

人工智能安全

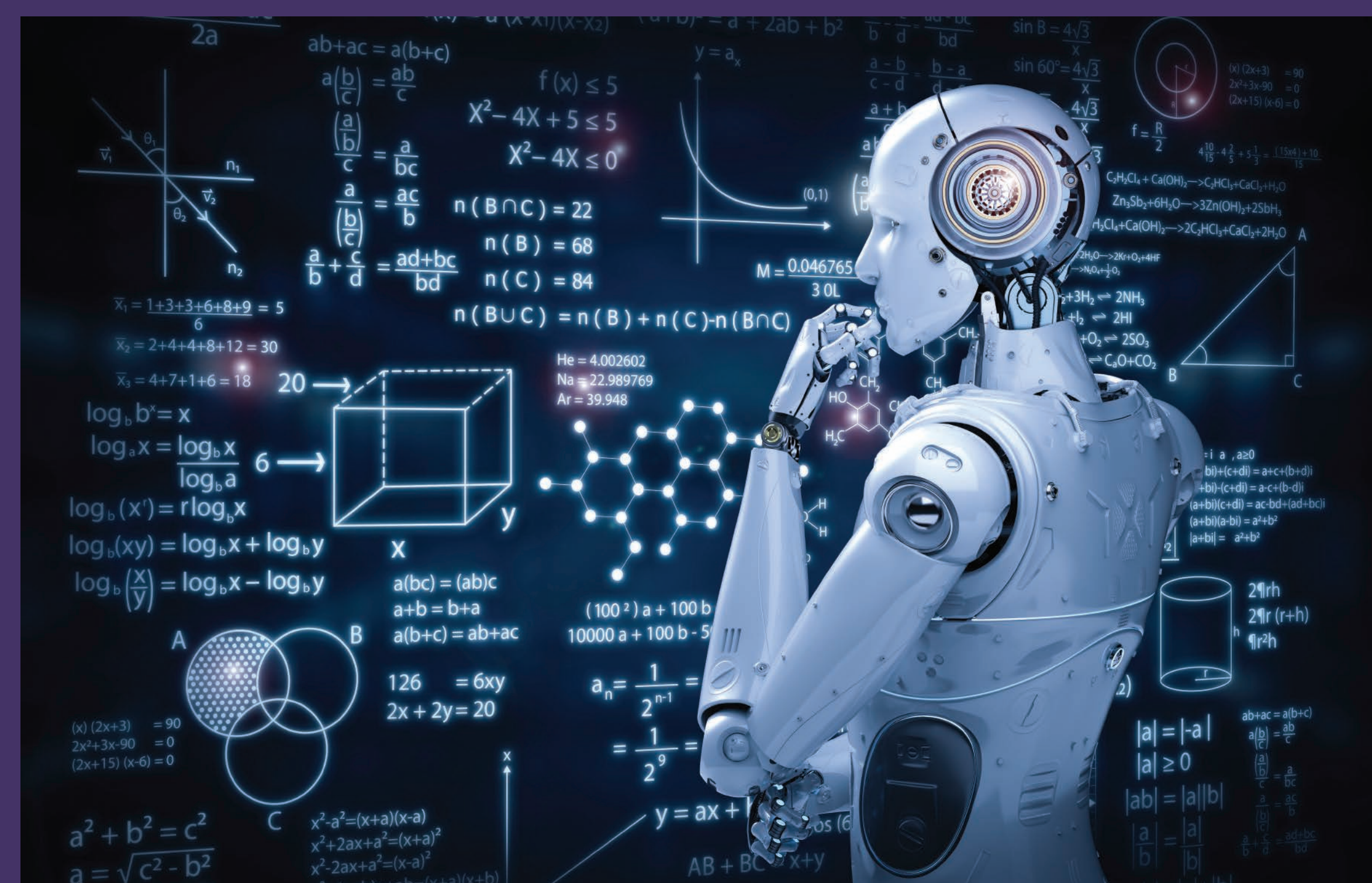
人工智能的潛在風險包括：惡意應用、私隱數據洩露、算法模型缺陷、輸出信息內容的安全風險、取代工人職位並降低就業率、敵對軍事應用。維護人工智能安全，必須確保人工智能可靠、可控、安全。

人工智能指一系列涉及以電腦程式和機器模仿人類解決問題的能力，應用科技例子包括臉容識別、語音識別、聊天機械人、數據分析、自動化決策或建議等。人工智能科技仍在演變中，更多新的應用或會出現。



鑑於人工智能一方面在促進生產力及經濟增長方面有巨大潛力及在香港日漸普及，另一方面亦存在私隱及道德風險，個人資料私隱專員公署於2021年8月頒布《開發及使用人工智能道德標準指引》，讓機構在開發及使用人工智能時有所依循。相關道德原則包括：問責、人為監督、透明度可解釋性、數據私隱、公平、有益、可靠穩健及安全。

人工智能科技在學術方面的應用



人工智能科技正在急速發展中。智能聊天機器人程式（例如 ChatGPT）在學術界的應用，成為全球高等教育界的重要議題。就學生在學習作業或撰寫論文是否可以使用人工智能程式，部分大學容許學生在符合特定條件（如作出明確引述）下可以使用；一些大學原則上暫時全面禁止使用（獲書面許可者除外），以待擬訂更全面的指引。

數據安全

數據安全是網絡空間安全的基礎，是國家安全的重要組成部分。數據是指任何以電子或者其他方式對信息的記錄。數據安全是指通過採取必要措施，確保數據處於有效保護和合法利用的狀態，以及具備保障持續安全狀態的能力。

維護數據安全面臨的機遇和挑戰包括：非法登入、篡改、使用、傳送數據，惡意攻擊，侵犯個人隱私等問題。

香港的《個人資料(私隱)條例》是專門為了保障個人資料安全而定立的。條例賦予國際認可的保障資料原則法定效力，並設立獨立的法定機構——個人資料私隱專員公署，以負責條例的執行工作和促使各界人士遵守條例的規定。

維護個人資料安全



私隱專員鍾麗玲表示，個人資料私隱專員公署於2022年接獲投訴個案上升，主要與2021年打擊起底的新條文生效有關。（2023年2月10日）

香港個人資料私隱專員公署公布2022年工作報告，指該年接獲的總體投訴個案上升15%，與起底相關的投訴佔近一半。與網絡私隱相關的騙案也時有發生，報告披露，香港銀行學會網絡被提醒存在保安漏洞，經電腦保安事故協調中心介入後仍未及時堵塞有關漏洞，令黑客有機可乘，「騎劫」學會多台伺服器以換取贖金，伺服器內載有超過11萬名市民的敏感個人資料。公署批評銀行學會在資料保安風險管理、資訊系統管理等方面存在不足。