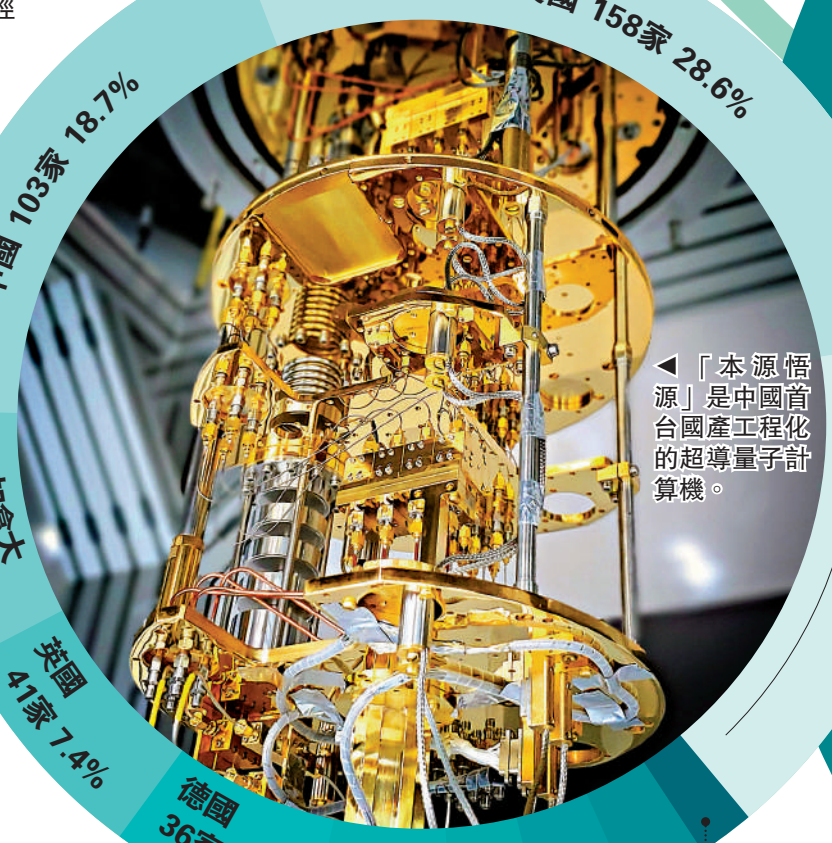
「本源悟空」裝備「抗量子攻擊護盾」

自主量子計算機 實現「攻守兼備」

2024年是「總體國家安全觀」提出十周年，總體國家安全觀強化「大安全」理念，涵蓋政治、軍事、國土、經濟、金融、文化、社會、科技、網絡、糧食、生態、資源、核、海外利益、太空、深海、極地、生物、人工智能、數據等諸多領域，形成制度安全、產業鏈供應鏈安全等新的安全理念，並隨着時代和實踐的發展而不斷豐富發展。

隨着全球開展「量子算力」競賽，現有「數據加密防線」缺口乍現，量子領域的「攻」與「守」成為業界一大聚焦。日前，中國第三代自主超導量子計算機「本源悟空」成功裝備國內首個PQC「抗量子攻擊護盾」——PQC（Post Quantum Cryptography後量子密碼）混合加密方法。這將使「本源悟空」更好抵禦其他量子計算機的攻擊，確保運行數據安全。本源悟空「鑄盾」，意味着中國自主超導量子計算機可以「攻守兼備」，成為中國數據安全新技術應用的重要探索。



◀「本源悟源」是中國首台國產工程化的超導量子計算機。

話你知

取名「悟空」 寓意72變

中國第三代72比特超導量子計算機取名「悟空」，來源於中國傳統文化中的神話人物孫悟空，寓意如孫悟空般「72變」。量子計算芯片安徽省重點實驗室副主任賈志龍博士介紹，「悟空」搭載的是72位超導量子芯片「悟空芯」。這款芯片在中國首條量子芯片生產線上製造，共有198個量子比特，其中包含72個工作量子比特和126個耦合器量子比特。

資料來源：央視網

量子信息領域企業分布

（截至2023年9月）
數據來源：中國信息通信研究院

量子安全直接通信「四大標準」

量子加密Q&A

固若金湯？

量子密碼能夠保證信息高度安全，即使攻擊者擁有無限計算能力，也未必可破解量子密碼。

獨一無二？

實現了通信雙方能夠互發加密信息，並使用各自的私鑰進行解密。公鑰，即可公開的鑰匙，用於信息加密，私鑰，需要保密，用於信息解密。由於公鑰和私鑰是通過數學方法生成的，且無法從公鑰推導出私鑰，因此具有極高的安全性。

雙向驗證？

哈希函數和數字簽名技術加持下，量子密碼能夠實現信息的數字簽名和認證，從而保證通信雙方能夠驗證信息的來源和完整性。

竊聽者

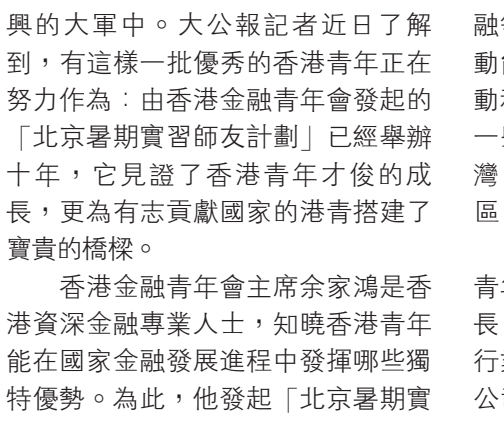
【大公報訊】綜合新華社、中國科學報報道：量子計算機因其超強算力可以對原本的公鑰密碼體系產生嚴重威脅，而PQC技術能夠有效地抵抗量子計算機的攻擊。因此，世界各國紛紛加速推進PQC遷移以替換原本的公鑰密碼體系。2023年，美國國家安全局發布文件，明確鼓勵盡早向PQC遷移。蘋果近期推出的iMessage加密方案以及谷歌在其瀏覽器中部署的混合加密方案均包含了PQC算法。

安徽省量子計算工程研究中心副主任竇猛漢介紹，「本源悟空」此次上載的PQC「抗量子攻擊護盾」由本源量子計算科技（合肥）有限公司研發，是國內首次實際應用，邁出攻守兼備新階段。

歐美強化布局 升級產品服務

美國早在2002年就發布《量子信息科學與技術規劃》，並在2021年10月發布抗量子密碼過渡路線圖。德國聯邦信息安全辦公室(BSI)2020年8月發布《後量子密碼遷移報告》，提出抗量子密碼遷移建議。

產業界方面，國際互聯網工程任務組（IETF）發布哈希類抗量子密碼技術標準；谷歌、微軟、東芝等企業已開展抗量子密碼技術和產品研發，在水下數據中心、地鐵等進行抗量子密碼試驗，推出相關商業服務和升級產品等。



▲本源量子多台量子計算機正在運行。 中新社

培育骨幹企業 做好風險預判

內地網絡安全界指出，密碼技術研發和應用直接關係國家安全。在當前信息技術飛速發展等形勢下，要高度重視、前瞻謀劃、系統推進抗量子密碼技術研發、應用等工作。

一是加強統籌布局，研究制定我國抗量子密碼行動計劃。積極跟蹤全球量子計算機、抗量子密碼等發展動態，強化布局謀劃。

二是強化研發與應用，加快培育一批抗量子密碼企業。加快培育一批抗量子密碼骨幹企業，鼓勵抗量子密碼與大數據、區塊鏈、雲計算等新一代信息技術融合創新，促進我國密碼產業生態發展。

三是做好風險預判，加快形成自主可控的技術標準體系。加強量子威脅、抗量子密碼應用的風險研判，構建全面的量子威脅防禦體系。

四是開展國際合作，爭取國際話語權和國際規則制定權。加強與ISO、ITU等國際標準化組織溝通，適時推動我國主導和參與的抗量子密碼國際標準。中國第三代自主超導量子計算機「本源悟空」今年1月6日上線運行，搭載72位自主超導量子芯片「悟空芯」，是目前先進的可編程、可交付超導量子計算機。截至4月10日，「本源悟空」已累計為來自117個國家的用戶完成逾16.9萬個運算任務，全球訪問量超551萬次。

歐美攻關抗量子密碼技術

美國
在2002年就發布《量子信息科學與技術規劃》，並在2021年10月發布抗量子密碼過渡路線圖

德國
德國聯邦信息安全辦公室（BSI）2020年8月發布《後量子密碼遷移報告》，提出抗量子密碼遷移建議

法國
法國總統2021年1月宣布啟動總金額18億歐元的國家量子技術投資計劃，其中1.5億歐元用於抗量子密碼技術。法國國家網絡安全局於2022年，發布《關於後量子密碼學遷移的科學和技術建議》，建議提出抗量子密碼發展的路線圖

科企
國際互聯網工程任務組（IETF）發布哈希類抗量子密碼技術標準
谷歌、微軟、東芝、LG、CryptoNext等企業已開展抗量子密碼技術和產品研發，在水下數據中心、地鐵等進行抗量子密碼試驗，推出相關商業服務和升級產品等

資料來源：中國科學報

維護國安 升級算法儲備技術

加速部署

從歐美國家的動向來看，抗量子密碼技術發展已進入關鍵時期，美國在這輪技術競賽中佔據先機和優勢。內地專家指出，中國須及早研究部署，警惕相關風險。

首先需要警惕抗量子密碼技術「卡脖子」風險。目前，全球抗量子密碼領域已基本形成「美國主導、歐洲跟隨」的格局，美抗量子密碼標準將在全球密碼領域的優勢地位進一步鞏固。一旦出現這種情況，中國將十分被動，面臨採用美標準帶來的網絡安全風險、巨額專利費用、喪失國際話語權等問題。抗量子密碼產業化壁壘風險也值得及早部署。目前，中國產業界在抗量子密碼領域的投入相對不足。一旦歐美抗量子密碼進入大規模實用化，中國企業可能需要數年時間購買和研發必要的技術，面臨密碼產品和服務的巨大壁壘，甚至失去密碼產品的國際競爭力和市場佔有率。

同時須警惕量子計算機帶來的網絡安全風險。據預測，量子計算機在10–20年將達到攻破現有密碼算法的能力，在此之前能否實現抗量子密碼的成熟應用和遷移，是非常關鍵也極具挑戰的工作。同時，在當前複雜的國際形勢下，也需要防範國外追溯性解密風險，即提前攔截和存儲有關量子加密信息並在量子計算機技術成熟後進行解密。 中國科學報

助港青搭建赴內地實習橋樑 了解金融強國建設

【大公報訊】記者馬靜北京報道：以中國式現代化推進「金融強國建設」漸入「加速度」，作為國際金融中心的香港，亦必將大有可為。擁有國際視野和極強專業能力的香港青年也正積極參與到強國建設和民族復興的大軍中。大公報記者近日了解到，有這樣一批優秀的香港青年正在努力作為：由香港金融青年會發起的「北京暑期實習師友計劃」已經舉辦十年，它見證了香港青年才俊的成長，更為有志貢獻國家的港青搭建了寶貴的橋樑。

香港金融青年會主席余家鴻是香港資深金融專業人士，知曉香港青年能在國家金融發展進程中發揮哪些獨特優勢。為此，他發起「北京暑期實習師友計劃」，為香港金融專業學子搭台賦能，「很高興，十年來大量香港青年參與這項活動，願意為國家金融強國建設發力，他們很多人都已經成長為香港金融界的骨幹人物。」

「當前國際形勢複雜，香港也需要面臨許多新的挑戰。香港金融青年會也在努力培養未來的金融領袖。」余家鴻認為，到內地大型企業和金融機構實習是讓香港金融才俊成長為金融領袖的重要一步，今年希望實習活動能有所創新，增加一些學生自主活動和更多與時俱進的內容，比如走進一些新興科技園區，未來還要走進大灣區一些與金融緊密相關的科技園區。

香港中文大學王嘉豪是香港金融青年會「北京暑期實習師友計劃」團長，他說，此前通過實習接觸了很多行業，包括科技風險諮詢、內地證券公司、非營利組織、四大會計師事務所和初創企業。這些充滿活力的行業匯聚在金融、諮詢和信息技術的交匯點上，為自己提供了涵蓋行業研究、項目管理、數據分析等方面的綜合技能。他認為香港青年在成為未來金融領袖方面擁有許多優勢。首先，香港大學在商科方面有較高排名，香港青年接受了高質量的教育，具備扎實的金融、經濟等相關領域的知識基礎。此外，香港眾多金融機構為年輕專業人士提供了豐富的實踐機會和職業發展空間，提升他們的專業技能和領導能力。

▲麥美娟（右）和余家鴻（中）與參加師友計劃的團員親切交流。 受訪者供圖

全國人大法工委：防控校園欺凌 依法追究刑責

【大公報訊】記者馬靜北京報道：近期，學生欺凌問題在內地引發廣泛關注。對此，全國人大常委會法工委發言人楊合慶19日在記者會上回應相關問題時指出，學生欺凌如果構成嚴重不良行為、違反治安管理行為或者犯罪行為的，有關部門應當依法處置，包括依法將欺凌者送入專門學校接受專門教育、作出治安管理處罰或者追究刑事責任等。他強調，下一步將完善工作機制，促進法律正確有效實施，為未成年人健康成長創造更好的社會環境。

楊合慶介紹，2020年修訂的未成年人保護法、預防未成年人犯罪法，對學生欺凌問題作了有針對性的規定。

一是規定了學生欺凌的含義，學生欺凌是指發生在學生之間，一方蓄意或者惡意通過肢體、語言及網絡等手段實施欺壓、侮辱，造成另一方人身傷害、財產損失或者精神損害的行為。

二是強調父母或者其他監護人不得放任、唆使未成年人欺凌他人。

三是明確學校處置學生欺凌的責任，包括建立學生欺凌防控工作制度，加強日常安全管理；依法認定和處理學生欺凌行為；對相關未成年學生及時給予心理輔導、教育和引導；對相關未成年學生的父母或者其他監護人給予必要的家庭教育指導；對實施欺凌的未成年學生依法加強管教；對嚴重的欺凌行為應當及時向公安機關、教育行政部門報告，並配合相關部門依法處理。

四是規定教育行政部門應當會同有關部門建立學生欺凌防控制度。

楊合慶還在記者會上介紹，十四屆全國人大常委會第九次會議於4月23日至26日在北京舉行，會議將繼續審議學位法草案、關稅法草案；審議委員長會議提請審議的國防教育法修訂草案；審議國務院提請審議的會計法修正草案、統計法修正草案、能源法草案、原子能法草案、反洗錢法修訂草案、農業技術推廣法等3部法律的修正案草案、關於授權國務院在海南自由貿易港暫時調整適用食品安全法有關規定的決定草案等。