荷蘭愛因荷芬科技大學進入抗量子加密標準競賽準決賽

駐歐盟兼駐比利時代表處教育組

美國國家標準技術研究院(NIST)所舉辦的抗量子加密的全球競賽中，荷蘭愛因荷芬科技大學(TU/e)的兩個團隊已順利進入準決賽。

根據該校表示，進入準決賽的兩種演算法很有可能成為新的加密標準。而另外還有兩個方案也已被選為替代方案，並將繼續參賽。

美國國家標準技術研究院(NIST)之競賽為了找到可以保護電腦的加密標準，美國國家標準技術研究院發起了一項為期多年的競賽，希望能找到最佳的解決方案。而獲獎的方案將成為全球政府和企業的新標準。

美國國家標準技術研究院於 2017 年開始發起的競賽，總共有 69 個競賽項目，目前已進入第三輪階段。對於這一輪的決賽，該研究院遴選七個入圍團隊，其中包括兩個來自愛因荷芬科技大學的團隊：Classic McEliece 和 NTRU。另外還選了八個備取團隊，其中也包括愛因荷芬科技大學的兩個團隊：NTRU Prime 和 SPHINCS＋。這些備取團隊也將進入第三輪的競賽，但需要到第四輪才有可能成為進入決賽的團隊 。

高安全性

數學暨電腦科學學院之編碼學和密碼學研究小組的教授 Tanja Lange 說:「我會向所有想避免機密被未來量子攻擊的人推薦 McEliece。對於空間有限的用戶，我建議使用 NTRU 和 NTRU Prime 進行加密。我很高興美國國家標準技術研究院分享了我的建議。」

SPHINCS＋團隊負責人兼助理教授 Andreas Hülsing 補充說：「很高興看到美國國家標準技術研究院讓我們的 NTRU 成為進入決賽的團隊之一。除此之外還認可 SPHINCS＋極為可靠的安全性，並宣布它可用於要求高安全性的應用程序。」

從今年秋季開始，進入決賽的團隊將接受最終檢視。但在此之前，參賽團隊有機會進一步調整他們的演算法。美國國家標準技術研究院預計整個過程將在未來兩到四年內完成。

脆弱的密碼學

世界各地的研究人員都正致力於製作量子電腦。這些電腦預計將可以解決一般電腦無法解決的問題，但由於量子電腦運算速度太快，也可能因此破壞保護我們敏感的通訊系統和數據的加密，例如國家機密和病歷。

儘管當前的加密算法在我們大多數的數據通訊中都可以正常運作，卻仍然很脆弱。他們使用一般電腦不可能破解且非常複雜的數學問題，而這些問題卻可以在功能強大的量子電腦上輕易解決。目前的量子電腦仍然缺乏執行此任務的計算能力，但情形也有可能隨時改變。美國國家標準技術研究院所舉辦的競賽目的即在此之前提出替代的演算法。

撰稿人/譯稿人：劉厚諄

資料來源：2020 年 7 月 27 日，TU/e in finale cryptostandaardwedstrijd voor quantumpc，https://www.computable.be/artikel/nieuws/security/7024488/5440850/tu-e-in-finale-cryptostandaardwedstrijd-voor-quantumpc.html