美国安局研发量子计算机 可破解全球任何密码

文章来源：闻客网

本文摘要：越来越多的报道表明，美国国安局（NSA）可以在全世界拦截、监听人们的通信数据和上网记录，然而面对拦截获取的加密信息，国安局还有一个工作——那就是破解加密，获取不加密的“明文”。据美国《华盛顿邮报》网站3日报道，国安局正在加紧研发性能强大的量子计算机，如果成功，可以破解全世界任何密码和加密算法。该报称，国安局的量子计算机，处理性能远远超过基于晶体管的传统计算机，将可以攻破目前用于金融业、医疗行业、商业、政府部门的所有加密信息。不过，美国的物理学家和计算机科学家，对于国安局量子计算机研发到何种水平，保持质疑，尤其是是否比学术界的研发水平更为先进。目前国安局并未对外披露任何进展，但是斯诺登披露的文件显示，国安局的量子计算机，研发水平并未超过学术界。国安局的一份机密文档提到：“在量子计算机研究上，全球的进展已经演变成欧盟和瑞士的相对领先。

腾讯科技 晨曦 1月3日编译

越来越多的报道表明，美国国安局（NSA）可以在全世界拦截、监听人们的通信数据和上网记录，然而面对拦截获取的加密信息，国安局还有一个工作——那就是破解加密，获取不加密的“明文”。据美国《华盛顿邮报》网站3日报道，国安局正在加紧研发性能强大的量子计算机，如果成功，可以破解全世界任何密码和加密算法。

该报称，国安局的量子计算机，处理性能远远超过基于晶体管的传统计算机，将可以攻破目前用于金融业、医疗行业、商业、政府部门的所有加密信息。

《华盛顿邮报》引述斯诺登披露的部分文件称，国安局的量子计算机研发计划，属于一个斥资7970万美元、名为“渗透硬目标”的研发计划，研发合同对外保密，在马里兰州College-Park的一个秘密实验室进行。

研发量子计算机，一直以来是科学研究机构的目标，其计算能力，将会对医学等领域起到重大推动作用。而对于美国国安局来说，量子计算的能力，主要体现在破解密码和加密上，它可以破解市面上几乎所有的“公钥加密技术”，目前全世界大量网站和政府部门，使用了诸如RSA等公钥加密算法。

不过，美国的物理学家和计算机科学家，对于国安局量子计算机研发到何种水平，保持质疑，尤其是是否比学术界的研发水平更为先进。目前国安局并未对外披露任何进展，但是斯诺登披露的文件显示，国安局的量子计算机，研发水平并未超过学术界。

美国麻省理工学院的学者Scott-Aaronson表示，国安局的量子计算机，大幅领先民用研究不太可能。

国安局的一份机密文档提到：“在量子计算机研究上，全球的进展已经演变成欧盟和瑞士的相对领先。”

麻省理工学院的量子力学教授劳埃德（Seth-Lloyd）认同国安局的评估，他表示，在过去十年中，欧盟和瑞士在量子计算上取得了重要进展，已经赶上了美国的水平。

秘密文件显示，国安局的量子计算机研发，在大型密闭的屋子中进行，术语称之为“法拉第笼”，主要是防止电磁能量外泄

或者进入，这是量子计算试验所必需的环境。

全世界第一台量子计算机何时研发成功，目前学术界并无一致观点。十年前，一些专家预测还需要花费10年到100年。而在五年前，劳埃德教授预测至少还需要十年（即大约在2020年研发成功）。

最近，劳埃德在接受媒体采访时表示，国安局研发用于破解加密的量子计算机，至少还需要五年时间，如果无法取得重要进展，则还需要等待更长时间。

实际上，一些公司已经宣布研发成功小型的量子计算机，比如加拿大的D-Wave系统公司，自称已经从2009年开始制造量子计算机，2012年，该公司对外销售一款价值1000万美元的量子计算机，客户包括谷歌(微博)、美国宇航局以及全美大学太空研究协会。

不过，这些市面上已经出现的小型量子计算机，显然无法完成美国国安局破解密码的任务。

资料显示，所谓量子计算机，是遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理设备。当某个装置处理和计算的是量子信息，运行的是量子算法时，它就可以称为量子计算机。

（闻客网 venk.cn）