技创新中心这个目标，坚持“四个面向”战略导向，要全面提升关键共性技术、颠覆性技术攻关能力，成为全球重要科学策源地；要全面提升科技成果转化能力，成为未来产业引领地；要全面提升科技人才培养和集聚能力，成为高水平人才高地；要全面提升科技要素配置能力，成为开放创新核心枢纽。

WAPI产业联盟参加 “红色之旅·走进怀柔第一党支部纪念馆”主题党日活动

WAPI产业联盟 刘剑昕



2024年11月1日，WAPI产业联盟参加“红色之旅·走进怀柔第一党支部纪念馆”主题党日活动。北京市中关村社团第二联合党委、各支部20余名代表参加活动。

首先，同志们参观了北京市廉政教育基地——怀柔第一党支部纪念馆。在这里通过观看革命教育短片《那一片红》，参观“点播火种”、“庙上星火”、“烽火怀柔”等主题展览，深入了解了怀柔第一支

部在抗战期间发挥的重要作用。通过追忆红色历史，感受先辈们不屈不挠的革命精神和不畏牺牲的奉献精神，强化对产业技术联盟党员同志和积极分子的党性教育、廉政教育。

随后，同志们以饱满的热情开启健步走活动。通过攀登雄伟险峻的明长城、参观明代守将栽培的古栗园，强健体魄、提升意志力，以更加饱满的精神状态投入到工作中去，为产业联盟发展贡献力量。

WAPI产业联盟参加“关爱生命 救在身边 党员先行” 应急救护知识培训主题党日活动

WAPI产业联盟 周园



2024年10月22日，WAPI产业联盟参加了北京市中关村社团第二联合党委、中关村产业技术联盟联合会、中关村紫能生物质燃气产业联盟、清华大学红十字协会学生分会组织的“科创星火”党建品牌——“关爱生命 救在身边 党员先行”应急救护知识培训主题党日活动。各支部、联盟党员、积极分子等20余名代表参加活动。

活动中，WAPI产业联盟周园等同志认真学习了清华大学红十字会学生分会志愿者刘鲁宁的应急救护知识讲解及示范，系统了解了实施心肺复苏的判断依据、心肺复苏和人工呼吸的施救程序，以及自动体外除颤仪（AED）的正确使用方法。随后，在志愿者带

领下，大家进行了心肺复苏模拟抢救和AED实操练习，通过认真实践，反复训练，基本了解并掌握了急救基本知识和技能。

周园等同志表示，学习并掌握应急救护技能非常必要，不仅可以帮助大家在紧急情况下迅速做出正确的反应，采取必要的急救措施，减少伤害程度，甚至可以挽救生命。这次培训通过学理论、真体验，让联盟同志们掌握了基本急救技能，提升了大家对生命的敬畏感和主动施予援手的社会责任感，贯彻了“人人学急救，党员当先锋”的思想意识，从技能上提升了党员和社会组织工作者的社会服务能力。

WAPI产业联盟发布

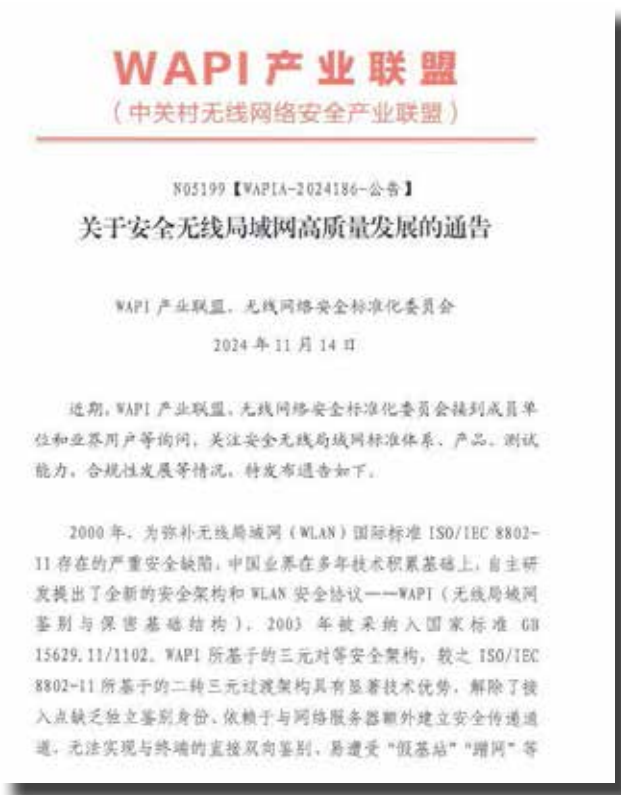
《关于安全无线局域网高质量发展的通告》

WAPI产业联盟 王立华

伴随WAPI规模建设和演进，产业市场对安全无线局域网标准体系、产品、测试能力、合规性发展等十分关切，并于近期密集向WAPI产业联盟反馈和咨询。

结合上述，WAPI产业联盟和无线网络安全标准化委员会迅速展开调研，于2024年11月14日发布《关于安全无线局域网高质量发展的通告》，就产业市场的核心关切予以说明，并倡导：要采用合规的、持续应对安全挑战的做法，共同推动安全WLAN高质量发展。

通告内容如下：



2000年，为弥补无线局域网（WLAN）国际标准ISO/IEC 8802-11存在的严重安全缺陷，中国业界在多年技术积累基础上，自主研发提出了全新的安全架构和WLAN安全协议——WAPI（无线局域网鉴别与保密基础结构），2003年被采纳入国家标准GB 15629.11/1102。WAPI所基于的三元对等安全架构，较之ISO/IEC 8802-11所基于的二转三元过渡架构具有显著技术优势，解除了接入点缺乏独立鉴别身份、依赖于与网络服务器额外建立安全传递通道，无法实现与终端的直接双向鉴别、易遭受“假基站”“蹭网”等安全隐患。GB 15629.11/1102标准的发布，标志着WAPI 1.0技术标准体系的形成。

2006年国家密码管理局发布第7号公告，批准了WLAN产品须采用的密码算法，包括对称密码算法SM4，签名算法ECDSA、密钥协商算法ECDH的指定椭圆曲线和参数，杂凑算法SHA-256。上述WLAN专用商密算法的发布，为WAPI技术标准体系持续演进提供了重要支撑。GB 15629.11—2003/XG1—2006、GB 15629.1101—2006、GB/T 15629.1103—2006、GB 15629.1104—2006四项国家标准发布后，基础安全技术、安全组网技术、网络管理技术、产品与解决方案、测试评价技术、创新应用等持续演进发展，八十余项国家、行业、团体标准陆续得到发布，WAPI 1.0技术标准体系不断完善，联盟测试实验室的产品和系统测试项目，演进至第四个版本。标准体系的深入实施显著推动了产业发展，支持WAPI 1.0技术标准体系的WLAN芯片超过500款型号、全球累计出货量超过270亿颗，移动终端和网络侧设备等超过22000款，为能源、海关、金融、政务、公安、交通、医疗、教育等行业提供着安全网络服务。

随着本世纪初迄今量子技术逐步取得突破及商业化进程的加快，使用传统密码算法的网络安全协议体系正面临重大挑战，迫切需要新一代WLAN安全技术标准。2015年，联盟组织成员单位提交标准制定申请并在通过评审后获批立项。2015年至2021年，标准编制组开发了草案稿、征求意见稿、送审稿和报批稿，期间经产品验证及多次标准会议，专家充分讨论、修改完善标准文本，2021年12月WAPI产业联盟、无线网络安全标准化委员会发布了T/WAPIA 046《无线局域网安全技术规范》，这是中国WLAN业界面向量子时代的网络安全挑战，结合适配通用商密算法SM2、SM3需求，使用更高性能商密算法SM4-GCM，满足身份保护需求和应对离线字典攻击、潜在量子计算攻击威胁，为向量子安全时代过渡的安全WLAN产品提供架构及协议支持的新贡献，使得安全WLAN技术标准体系得到新的发展，标志着进入了WAPI 2.0技术标准体系阶段。

T/WAPIA 046适配了通用商密算法SM2和SM3，并持续使用SM4，对WAPI 1.0技术标准体系中WLAN安全协议内容进行了扩展，增加了适配后的机制选项，包括新增WAI2协议、快速切换机制等，在密码算法强度、身份保护、抗离线字典攻击和应对量子计算攻击等安全性方面有显著增强，使WLAN设备持续满足合规要求、支持形成可信赖WLAN网络和服务，适用于更高安全要求的应用环境，是对量子技术发展和量子时代新安全威胁的及时应对。同时，T/WAPIA 046提供了一种更高安全性、面向量子时代安全需求的新选择，在技术及标准层面，T/WAPIA 046兼容WAPI 1.0技术标准体系，在实际部署中提供了向WAPI 2.0安全方案的有序过渡，适应了平滑演进、兼

容互通的产业需求。

T/WAPIA 046发布实施后，因其结合和兼顾了面向量子时代安全和使用通用商密算法的需求，得到业界的关注和响应。多厂商多类别产品开发、联盟测试平台能力建设，稳步进展。同时，联盟不间断地收集和响应在产业实施过程中成员单位和业界各方提出的意见、建议，持续追求在不降低安全性的前提下，进一步减少技术演进升级的投入，尽力将芯片等硬件系统升级的工作减至最少，在满足合规性需求的前提下，进一步保护投资。目前，标委会针对T/WAPIA 046中WAI2协议封装及以太网类型字段标识的改进，已通过修改单项目立项，正在制定中。

根据联盟统计的产业情况，实施T/WAPIA 046的典型方式是采用软件升级方式（作为软件补丁部署在WAPI 1.0标准符合性设备上），按照目前计划，未来半年内将有多个联盟成员单位发布STA、AP/AC、AS等系列符合T/WAPIA 046的产品，为行业和产业应用提供合规、兼顾面向量子时代安全和通用商密算法应用需求的产品和网络系统解决方案。联盟测试实验室已经过整备和样本测试，2024年内将正式接受成员单位的产品标准符合性委托测试，并出具测试报告，供业界采用。联盟将继续做好和产业、行业决策机构和采购政策的衔接，使产业、行业能及时采用合规、具有更高安全性、面向量子时代安全需求的产品和网络，支持保障网络服务的安全性。

在产品测试和示范应用中，存在同一网络SSID内，不同版本WAPI机制并存，以及同一版本机制中证书鉴别和预共享密钥鉴别混用的情况，由于预共享密钥鉴别面临的安全管理风险较大、仅适用于满足短时间临时组网的需求，与证书鉴别机制安全性差异

大，以及不同版本WAPI机制的安全等级不同，为防止降维攻击，应用中应避免不同版本WAPI机制，以及同一版本机制中证书鉴别和预共享密钥鉴别在同一网络中同时启用服务的做法。

目前业界存在部分在现有WAPI 1.0技术标准体系的基础上，在产品开发中直接替换原有WLAN专用商密算法、使用通用商密算法的做法，这种做法因缺少技术演进的前瞻性，不是现有标准体系支持的合规方式。并且，通过这种方式开发的产品不具备技术标准体系演进形成的新的安全能力。对此联盟倡导：采用合规的、持续应对安全挑战的做法，共同推动安全WLAN高质量发展。

无线网络网络安全标准化委员会2024年第四次主任委员会议 (总第11次) 顺利召开

WAPI产业联盟 刘剑昕

2024年12月4日，无线网络网络安全标准化委员会主任委员曹军主持召开2024年第四次主任委员会议。副主任委员王立建、陶洪波、王宏、张璐璐、黄振海，及联盟秘书处标准化部负责同志参加了会议。

会议包括：对上一次主任委员会议精神落实情况、2024年第4季度工作要点、第四届标委会换届工作进展、标委会全体会议筹备情况、团体标准组织综合绩效评价工作、2025年标准化重点工作任务等进行讨论。

标委会总体组(WG1)黄振海汇报了上次主任委员会议精神落实情况及2024年第4季度工作要点。2024年第三次主任委员会议之后，标委会结合会议指导意见积极开展工作，在标准制定、标准实施、标准平台和生态等多个方面取得了进展。

在标准制定方面，本周期内，新立项8项团体标准，另有5项立项正在审批中；国际标准项目《Guidelines for Designing Communication Security Protocols in the Context of Migration to Post-quantum Cryptography (GD-CSP-PQC)》(向后量子加密技术迁移背景下的通信安全协议设计指南)进入预备工作项目(PWI)阶段。

在标准实施方面，发布《关于安全无线局域网高质量发展的通告》；符合WAPI标准体系的产品创新成果喜人；多厂商发布全国产系列产品并通过联盟测试实验室测试；WAPI协议基础要素(ECDSA、ECDH、SHA-256)测评正在有序开展。

在标准平台和生态方面，顺利召开2024年第三次标准工作及项目组会议；WAPI协议基础要素测评服务正式纳入新版《无线局域网鉴别与保密基础结构(WAPI)功能测试项目》。多家媒体对上述工作进行了报道。

联盟秘书长张璐璐汇报了第四届无线网络网络安全标准化委员会换届进展情况。自2024年6月起，在换届工作领导小组的指导下，根据《无线网络网络安全标准化委员会导则》《WAPI产业联盟标准化工作管理办法》，开展标委会换届工作。经委员候选人征集、委员候选人评审、主任委员/副主任委员提名、评审结果公示等程序，目前第四届标委会委员共85人，包括1名主任委员，5名副主任委员，79名委员。

张璐璐还报告了第三届无线网络网络安全标准化委员会第五次会议、第四届无线网络网络安全标准化委员会第一次会议、2024年第四次标准工作和项目组会议的筹备情况，以及团体标准组织综合绩效评价工作进展情况。黄振海报告了拟提交标委会全会审议的2025年标准化重点工作任务。

与会主任委员、副主任委员对上述工作给予肯定，也提出了“要进一步推进高质量安全无线局域网标准体系完善、要紧密围绕市场需求加强应用标准的创新、要进一步强化测试标准对产业市场的支撑保障作用、要持续提升项目编辑和标准主笔人的文本编写质量”等工作要求。

第三届无线网络安全标准化委员会第五次会议成功召开

WAPI产业联盟 周园

2024年12月17日，第三届无线网络安全标准化委员会（以下简称标委会）第五次会议成功召开。会议报告了第三届标委会四年来的整体工作、2024年标委会工作，以及标委会下设7个工作组的《2024年度工作总结和2025年度工作建议》。经审议，通过了上述文件。

来自无线网络安全技术国家工程研究中心、中国通用技术研究院、国家无线电监测中心检测中心、中国物品编码中心、空天地一体化综合业务网全国重点实验室（西安电子科技大学）、中国南方电网电力调度控制中心、中国电力科学研究院有限公司、国网山东电力省公司电力科学研究院、南方电网数字电网科技（广东）有限公司、深圳市国电科技通信有限公司、广电计量检测集团股份有限公司、江苏省电子信

息产品质量监督检验研究院(江苏省信息安全测评中心)、西电捷通公司、北京数字认证股份有限公司、华为技术有限公司、新华三技术有限公司、北京联盛德微电子有限责任公司、深圳市信锐网科技术有限公司、北京华信傲天网络技术有限公司、广州莲雾科技有限公司、上海乐研电气有限公司、深圳市智开科技有限公司、西安芯语慧联信息科技有限公司、南京博洛米通信技术有限公司、科大国盾量子技术股份有限公司、重庆华联众智公司、北京大学信息工程学院、中国计量大学等单位，以及无线网络安全标准化委员会、ISO/IEC JTC 1/SC 6国内技术对口单位、工业和信息化部宽带无线IP标准工作组等标准组织的40余位代表参会。



会议由标委会副主任委员、WAPI产业联盟秘书长张璐璐主持。



图：标委会副主任委员、WAPI产业联盟秘书长 张璐璐



图：标委会副主任委员 黄振海

标委会副主任委员黄振海受标委会主任委员曹军委托宣读致辞。首先感谢各位委员这四年的持续努力和付出。第三届无线网络安全标准化委员会在标准编制、标准实施、标准平台建设、标准生态提升等方面，不断协同创新，推动形成和完善了安全无线局域网标准体系，并正在向着更高质量和面向量子时代前进。

曹军对下一步工作提出了要求。一是要更加聚焦典型业务场景和突出问题，从产业业务场景的全生命周期、全链条来思考、规范和提高网络的整体安全性和健壮性，深入开展创新标准制定和推动实施；二是要继续拓展全球视野，积极参与网络安全

国际标准规则制定。为业界供给安全网络服务相关的技术手段和应对方法，不断提高产业和行业的安全意识和防范能力。要加强国际合作，共同应对跨国网络攻击和信息泄露等安全威胁。三是标委会委员要积极履职，加强协调和经验分享，促进标委会高质量运行，共同构建一个安全、可信赖、持续满足业界需求的无线网络生态。

2024年标委会工作进展顺利，标委会委员牵头/参与7项国际标准，15项国际标准研制预工作项目（PW1），发布（获发布）中关村标准2项、团体标准5项，获北京市高质量团体标准1项，新立项团体标准20项，完成了2024年团体标准复审。

总体工作组（WG1）组长黄振海、网络安全工作组（WG2）组长杜志强、无线网络工作组（WG3）组长张国强、产品与解决方案工作组（WG4）组长侯鹏亮、互操作测试工作组（WG5）组长尹玉昂、特别任务管理工作组（WG6）组长、生态环境工作组（WG7）组长张璐璐汇报了本工作组《2024年度工作总结和2025年度工作建议》。与会委员对上述工作进行审议，就部分内容提出意见和建议，并形成相关决议。

黄振海汇报了《第三届无线网络安全标准化委员会工作报告》。四年来，第三届标委会在平台建设方面，建立了主任委员会议机制，形成了WAPI标准体系相关信息搜集和处理流程，完善了标准文本网站下载机制，修订多项管理文件，现有委员99人；在标准编制方面发布（获发布）国际标准9项、国家标准4项、地方标准1项、中关村标准3项、团体标准27项；此外，标委会在标准实施、标准复审、标准生态等方面均取得了显著的提升。第三届标委会工作成果显著，荣获2022年中国标准创新贡献一等奖、2023年工信部百项团标应用示范项目、2023年工业和信息化领



域商用密码典型应用方案、2024年北京市高质量团体标准。践行了国家战略，取得良好的社会反响。

会上，对2024年做出积极贡献的23位标委会委员和4位项目编辑予以肯定和鼓励。

2024年标委会的主任、副主任委员、各工作组组长、各项目编辑积极履职，数十位委员参与了标准的起草、实施等工作，推动了标准化工作的高质量推进。很多委员发挥自身优势，表现突出：有些委员作为国家和重要行业部门的标准化专家，坚持以合规性保障国家网络安全，发挥自己的主观能动性和资源优势，推动国家和行业标准引用WAPI标准体系；有些委员在本行业领域积极组织开展WAPI标准的建设应用，持续推动安全无线局域网高质量发展；有些委员对每份标准提出实质性意见，对标准编制人员给予悉心指导和培训，促进团体标准质量持续提升；有些委员及时准确地呈现标委会工作，对标准化、产业化、市场化、国际化成果予以客观宣传；还有些委员支持并高质量协办了标准工作和项目组会议……这些实实在在

的工作和贡献，促进了标委会良性生态环境建设，也让标准产业协同创新工作向更高质量齐心迈进。

会上为贡献突出的委员和项目编辑代表颁发了鼓励函，大家以热烈掌声向这些同志致敬。

无线网络安全标准化委员会是在无线网络和网络安全专业领域内，从事标准起草、技术审查、标准实施等标准化工作的非法人技术组织，负责WAPI产业联盟团体标准的制定、发布、实施，推动团体标准被国际、国外、中国、行业以及其他团体标准的采用和引用。标委会秘书处工作由WAPI产业联盟承担。

标委会由单位委员和专家委员组成，主要来自生产者、经营者、使用者、消费者、公共利益方等，具广泛性和代表性。标委会每届任期4年，任期届满换届。依据《无线网络安全标准化委员会导则》和《WAPI产业联盟标准化工作管理办法》开展工作。

依据GB/T 20004.1《团体标准化 第1部分：良好行为指南》规范要求，标委会设置了管理协调层、技术协调层、标准编制层。



南网数网科技“电鸿”系列低功耗WAPI模组 通过联盟测评

WAPI产业联盟 王立华

2024年11月15日，南方电网数字电网科技（广东）有限公司（以下简称数网科技）自主研发的WAPI MCU“电鸿”低功耗WAPI通信模组工业型/商业型产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及功能测试和WAPI协议基础要素测评（包括国家密码管理局第7号公告发布的ECDSA、ECDH、SHA-256等算法）。联盟为上述产品出具了测评报告。

上述WAPI终端模组型号分别为：SWKJ-DH-H001（工业型）、SWKJ-DH-L001（商业型）。它们均采用高度集成的2.4GHz WAPI&BLE低功耗SoC芯片，并采用通过国家商用密码认证的安全芯片对密钥进行安全存储和执行密码运算，是基于数网科技低功耗WAPI模组解决方案的高规格、全国产、高安全系列产品。另据数网科技介绍，上述产品同步支持电力鸿蒙操作系统（PowerHarmony+PHM V1.0），已通过相关机构检测，具有覆盖广、速率高、安全稳定、实用美观等特点，能够满足现下电力行业“大带宽、大连接、移动性强”的WAPI网络建设要求，同时也适用于教育、金融、能源、交通、制造等行业，助力用户开展WAPI数字化建设/改造工程。

近年来，南方电网公司积极响应国家开源体系

建设号召，于2023年10月31日发布了电鸿物联操作系统，填补了电力行业统一物联网操作系统的空白。

“电鸿”是面向新型电力系统和新型能源体系构建的互联互通、开放共享的电力物联体系。“电鸿”以开源“鸿蒙”和开源“欧拉”为底座，强化电力终端及用电设备广域分布、海量连接、安全可靠特性，推动能源、交通、智能家居等跨行业跨领域协同，拓展电力服务边界，提升服务质效，催生新型能源生态。加快发展“电鸿”对我国能源高质量发展具有重要意义。“电鸿”在实践中得到了广大生态伙伴的积极响应和支持，200家产业链厂商加入“电鸿”生态，带动“超7亿+生态设备”协同发展。目前“电鸿”应用在深圳前海、广州南沙、珠海横琴的全域综合示范区成效显著。

数网科技表示，下一步将继续推进“WAPI+电鸿”的研发、适配及应用，将“WAPI+电鸿”融入电力系统数字化智能化转型关键环节，构筑能源生态的数字化底座。未来，“WAPI+电鸿”将继续以开放包容的姿态，携手全产业链生态伙伴共筑坚实、高效、智能的数字电网，“以电为媒、通连万物”，为筑牢能源生态体系数字底座、加快发展新质生产力贡献力量。

智开科技WAPI系列产品通过联盟测试

WAPI产业联盟 王立华



2024年11月18日，深圳市智开科技有限公司（以下简称智开科技）的无线局域网系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础机构（WAPI）互通性、完整性及功能测试。本次测试依据2024年3月版WAPI功能测试项开展，通过后联盟为上述设备出具了测试报告。

本次测试通过的无线接入点（AP）型号分别为ZK-WAP6-8200、ZK-WAP6-3200X、ZK-WAP5-1200X；终端（STA）型号为ZK-NC-2110T。其中AP设备采用瘦架构组网方式，支持本地转发与集中转发模式。AP与STA设备均支持2.4/5GHz双频接入，通信速率支持802.11ac协议。能够满足电力行业“大宽带、大链接、移动性强”的WAPI网络建设需求。

据智开科技介绍，ZK-WAP6-8200（室内型）、ZK-WAP6-3200X（室外型）这两款AP为智开科技

新一代电力专用AP，针对电力厂站感应电强、浮尘多等应用场景作了特别设计和处理，具有更好的环境适应性；ZK-WAP5-1200X室外型AP支持多跳互联进行数据传输，最大实测可支持26跳互联，可应用于输电线路视频监控数据回传；ZK-NC-2110T为双频免驱无线网卡，自带电池，可持续工作4小时，可通过Type-C连接手机、PAD、笔记本电脑等，使得随身携带的作业终端快速连接WAPI网络。

智开科技表示，公司基于电力生产场景持续创新，不断迭代WAPI全系列产品，不断基于电力场景推出多种应用终端和解决方案。未来，智开科技将继续研发基于WAPI的网络侧产品和终端产品，进一步拓展WAPI产品序列，为市场用户提供更加丰富的解决方案。

南网超高压公司在国内率先实现所辖站点 WAPI无线局域网全覆盖

中国能源新闻网

南方电网超高压输电公司（以下简称“南网超高压公司”）完成所辖全部47个站点WAPI（Wireless LAN Authentication and Privacy Infrastructure）无线局域网建设，在全国率先实现所辖站点无线局域网全覆盖，可为数字电网各类新型智能业务提供宽带、安全、泛在、灵活的无线接入方式，为数字电网建设提供强力支撑。

据悉，随着南方电网公司数字化转型和数字电网、新型电力系统建设的推进，涌现出以智能巡视、智慧安监、移动办公为代表的新型智能业务。这类业务总体呈现出“大带宽、移动性、大连接”的特点。目前，此类业务普遍采用公网通信或有线连接等接入方式，存在公网信号弱、资费高，建设运维成本高、施工周期长等问题。WAPI无线局域网鉴别与保密基础结构，是中国无线局域网安全强制性标准。符合WAPI标准的安全无线局域网具有带宽充足、安全可控、部署灵活、效益显著等优点，经验证适合变电站、仓库、输电管廊等场景内的无线网络覆盖。

南网超高压公司扎实推动南方电网公司数字生产通信专项规划落实落地，以“四交五直一海缆”数字化智能化场景站点建设为契机，加快推进WAPI无线局域网建设。面向站内智能终端视频、语音、数据等业务无线接入的需求，打通通信链路“最后一公里”，助力数字电网建设。完成站点的WAPI无线局域网建设，有力支撑南网超高压公司实现全域物联网“电网设备全在线、电网状态全感知和电网信息全透明”的目标，为数字电网建设注入强劲动力。

在设计规划阶段，南网超高压公司基于试点建设经验，针对不同电压等级的换流站、变电站制定了3套网络建设的典型设计方案，规范了网络架构、布点设计、组网方案、施工工艺等方面6大类29小项的措施和要求；同时印发网络工程测试指引，对网络性能参数、工程施工提供可量化的验收标准，为工程的高质量、高速度建设奠定了坚实基础。在建设实施阶段，南网超高压公司严格把控WAPI网络建设质量，以专人专班开展现场监督管理，重点做好隐蔽工程的细节质量管控；强化站内施工安全管理，严格执行承包商“同进同出”制度，确保人员、设备安全。

南网超高压公司昆明局普洱换流站站长侯世金很高兴地对笔者说：“WAPI无线局域网建成后，我们普洱换流站实现了无线局域网信号全覆盖，智能巡检机器人、北斗手持机等智能设备广泛接入，信息传输效率提升了4倍以上，工作效率提升2倍以上，数字电网建设进度大幅提升。”

国网冀北唐山供电公司创新应用WAPI技术 实现低压分布式光伏直采直控

国家电网报

2024年11月11日，冀北唐山供电公司电力调度控制中心采用无线局域网鉴别与保密基础结构（WAPI）本地通信技术实现了低压分布式光伏采集与控制，标志该公司破解了低压分布式光伏柔性调控通信的技术难题。

目前，唐山地区分布式光伏并网户数达10.8万户，并网容量达306万千瓦。此前，唐山供电公司通过高速电力线载波技术等实现了低压分布式光伏逆变器至台区之间的本地通信，但存在部署困难、稳定性差、传输速率低、安全性无法保障等问题。

唐山供电公司创新应用WAPI本地通信技术，以玉田县东芦庄台区为试点，对该台区分布式光伏进行采集控制的通信验证，通过数据传输装置解决现场数据转发等问题，防范非法终端接入WAPI网络以及业务数据被窃取、破坏、篡改等风险，实现低压分布式光伏逆变器至台区和主站数据的安全可靠传输，为分布式光伏等新能源电源的可观、可测、可调、可控功能提供通信技术支撑。



宁夏首次在750千伏变电站应用蓄电池远程核容养护系统

探索并入沙湖WAPI网络

新华网

2024年11月25日，国网宁夏超高压公司在沙湖750千伏变电站投入使用蓄电池远程核容养护系统，标志着宁夏电网在智能化、自动化运维方面又迈出重要一步。接下来，公司将探索把此系统并入沙湖WAPI网络（站内专用安全无线网络），进一步提高数据上传、分析速率，为电网的提质增效、稳定可靠运行提供更加智能化和安全化的坚实保障。

蓄电池作为变电站的备用电源，当变电站突发故障或停电时，能够迅速提供短期电力保障。按照规定要求，需定期对蓄电池组进行核对性放电试验，检查蓄电池容量、及时发现老化电池，保证蓄电池始终保持健康运行状态。蓄电池远程核容养护系统是一种集成蓄电池在线监测、数据分析、故障诊断告警和远程操控的先进系统，能够实时对蓄电池组单体电压、内阻、极柱温度、组端电压、组端电流、蓄电池容量等参数进行在线监控及告警。同时实现远程在线蓄电池容量放电测试。常规进行蓄电池充放电试验过程复杂，需要进行拆线、接线、直流切换、放电仪参数设置等8项步骤，2组蓄电池分组连续充放电过程耗时约40个小时，人员每隔1小时需进行单组约104个蓄电池数据的不间断抄录比对，费时费力。另外在拆接线过程中存在人身触电风险和充放电试验完成后蓄电池未恢复至母线的脱出风险。

此系统投入运行后，运维人员无需到测试现场，只需要在装置上按规定按钮设置好参数后，通过平台网络即可启动蓄电池组放电容量测试，实现蓄电池全程自动充放电。一方面彻底消除了作业过程中人身和设备的安全风险，有效提升了工作安全；另一方面可高效压减工作量，降低运维人员劳动强度，显著提高工作效率。此外，以前蓄电池放电产生的电能转化成热量散到空气中，而系统配备节能型充放电模块，支持将蓄电池组的电能逆变成交流，利用现有的负载将蓄电池放电产生的电能供给站用交流使用，达到安全节能的目的。

国网宁夏超高压公司高度重视此次蓄电池远程核容养护系统的应用，从人员安排、现场勘查到现场施工方案的编制等方面进行了全面部署和精心组织，积极参与系统的安装、调试和运行维护工作，有力确保了系统的顺利投入使用。

国家电网命名20支国际标准化创新团队

国家电网报

为创新国际标准化工作机制和人才培养模式，加快推动一批重点领域国际标准取得突破，国家电网有限公司近日印发通知，命名首批20支国际标准化创新团队。

当前，国际标准工作环境日益严峻，我国国际标准化工作面临挑战。此次国际标准化创新团队命名，目的在于主动创新工作模式，产出更多国际标准成果，巩固提升公司国际竞争力。经过严格评审论证，高压直流技术与装备创新团队等20支创新团队获得命名，涉及特高压及先进输电、分布式电力能源、电力装备与材料、智能量测、负荷侧供需互动等传统技术领域，以及新能源、新能源汽车、新型储能、低碳节能、新一代信息技术等新兴技术领域。各创新团队由来自科研、产业、生产单位的人员联合组成，专业互补性强，易于形成竞争合力，共同推进相关领域国际标准研制。

通知要求，首批国际标准化创新团队建设期为3年，聚焦新型电力系统核心技术领域，开展先进技术发展趋势跟踪分析；布局重点领域国际标准研制，推动一批核心国际标准立项和发布，成立国际标准组织新技术机构或区域性国际标准组织等；以“战”练兵，加强国际标准化青年专家培育，培养一批语言优、技术强的复合型国际标准化人才。公司将对创新团队实行考评制度。表现优异、成果突出的创新团队可优先被推荐为国家级国际标准化创新团队，并在科技项目、标准化人才培养等方面获得优先支持。

据了解，截至今年10月，公司已主导立项国际标准282项，其中126项已发布，实现国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU）三大国际标准组织全覆盖。各创新团队的建设将为公司国际标准化工作注入新动能。

20支国际标准化创新团队名录

序号	技术领域	团队名称	承担单位
1	特高压及先进输电	国际标准化创新团队 (高压直流技术与装备)	中国电科院、国网冀北电力、国网浙江电力、国网江苏电力、国网河北电力
2		国际标准化创新团队 (特高压交流输电系统)	中国电科院、国网安徽电力、国网四川电力、国网西北分部、国网山东电力
3		国际标准化创新团队 (柔性直流输电)	国网经研院、南瑞集团、国网四川电力、国网直流中心、国网冀北电力
4		国际标准化创新团队 (状态监测和风险控制)	国网网四川电力、国网工研院、中国电科院、国网青海电力、国网湖南电力
5	分布式电力能源	国际标准化创新团队 (分散式电力能源系统)	中国电科院、国网山东电力、国网福建电力、国网安徽电力、国网江苏电力
6	智能量测	国际标准化创新团队 (电能计量与信息采集)	中国电科院、中电装备公司、国网浙江电力、国网重庆电力、国网冀北电力
7	电力装备与材料	国际标准化创新团队 (电力机器人)	国网山东电力、中国电科院、国网上海电力、南瑞集团、国网湖南电力
8		国际标准化创新团队 (电力设备环境适应性)	国网福建电力、国网工研院、国网新疆电力、国网蒙东电力
9	负荷侧供需互动	国际标准化创新团队 (负荷资源评估与柔性调控)	国网江苏电力、南瑞集团、国网信通产业集团、国网能源院、国网湖南电力
10		国际标准化创新团队 (分布式资源供需可信互动)	国网浙江电力、中国电科院、国网数科公司、国网信通产业集团、国网河北电力
11	新能源	国际标准化创新团队 (新能源发电及并网)	中国电科院、国网福建电力、国网甘肃电力、国网冀北电力
12		国际标准化创新团队 (电力系统频率与电压管理)	国网江苏电力、南瑞集团、国网冀北电力、国网新疆电力、国网湖南电力
13	新能源汽车	国际标准化创新团队 (车网互动)	南瑞集团、国网车网技术公司、国网上海电力、国网浙江电力、国网北京电力
14	新型储能	国际标准化创新团队 (电力储能)	中国电科院、国网上海电力、国网山东电力、南瑞集团、国网辽宁电力
15	低碳节能	国际标准化创新团队 (电力碳计量及智能推演)	国网四川电力、北京电力交易中心、国网数科公司、中国电科院、国网重庆电力
16	新一代信息技术	国际标准化创新团队 (新一代电力信息通信)	中国电科院、国网信通产业集团、国网新疆电力、国网河南电力、国网江西电力
17		国际标准化创新团队 (电力人工智能)	中国电科院、国网上海电力、国网浙江电力、国网信通产业集团、国网大数据中心
18		国际标准化创新团队 (工控系统及网络安全)	国网湖北电力、中国电科院、国网重庆电力、国网山东电力、南瑞集团
19		国际标准化创新团队 (电力物联及未来网络)	国网山东电力、南瑞集团、国网湖南电力、国网湖北电力、国网宁夏电力
20		国际标准化创新团队 (未来城市智慧电网)	国网上海电力、南瑞集团、国网数科公司、国网车网技术公司、国网北京电力

华信傲天携手伟仕佳杰 制造业数字化转型新篇章

华信傲天

2024年11月14日，在华信傲天携手伟仕佳杰开展的“共创共享，助力增长”华东核心代理商赋能会上，华信傲天凭借其卓越的制造业解决方案，成为数字化转型佼佼者和全场焦点。

会上华信傲天分享了针对制造业数字化转型的定制化解决方案。该方案以智能制造为核心，融合了云计算、大数据、人工智能以及物联网等先进技术，旨在帮助制造业企业在办公网、生产网、仓储网实现网络的智能化、自动化与精益化。该方案支持WAPI。

目前华信傲天拥有全系列WAPI产品，支持一站式交付国家级安全WAPI网络，不仅满足了国家对于网络安全的严格要求，还提供了与国际标准兼容的开放性。通过采用WAPI技术，华信傲天确保了数据传输的加密性和完整性，有效防止了数据泄露和网络攻击。同时，WAPI解决方案还支持灵活的网络扩展和升级，能够适应不断变化的业务需求和技术发展。



华为参加

2024年通信新技术暨配电通信技术专题交流论坛

浙江省电力学会

日前在2024年通信新技术暨配电通信技术专题交流论坛上，华为等联盟会员单位参加会议，与会通信技术骨干与华为专家就WAPI安全无线局域网、全光目标网、HPLC+HRF双模通信等电力通信领域解决方案进行了深入交流。

本次会议旨在分享最新通信技术领域研究成果，探讨新型电力系统背景下配电通信网面临的机遇和挑战，分享电力通信创新实践经验。

论坛由工信部产业发展促进中心“智能电网技术与装备”委员会主任刘建明主持，浙江大学信息与电子工程学院教授、副院长王玮、华为NCE产品首席架构设计师王鹏、国网浙江信通公司通信中心副主任邱兰馨、国网泉州供电公司配网通信专家张宏坡、国网陕西信通公司通信专家王晨等分别做主题宣讲。

高通发布骁龙8至尊版移动平台 支持WAPI

高通

2024年10月21日，高通技术公司发布了骁龙8至尊版移动平台，支持WAPI。

据介绍，骁龙8至尊版移动平台首次采用了一系列领先技术，包括第二代定制的高通Oryon CPU、高通Adreno™ GPU和增强的高通Hexagon™ NPU，可带来颠覆性的性能提升。上述创新赋能骁龙8至尊版能够变革用户使用终端的体验，同时在搭载骁龙平台的智能手机上实现终端侧多模态生成式AI应用。

华硕、荣耀、iQOO、摩托罗拉、努比亚、一加、OPPO、红魔、Redmi、真我realme、三星、vivo、Xiaomi和ZTE等OEM厂商和智能手机品牌将在未来几周发布搭载骁龙8至尊版的终端。

MTK发布天玑9400移动芯片 支持WAPI

MediaTek

2024年10月9日，MediaTek发布天玑9400旗舰5G智能体AI芯片，支持WAPI，赋能移动终端向AI智能化加速迈进。

据介绍，MediaTek天玑9400凭借先进的第二代全大核架构设计、强力升级的GPU和NPU处理器，具备强大的高智能、高性能、高效能、低功耗特性，在端侧AI、移动游戏及专业影像等方面实现体验跃升。同时，天玑9400支持各类功能强大的“智能化”AI应用，可预测用户需求并提供个性化的智能服务，为终端设备赋予先进的生成式AI能力。

首批采用MediaTek天玑9400芯片的智能手机预计将于2024年第四季度上市。

西电捷通、中兴微、华为等联盟会员 在2024年数据通信标准化会上分享标准情况

物联网研究中心

2024年11月19日，2024年数据通信标准化会议在北京成功举办。西电捷通、中兴微、华为等联盟会员参会并做标准工作报告和分享。

本次会议由电子技术标准化研究院、全国信息技术标准化技术委员会数据通信分技术委员会主办。工业和信息化部电子信息司电子系统处处长金磊、国家市场监督管理总局标准技术管理司信息技术与自动化标准处处长刘大山、中国电子技术标准化研究院副院长范科峰出席会议并致辞。会议由中国电子技术标准化研究院物联网研究中心副主任卓兰主持。来自数据通信领域产学研用单位50余名代表参加会议。

在专题报告环节，中国电子技术标准化研究院物联网研究中心网络技术研究室主任杨宏、西安西电捷通无线网络通信股份有限公司副总经理黄振海、中国电子技术标准化研究院工程师雷根先后做全国信标委数据通信分技术委员会、ISO/IEC JTC 1/SC 6、IEC SyC COMM等标准化组织的工作介绍。深圳市中兴微电子技术有限公司标准总监孙波、华为技术有限公司数据通信产品线网络协议实验室主任高强周、国际星闪联盟标准与测试经理甄斌、世界无线局域网应用发展联盟秘书长杨涛分别做IEEE 802、IETF、星闪、WAA等标准化组织的工作分享。

金磊处长表示，随着新一轮科技革命和产业变革深入发展，数据通信作为前沿技术发展的根本性、基础性、保障性技术，将迎来新的发展机遇和挑战。希望数据通信标准化工作能够紧跟产业发展，推动标准体系与产业发展充分协同，促进标准研制与成果转化深度结合，加强国内标准与国际标准有机衔接，助力提升我国电子信息产业发展优势。

刘大山处长表示，数据通信是落实数字中国、数字乡村等重大战略的重要措施。数据通信标准化是引领新型基础设施建设的重要抓手，是促进产业数字化转型的关键环节，是增强信息产业国际竞争力的有效手段。在全新起点上，数据通信标准化应围绕网络技术前沿领域，满足行业迫切需求，完善标准体系建设、深化标准应用实施、打造标准生态圈层、开展国际交流与合作，推动数据通信产业高质量发展。

范科峰副院长表示，标准对信息通信产业具有基础性、先导性作用。近年来，电子标准院持续深耕标准化主责主业，完善数据通信标准体系，优化标准化组织建设，提升标准验证和服务能力，培育产业生态，取得显著成效。新形势下，电子标准院将贯彻决策部署，优化顶层设计，充分发挥全国信标委数据通信分委会平台作用，凝聚国内外资源，形成工作合力，做好标准有效供给与实施推广，促进我国在数据通信领域实现新突破。

谨慎采购美国芯片 中国互联网协会等四协会发声

人民日报

中国互联网协会声明

近日，美国以国家安全为借口，进一步加大了对华半导体出口的限制措施。美国频繁调整管制规则，持续升级贸易壁垒，无视国际贸易规则，对我国互联网产业的健康稳定发展造成了实质性损害，我会表示坚决反对。美国这种将国家安全概念泛化，并滥用出口管制手段对中国进行无端封锁和打压的做法，已经动摇业界对美国芯片产品的信任和信心。

为确保我国互联网产业安全、稳定、可持续发展，我会呼吁国内企业主动采取应对措施，审慎选择采购美国芯片，寻求扩大与其他国家和地区芯片企业的合作，并积极使用内外资企业在华生产制造的芯片。

尽管美国忽视全球供应链的稳定与安全，我国仍应坚持扩大自主开放。在确保安全的基础上，继续坚定地与全球各方建立并维护合作共赢的关系，推动全球经济的繁荣发展。在信息技术革命的关键时期，中国应与全球各界携手共进，共同攀登技术高峰，携手构建更加美好的数字未来。

中国半导体行业协会声明

12月2日，美国政府宣布了新一轮对华出口限制措施，将140余家中国企业加入贸易限制清单，涉及半导体制造设备、电子设计自动化工具等多个种类的半导体产品。美方的行为再一次破坏了全球半导体产业长期以来达成的公平、合理、无歧视的共识和WTO公平贸易的宗旨，违背了全球半导体企业共同遵循的世界半导体理事会（WSC）章程精神，伤害了全球半导体从业者团结协作的努力。美国政府随意修改贸易规则给全球半导体产业链的安全稳定已经造成实质性损害。中国半导体行业协会对此表示严重关切和坚决反对。

在全球经济一体化的今天，美国的单边主义行为不仅损害了中美两国企业的利益，也极大增加了全球半导体供应链成本。随着美国出口管制措施不断加码，其反噬效应也在持续扩大，美国对华管制措施的随意性对美国企业也造成了供应链中断、运营成本上升等影响，影响了美国芯片产品的稳定供应，美国芯片产品不再安全、不再可靠，中国相关行业将不得不谨慎采购美国芯片。

中国半导体产业的发展根植于全球化，成长和壮大于全球化。我们将始终坚持开放合作，积极同各国半导体上下游企业深化合作，促进全球产业的繁荣发展。我们强烈要求美国政府尊重行业共识，回归WSC章程的精神，维护全球半导体产业的共同利益，肩负起大国应有的担当和责任。中国半导体行业协会将维护WSC已形成的公平原则和产业共识，坚决捍卫中国半导体企业及全球供应链合作伙伴利益。呼吁相关国家和地区的企业要努力成为可靠半导体产品供应商，也呼吁中国政府支持可靠半导体产品供应商的稳定发展。

中国汽车工业协会声明

2024年12月2日，美国商务部以维护国家安全为由，宣布了新的出口管制规定，将140家中国企业列入实体清单，将更多半导体设备、高带宽存储芯片等半导体产品列入出口管制。

中国汽车工业协会坚决反对美国政府泛化国家安全概念，滥用出口管制措施，对中国进行恶意的封锁和打压，这种行为严重违反市场经济规律和公平竞争原则，破坏国际经贸秩序，扰乱全球产业链的稳定，最终损害的是所有国家的利益。

美国政府随意修改管制规则，严重影响了美国芯片产品的稳定供应，中国汽车行业对采购美国企业芯片产品的信任和信心正在被动摇，美国汽车芯片产品不再可靠、不再安全。为保障汽车产业链、供应链安全稳定，协会建议中国汽车企业谨慎采购美国芯片。

汽车是高度全球化的行业，中国汽车产业始终根植于全球化发展。中国汽车产业处于快速发展阶段，尤其是新能源汽车的高速发展是全球绿色、低碳转型的重要推动力量，也为全球汽车产业链提供了广阔的市场空间，我们欢迎全球芯片企业加强与中国汽车、芯片企业开展多方面合作，在华投资、共同研发，共享发展机会。

中国通信企业协会声明

近期，美国新增对华出口限制，将140家中国半导体公司列入贸易限制名单，禁止大多数美国供应商向这些公司发货。对美方的上述做法，中国通信企业协会表示坚决反对。

我会认为，美方以所谓国家安全为由，滥用国家力量，打压中方企业，这是赤裸裸的经济和科技霸凌，是对美方一贯标榜的市场经济原则的公然否定，损害了中国信息通信行业和包括美国用户在内的全球消费者的正当权益。美方应停止将国家安全概念泛化、将经济问题政治化的错误做法，为各国企业发展营造公平、公正、无歧视的环境。

美国政府持续泛化国家安全概念，肆意修改管制规则，限制对中国芯片和半导体设备供应，既严重破坏了国际贸易规则，又给中国信息通信行业的产业链、供应链安全稳定带来实质性损害。中国信息通信业对于采购美国企业芯片产品的信任和信心已经动摇，认为美国芯片产品不再可靠，不再安全，呼吁政府开展关键信息基础设施供应链安全调查，采取有力措施，保障关键信息基础设施安全稳定运行。

美国对华管制措施的随意性影响了美国芯片产品的稳定供应，为保障信息通信行业的产业链、供应链安全稳定，应谨慎采购美国芯片。相关企业应扩大与其他国家和地区芯片企业合作，平等对待内外资企业在中国生产的产品。

中国坚持科技成果造福全人类的理念，将进一步扩大包括集成电路产业在内的高科技产业高水平开放，积极助力知识和技术全球流动，加快数字化、智能化发展，在确保安全的前提下持续深化与各方互利共赢合作，为信息通信技术及产品应用拓宽市场空间，实现高质量发展和高水平安全的良性互动，从而促进全球产业繁荣发展。

中国通信企业协会是中国信息通信行业的社会组织，代表中国信息通信行业的利益，我会对美方的做法表示强烈不满，将坚定维护中国信息通信企业正当权益。

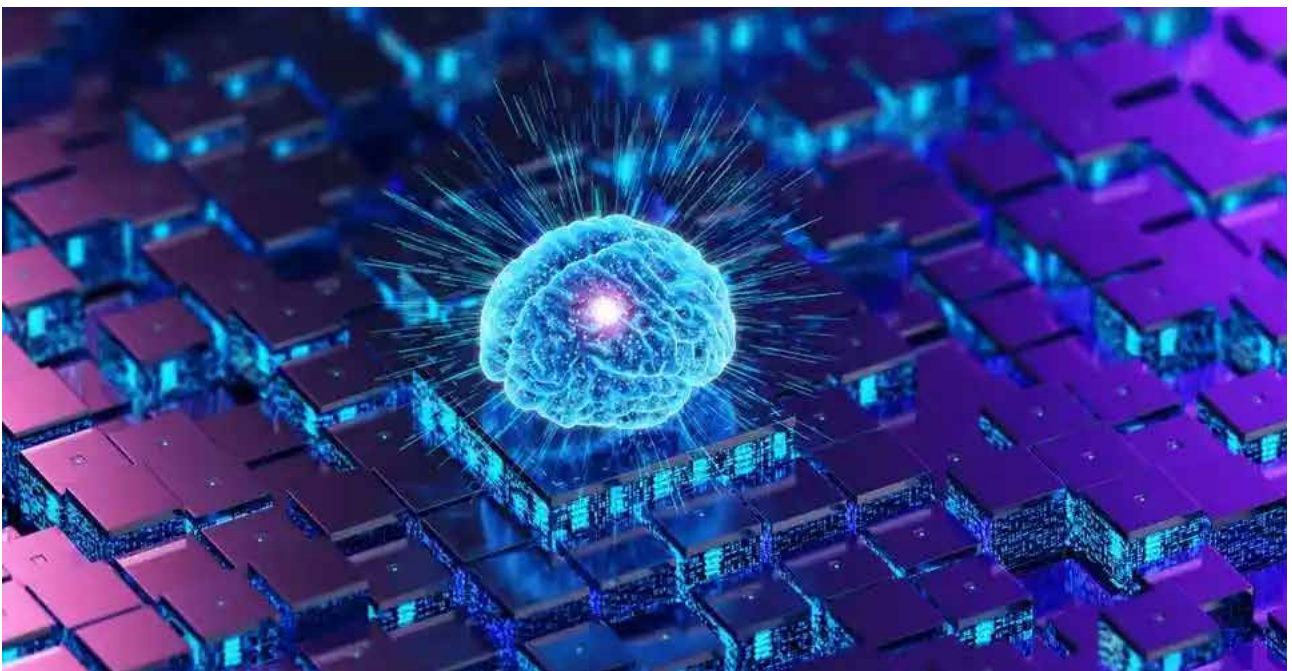
面向量子时代安全需求的WAPI 2.0技术标准体系

无线网络安全技术国家工程研究中心

随着量子技术逐步取得突破及商业化进程的加快，使用传统密码算法的网络安全协议体系面临重大挑战，迫切需要形成新一代WLAN安全技术标准体系。WAPI 2.0技术标准体系的演进目标是面向量子时代安全需求，提供抗量子攻击能力，并在身份保护、防范离线字典攻击等方面提供更高安全性，支持快速切换、确保承载的多媒体业务传输具备更高质量等。WAPI产业联盟、无线网络安全标准化委员会发布的T/WAPIA 046《无线局域网安全技术规范》，是WAPI 2.0技术标准体系的第一项标准。

一、背景

2000年，为弥补无线局域网（WLAN）国际标准ISO/IEC 8802-11存在的严重安全缺陷，中国业界在多年技术积累基础上，自主研发提出了全新的安全架构和WLAN安全协议——WAPI（无线局域网鉴别与保密基础结构），2003年被采纳入国家标准GB 15629.11/1102。WAPI所基于的三元对等安全架构，较之ISO/IEC 8802-11所基于的二转三元过渡架构具有显著技术优势，解除了接入点缺乏独立鉴别身份、依赖于与网络服务器额外建立安全传递通道，无法直接实现与终端的直接双向鉴别等安全隐患。GB 15629.11/1102标准的发布，标志着WAPI 1.0技术标准体系的形成。后续八十余项国家、行业、团体标准陆续得到发布，WAPI 1.0技术标准体系不断完善，联盟测试实验室的产品和系统测试项目，演进四个版本，持续支撑着产业创新发展。



随着量子技术的发展和突破，使用传统密码算法的网络安全协议体系正面临重大挑战，亟需形成和完善WAPI 2.0技术标准体系，面向量子时代安全需求，为无线局域网提供抗量子攻击能力。同时，随着WLAN技术的持续演进，以及SM2、SM3通用商密算法标准发布，无线局域网安全本身在身份保护、抗离线字典攻击等方面又产生了新需求，迫切需要在WAPI 2.0技术标准体系中得到响应和规范。

在上述背景下，2021年12月WAPI产业联盟、无线网络安全标准化委员会发布了T/WAPIA 046《无线局域网安全技术规范》，这是中国WLAN业界面向量子时代的网络安全挑战，结合适配通用商密算法SM2、SM3需求，使用更高性能商密算法SM4-GCM，满足身份保护需求和应对离线字典攻击、潜在量子计算攻击威胁，为向量子安全时代演进的安全WLAN产品提供架构及协议支持的新贡献。

二、T/WAPIA 046技术标准介绍

T/WAPIA 046规范的安全协议，具备身份鉴别、端口控制、密钥建立、保密通信以及WLAN管理帧保护和快速切换等功能，同时规定了与多种模式WLAN物理层技术协作时的工作方式，包括如下部分：

1、鉴别和密钥管理

- a) WAI证书鉴别和密钥管理；
- b) WAI预共享密钥鉴别和密钥管理；
- c) WAI2证书鉴别和密钥管理，采用证书的原子密钥建立与实体鉴别（AKEA-C）；
- d) WAI2预共享密钥鉴别和密钥管理，采用预共享密钥的原子密钥建立与实体鉴别（AKEA-P）。

2、WPI数据保密，包括两种工作模式：

- a) WPI-SM4-OFB+CMAC-128；
- b) WPI-SM4-GCM-128。

WAI2鉴别协议基于原子密钥建立与实体鉴别协议（AKEA），支持证书和共享密钥两种机制。在WLAN通信环境中，一个完整的通信过程既实现实体鉴别又实现保密通信，则需要实体鉴别机制和密钥建立机制二者结合。之前业界通常做法是将上述两个标准体系中分别规范的实体鉴别和密钥建立机制简单叠加组合，这种做法在流程上交互消息多，在叠加的过程中还必须考虑安全衔接等技术细节，局限性大。AKEA首次提出了原子机制，可同步实现实体身份鉴别和密钥建立两个功能，基于三元对等安全架构，具备身份保护能力、抗字典攻击、应对潜在量子计算攻击威胁等能力，提供了传统非对称密码算法向后量子密码算法演进阶段的协议安全能力提升。同时，在安全性方面，AKEA面向已知和目前可预测的各种应用技术需求，提出了通用的技术组件以

备调用；提供了多种技术机制选项，完备且适用于多样化的应用场景；在协议设计过程中，使用多种密码机制保证消息传递过程中的保密性和完整性；在同步实现密钥建立与实体鉴别过程中，利用杂凑链、身份保护、完整性校验以及签名验签等方式，保证了协议设计的原子性。



图1：密钥建立和实体鉴别模型

WAI2鉴别协议基于AKEA，使用不可还原且不可分割的消息交换序列，为两个对等实体提供实体身份鉴别和密钥建立，任何实体在收到最后一条消息之前均无法完成对其对等实体的身份鉴别或密钥建立，可满足合法客户端访问合法网络以及保密通信的安全需求。WAI2提供了一种量子安全中期演进架构，以融合运用经典密码体制的方式，为网络空间提供应对潜在量子计算攻击威胁的防御能力。

WAI2证书鉴别和密钥管理协议，选择采用主动身份保护的双向鉴别模式，预装证书后，AKEA-C支持X.509 V3及以上版本的证书规格，终端（STA）和接入点（AP）的证书通过鉴别服务器（AS）的参与完成鉴别过程。AKEA-C鉴别协议需要AS的参与，如果STA信任多个AS，STA需要提供信任的AS列表。

WAI2预共享密钥鉴别和密钥管理协议，双向鉴别模式需预置共享密钥。AKEA-P支持高强度的身份鉴别密钥和秘密的密钥交换功能，该功能对密钥交换过程进行保护，并采用非对称算法进行密钥交换，降低字典攻击的风险。

WAI2协议支持STA在AP之间快速切换，快速切换协议支持STA在AP之前无缝切换，大大降低切换时延，满足语音等上层业务持续连接需求。

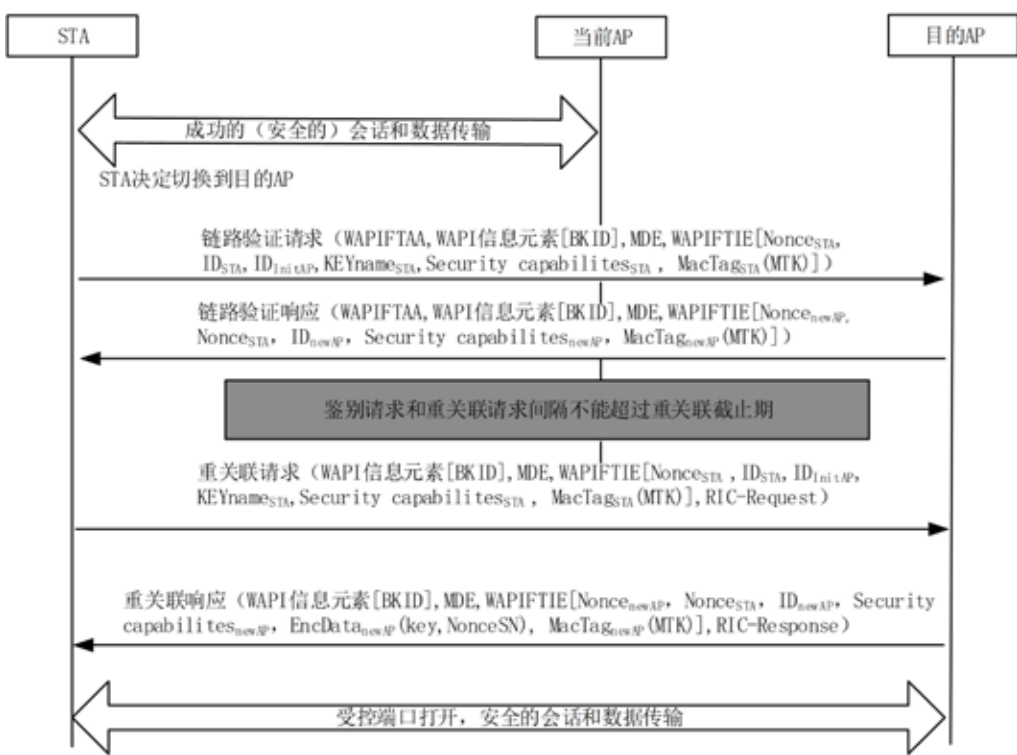


图2: WAPI快速切换协议流程

三、T/WAPIA 046安全增强

T/WAPIA 046在安全性、隐私保护、应对潜在量子计算攻击威胁和防范离线字典攻击等方面，对现有WAPI 1.0技术标准体系进行了升级与增强。包括：

1、升级采用向量子安全时代的安全协议方案缓解量子威胁，降低WLAN通信系统数据“先存储，后破解”的风险

传统的公钥密码体系，如RSA、ECC（椭圆曲线密码学）等，依赖于整数因式分解和离散对数问题的计算难度，破解所需的时间漫长，在现有技术条件下也是安全的。然而，随着量子计算机的发展，量子算法被发现能够快速破解这些问题，从而威胁传统公钥密码体系的安全性；将现在无法破解的WLAN数据先存储起来，

等到日后量子计算机成熟再进行破解——“先存储，后破解”也是威胁当前WLAN安全的一种攻击手段。虽然目前量子计算机没有达到威胁经典加密的水平，但需要提前准备好应对措施，为了应对潜在量子计算攻击威胁，T/WAPIA 046升级采用AKEA机制，AKEA采取混合设计策略，缓解量子威胁，提供了向量子安全时代过渡的统一鉴别与密钥建立解决方案。

2、新增支持身份保护功能，在保障通信安全的同时保护用户隐私

数字身份是无线网络安全接入证明用户或设备真实身份的重要凭证，数字身份中的信息不仅包括基本的身份信息，如名称、唯一标识等，还可能包括更为敏感的其他管理信息、行为数据等。这些信息一旦被非法获取或泄露，很可能给个人或系统构成安全威胁。

T/WAPIA 046增加了对数字身份的保护，只允许受保护的身份数据在参与WAPI鉴别过程的实体设备间传递，系统外将无法直接在协议交互过程数据中访问到用户身份数据，防范隐私泄露，实现在无线接入过程中用户身份等敏感信息不会被窃取，防止用户轨迹被非法追踪。

3、新增支持快速切换机制，满足音视频等流媒体业务无中断传输

WLAN具有高带宽、高速率、移动性、安全等优势，是个人家庭网络和行业局域网络的首选，如手持设备移动、巡检机器人行进等，经常出现无线切换网络的情况，切换过程中如果是断开重连则一般需要数秒才能重新建立链路，视频等实时通信业务可能出现卡顿、黑屏甚至中断等。T/WAPIA 046增加支持了快速切换机制，通过STA和AP间的快速切换协议，在同一移动域范围内可将切换时间控制在毫秒级，减少客户端在切换过程中的时间延迟，保证业务数据连接的连续性，实现流畅切换提高服务质量。

4、升级支持防范离线字典攻击，提供可靠前向安全性，防范窃听者暴力破解获得密码和通信数据

基于预共享密钥的鉴别机制通常采用口令作为网络接入的凭证，是个人网络及临时网络常用的安全方式。由于无线电波的开放性，攻击者在无线通信中很容易捕获无线电波获取通信数据，通过使用一个预先定义好的单词列表（称为密码字典，例如：英文单字、生日的数字组合、以及各种常被使用的密码等）来尝试破解，或尝试所有可能的口令组合的方式等暴力字典攻击来猜测口令，可直接攻击网络，也可能因解密之前捕获的数据而获取用户敏感信息。协议升级结合密码技术应用，隐藏密钥直接运算结果信息，防止窃听者通过离线暴力字典攻击来猜测口令，使攻击者更难破解无线口令，即使攻击者知道网络的口令，也无法解密之前曾捕获的通信数据。

5、全面适配通用国密算法，提供更高强度安全

T/WAPIA 046在WAPI 1.0技术标准体系的基础上进一步提升了安全性，提升了密码防御强度，适配通用商密算法SM2和SM3，提供256位更高强度的安全；持续使用SM4，规范了更高性能商密算法模式SM4-GCM。

同时，T/WAPIA 046兼容WAPI 1.0技术标准体系，在实际部署中提供了向新安全方案的有序过渡，适应了平滑演进、兼容互通的产业需求。

关于无线网络安全技术国家工程研究中心

无线网络安全技术国家工程研究中心，以下简称“工程中心”是国家（发展改革委）在基础性网络连接和互联安全领域布局的唯一的产业技术创新基础设施，成立于2011年12月，设有技术集成研发、密码工程验证、协议测试技术、电子政务应用、智能电网研发应用、产业协作等六个中心。

自2011年12月成立以来，工程中心聚焦网络空间安全基础共性技术，聚合国内外优质创新资源，开展区域性跨学科、大协同的基础研究和应用基础研究，持续深入解决网络信息领域原创性关键技术和“卡脖子”技术，推动科技成果转化与产业化，在“新基建”中发挥好产业技术创新基础设施的国家队作用。

工程中心已提出/参与提出20余项国际领先的网络安全协议技术，涵盖无线局域网（WLAN）、有线局域网、近场通信（NFC）、射频识别（RFID）、移动通信等网络安全领域，应用场景包括工控、金融、电力、海关、能源、交通等行业，以及物联网、智能家居、车联网、电子支付等，促进形成了三元对等（虎符TePA）网络安全技术架构体系。

工程中心为全球的用户提供不断创新的网络安全协议技术与解决方案和安全网络装备与解决方案，致力于保障网络连接的安全与可信。对密码算法、密码机制的长期深入研究，保障了安全协议安全高效执行和法规遵从。

WAPI 产业联盟成员单位名录

- 中国移动通信集团公司
中国电信集团公司
中国联合网络通信集团有限公司
国家密码管理局商用密码检测中心
国家无线电监测中心检测中心
西电捷通公司
北大方正集团有限公司
北京中电华大电子设计有限责任公司
中电科普天科技股份有限公司
深圳市明华澳汉智能卡有限公司
北京数字认证股份有限公司
北京六合万通微电子技术股份有限公司
无锡中太数据通信有限公司
青岛海尔科技有限公司
海信集团有限公司
联想(北京)有限公司
华为技术有限公司
大唐移动通信设备有限公司
北京朗波芯微技术有限公司
大唐微电子技术有限公司
上海鼎芯科技有限公司
北京天一集成科技有限公司
北京联信永益信息技术有限公司
深圳鑫金浪电子有限公司
深圳市普天宜通科技有限公司
北京汉铭信通科技有限公司
西安大唐电信有限公司
深圳共进电子股份有限公司
北京华安广通科技发展有限公司
深圳国人通信有限公司
东蓝数码有限公司
美国安移通网络公司北京代表处
北京五龙电信技术公司
北京同耀通电子科技有限公司
北京登合科技有限公司
宇龙计算机通信科技(深圳)有限公司
上海润欣科技有限公司
弘浩明传科技股份有限公司
京信通信技术(广州)有限公司
北京城市热点资讯有限公司
优比无线技术(深圳)有限公司
南京智达康无线通信科技股份有限公司
上海欣民通信技术有限公司
福建三元达通讯股份有限公司
- 新华三技术有限公司
北京傲天动联技术股份有限公司
中兴通讯股份有限公司
武汉虹信通信技术有限责任公司
广州市卓纪思网络科技有限公司
赛芯电子技术(上海)有限公司
雷凌科技股份有限公司
瑞晟微电子(苏州)有限公司
联发科技股份有限公司
四川天邑信息科技股份有限公司
湖南城市热点无线通信有限公司
珠海市魅族科技有限公司
深圳市雄脉科技有限公司
奥泰尔科技(深圳)有限公司
北京网贝合创科技有限公司
网件(北京)网络技术有限公司
上海市数字证书认证中心有限公司
北京创原天地科技有限公司
阿德利亚科技(北京)有限责任公司
深圳市华讯方舟软件信息有限公司
迈创智慧供应链股份有限公司
科通宽带技术(深圳)有限公司
邦讯技术股份有限公司
惠州市宝丰信息科技有限公司
晨星软件研发(深圳)有限公司
卓望数码技术(深圳)有限公司
迈普通信技术股份有限公司
北京汇通融业科技发展有限公司
上海寰创通信科技有限公司
吉翁电子(深圳)有限公司
北京汇为永兴科技有限公司
福建星网锐捷网络有限公司
北京新岸线移动多媒体技术有限公司
广东欧珀移动通信有限公司
上海贝尔股份有限公司
成都鼎桥通信技术有限公司
飞天联合(北京)系统技术有限公司
中国电力科学研究院
锐迪科微电子(上海)有限公司
苏州汉明科技有限公司
神州数码网络(北京)有限公司
北京必虎科技股份有限公司
北京市政务信息安全保障中心
天津赞普科技股份有限公司
- 上海连尚网络科技有限公司
深圳市瑞科慧联科技有限公司
深圳市信锐网科技术有限公司
福建新大陆通信科技股份有限公司
北京比邻科技有限公司
天津市电子机电产品检测中心
高通无线通信技术(中国)有限公司
中科开创(广州)智能科技发展有限公司
北京华信傲天网络技术有限公司
南京博洛米通信技术有限公司
广西新海通信科技有限公司
上海麓慧科技有限公司
深圳市智开科技有限公司
南方电网数字电网研究院有限公司
深圳航天科创实业有限公司
南方电网深圳数字电网研究院有限公司
广西电力线路器材厂有限责任公司
广西通量能源技术有限公司
恩智浦(中国)管理有限公司
南方电网科学研究院有限责任公司
山东华辰泰尔信息科技股份有限公司
山东思极科技有限公司
深圳市国电科技通信有限公司
北京至周科技有限公司
北京联盛德微电子有限责任公司
北京市柴傅律师事务所
北京佰才邦技术股份有限公司
瑞斯康达科技发展股份有限公司
北京智芯微电子科技有限公司
广州莲雾科技有限公司
安徽皖通邮电股份有限公司
东瑞易达科技(山东)有限公司
北京邦粹科技有限公司
西安芯语慧联信息科技有限公司
重庆物奇微电子股份有限公司
山东鲁软数字科技有限公司
上海威锐电子科技股份有限公司
国网智能科技股份有限公司
北京锐云通信息技术有限公司
北京中电飞华通信有限公司
广东优力普物联科技有限公司
广州广哈通信股份有限公司
南京云程半导体有限公司
许昌许继软件技术有限公司
深圳鼎信通达股份有限公司

WAPI Alliance
产业联盟



地 址：北京市海淀区知春路27号量子芯座1608室

邮 编：100191

电 话：010-82351181

传 真：010-82351181 ext. 1901

邮 箱：wapi@wapia.org

网 址：<http://www.wapia.org.cn>