量子コンピュータおよび量子暗号の動向および関連するスタートアップの発展の方向性

TAcc+ スタートアップ分析チーム

量子コンピューティング（Quantum computing）技術の急速な発展は、現在使用されている暗号化および復号化システムに衝撃を与えることになる。自分で蒔いた種は自分で刈り取る、という訳で、先進国ではすでに次世代の情報セキュリティ技術（「量子暗号（Quantum Cryptography）」）の研究および規格の制定が進められており、後進の国は遅れをとらないようにしなければ、リスクをコントロールしビジネスチャンスを掴むことができなくなるのは必定である。

量子には、光子、電子またはイオンなどがあり、物理的な操作によって量子の重ね合わせおよび量子のもつれが形成する。このような特性の下では、1つの量子が同時に 2 種類の物理状態にあり、かつ 2 つの量子間に接続が形成され、たとえ同じ空間にない場合でも、リアルタイムに相互に影響し合うことが可能である。科学者はこの特性を量子コンピューティングの基本単位として、コンピューティングに応用し、量子ビット（qubit）と呼んでいる。量子コンピューティングは、特定の種類の数学問題を解くための強大な能力を有しており、素因数分解（RSA）など現在の主流の暗号化アルゴリズムを簡単に解読することができるため、高度にデジタル化した世界の政治経済環境に避けられない衝撃およびリスクをもたらすことになる。2019 年に米国のナショナルアカデミーズプレス（National Academies Press）が出版した書籍『量子コンピューティング：進展およびビジョン』では、代表的なアルゴリズムである Shor を使用して RSA1024 を解読する場合は概ね 2,300 量子ビットが、Grover のアルゴリズムを使用して AES-GCM を解読する場合は 3,000 量子ビットが必要であると指摘されている。

1.全世界における量子コンピュータの発展動向

現在、先進各国は続々と量子情報技術の研究開発に対する投資を加速しており、中でも EU、米国、中国、日本および韓国が関連技術の特許申請数でトップを走っている。IBM、Google、Microsoft、Intel、Amazon など大手テクノロジー企業は、いずれもすでに長年にわたる投資を経て、優位なリードを獲得している。例えば、IBM は 2020 年に 65 量子ビットの量子プロセッサ「IBM Quantum Hummingbird」を、2021 年に 127 量子ビットのプロセッサ「IBM Eagle」をリリースした。それらを用いれば、従来のコンピュータでは量子回路を正確かつ確実にシミュレートできないという問題を改善することができる。2022 年には、「Eagle」よりも性能が 10 倍向上した 433 量子ビットのプロセッサ「IBM Osprey」が誕生し、現在のスパコンでも解決不可能な問題を処理することが可能となった。続く 2023 年には 1,121 量子ビットの量子コンピューティングプロセッサ「Condor」が発表されたほか、2025 年に 4,000 量子ビット以上のプロセッサを開発することも計画されている。量子ビット数の継続的な増大のほか、コンピューティング能力に影響を与えうる要

素として、業界では現在、量子の誤り訂正および誤り耐性の向上にも重点を置いている。IBM はこのほか、モジュール化システム「Quantum System 2」を提示しているが、これは複数の量子プロセッサを緊密に接続して、量子コンピューティングが発揮する潜在能力の規模を大きくするものであり、2023 年末の IBM 量子サミットでは、このシステムを基礎とした、現時点で最高の性能、最低のエラー率を誇る量子プロセッサ「Heron」が発表された。

一方、中国大陸では、産学官や研究機関の能力を統合しての開発が進められている。例えば、アリババグループは 2023 年 11 月に傘下の研究機関の量子コンピューティング実験室および関連設備を浙江大学に寄贈し、続いて百度グループも 2024 年 1 月に傘下の実験室および設備を政府の支援する研究機関に寄贈した。量子コンピュータの主要研究開発機関である中国科学技術大学では、2020 年に 76 光子の光量子計算プロトタイプ機「九章」が完成し、続いて 2021 年には 113 光子の「九章二号」が開発された。2023 年には 255 光子の光量子計算プロトタイプ機「九章三号」が完成している。

台湾中央研究院は、2023 年 10 月に量子チップを開発し、2024 年 1 月 29 日には初の自社開発 5 ビット超伝導フルシステム量子コンピュータの完成を発表した。それを利用して量子コンピュータエコシステムの開発プラットフォームを確立し、汎用的な量子コンピュータハードウェア技術、光量子技術、量子ソフトウェア技術およびアプリケーション開発、周辺の主要コンポーネントなどに焦点を当てることで、将来的には、高性能コンピュータとの緊密な連携による、全体的なコンピューティング性能の向上を目指していく。

量子テクノロジーの推進には学際的な統合が必要であり、関連する知識分野は物理、化学、数学、情報工学、電気機械など多岐にわたる。台湾量子電脳協会の理事長である張慶瑞教授は 2023 年のインタビューにおいて、量子テクノロジーの発展が今後段階的に進んでいくと指摘した。計算能力の向上および安定性の面で飛躍的な成長を遂げる「量子ブレイクスルー」段階から、現在のスパコンで解決することが困難な特定の複雑な問題の処理において全面的な優位性を得ることができる「量子アドバンテージ」段階を経て、さらに現在のネットワークエコシステムと同様に、あらゆる分野、あらゆる業界、あらゆる学問の基礎的環境となる「量子エコシステム」段階へと発展する、というのである。張教授は、今後 5～6 年で「量子ブレイクスルー」の課題が部分的に解決し、かつ課題の内容も研究面から工学面へと徐々に移行して、実用化に近づいていくと予測している。オーストラリアのニュー・サウス・ウェールズ大学（UNSW）が世界初の量子工学部を設置して以来、ヨーロッパ、中国大陸、米国でも高等教育機関において続々と関連の学部が開設され、量子エンジニアが積極的に育成されている。さらに、米国では、次世代が量子エコシステムの環境にシームレスに移行できるよう、量子テクノロジーの動作原理を常識教育として幼児教育に組み込む取組もすでに始まっている。

量子コンピュータは特定の演算において非常に速い速度を誇るが、現時点ではまだ限界があり、従来のコンピュータに代替するのではなく、それと相互補完する形で使用されている。量子状態の高度な不安定性により、現在開

発されている量子コンピュータはいずれも絶対零度（-273℃）環境下での動作が必須であるので、現時点ではクラウド上での特定演算の実行にしか対応することができず、初期段階では医薬品、気象、材料、金融、人工知能などの研究および分析への利用が見込まれている。

2.ポスト量子暗号の発展の現況

量子コンピュータの現時点での発展状況からすると、短期的には既存の暗号システムへの影響は大きくないが、本当の問題はそこではない。例えば暗号化アルゴリズム「SHA-1」は、2005 年に効果的な攻撃方法が発見されてからも使用され続け、2017 年になってようやく各大手企業が続々と使用停止するに至った。米国国立標準技術研究所（NIST）は 2022 年に、2030 年以降は SHA-1 の使用を停止すると発表している。指数関数的に成長する量子技術および各国間のサイバー軍拡競争の中で、量子によってもたらされる衝撃に耐えうる暗号化技術をどのようにしてタイムリーに制定、標準化かつ導入するかこそ、全世界が力を合わせて取り組まなければならない課題である。

NIST は 2016 年にポスト量子暗号（Post-Quantum Cryptography、PQC）の標準化プロセスを開始し、量子コンピューティング時代到来時の汎用的な暗号化アルゴリズムとして、現在の主流な暗号化アルゴリズムに代替し、量子コンピューティングによって解読される可能性が最も低いアルゴリズムを見つけ出すべく、世界中からアルゴリズムを公募した。2020 年 7 月には、公開鍵暗号と鍵カプセル化メカニズム（PKE/KEMs）およびデジタル署名の 2 分野において、7 つの第 3 ラウンド候補アルゴリズムを発表した。

量子コンピュータによる暗号解読の威脅への対処には、大きく分けて 2 つの方法がある。暗号学に基づくポスト量子暗号（PQC）と、量子技術に基づく量子鍵配送（Quantum Key Distribution、QKD）である。米国国家安全保障局（NSA）は、QKD について、理論的には解読不可能で絶対に安全であるが、現時点では、専用設備が必要であること、インフラコストおよび内部威脅リスクが必然的に増大することなどの技術的限界があるため、QKD の使用を推奨しないという見解を発表している。一方、PQC については、PQC 標準化コンペティションの第 3 ラウンドに進出した候補 7 チームと補欠 8 チームによる計 15 種のアルゴリズムのうち、7 種が格子アルゴリズムである。格子アルゴリズムは現行の RSA および楕円曲線暗号システムとは異なり、量子コンピュータの得意とする課題ではない上、生成される公開鍵、秘密鍵、暗号文、デジタル署名などの長さが現行暗号システムの 10 倍程度にすぎないため、主要な研究対象となっている。

3 ラウンド、6 年間にわたる選抜を経て、NIST は 2022 年 7 月 5 日に第 1 期分として入選した 4 種のアルゴリズムを発表した。公開鍵暗号と鍵カプセル化メカニズムに用いられるアルゴリズム「CRYSTALS-Kyber」、およびデジタル署名に用いられる 3 種のアルゴリズム「CRYSTALS-Dilithium」、「FALCON」、「SPHINCS+」である。同時に NIST は、公開鍵暗号と鍵カプセル化メカニズム分野で第 4 ラウンドに進出した候補アルゴリズムリストをも発表し、第 2 期に入選したアルゴリズムを 2024 年にリリースし、正式に標準

を公開すると決定した。NIST の説明によると、実用的なニーズに応えられるよう、単一のアルゴリズムを使用してセキュリティホールを発見されることを回避してセキュリティを確保するために、あらゆる使用シナリオに対して 2 つ以上のアルゴリズムを提供できるようにならなければならない、ということである。

直近で大規模な暗号化アルゴリズムの変更があったのは 2000 年頃であるが、各大手企業でのアルゴリズム「AES」の導入に 10 年近くを要したため、NIST はすべての組織に対し、まもなくリリースされる新アルゴリズムの導入準備を前倒しで開始することも呼びかけている。そのための 6 つの推奨手順として、組織内で公開鍵暗号が使用されているシステムの把握、新たな暗号標準のテスト、新たな暗号標準への転換計画の制定、新たな調達方針の確立、内部の IT 部門とサプライヤによる対応準備の推進、従業員研修の実施、が挙げられており、これらを通じて関連するビジネスチャンスも自然と生まれてくる、とされている。

3.関連するスタートアップの発展の方向性

コンサルティング会社であるマッキンゼー・アンド・カンパニー社による 2022 年時点での報告によれば、量子コンピューティング分野に参入するスタートアップ企業が最も多い国は米国、英国、カナダである。近年、多くの量子コンピュータスタートアップがベンチャーキャピタルや政府から投資を受けており、例えば英国の量子テクノロジースタートアップ Quantum Motion 社は 2023 年に行った直近の資金調達で、英国政府およびベンチャーキャピタル企業から合計 4,200 万英ポンドの投資を獲得している。それに加えてこれまでに累計で約 2,400 万米ドルを調達しており、その合計調達額は約 22.7 億台湾ドルに上る。同社はそれらを利用して、量子プロセッサの開発を加速させていく。同年にはこのほか、フランスのスタートアップ Pasqal 社が 1 億ユーロを、イスラエルのスタートアップ Quantum Machines 社がシリーズ B で 700 億米ドルを、オーストラリアのスタートアップ Quantum Brilliance 社が 1,800 万米ドルを調達するなどしている。また、大手テクノロジー企業も社内で積極的にスタートアップを育成しており、例えば Google の親会社 Alphabet 社は、2022 年に量子コンピューティング業務を独立させてスタートアップ Sandbox AQ 社とした。同社は 2023 年に 5 億米ドルを調達している。以上の状況から、ベンチャーキャピタル市場における量子テクノロジー分野の盛り上がりが見て取れる。

ベンチャー投資家による多額の投資は、量子テクノロジーの商業化の足取りを好意的に捉えていることの表れである。例えば、2022 年に設立されたフランスの量子テクノロジースタートアップ Quobly 社は、2030 年までに世界初の百万量子ビットの量子コンピュータを開発することを目指しているが、創業者である Maud Vinet 氏は、AI モデルの基礎であるニューラルネットワークの演算を量子ビットで行えば、理論的には大幅な節電を実現できる、と指摘している。アドバンスト・マイクロ・デバイセズの CEO である蘇姿丰氏は、「生成 AI によってコンピューティングの需要は急速に増大しており、10 年後には 1 台のスパコンによるコンピューティングで原子力発電所 1 基分の

電力を消費する可能性がある。このことからも量子コンピューティングに潜在するビジネスチャンスが膨大であることが分かる」と評している。

台湾は、量子コンピュータの発展においては先進国に多少とも水をあけられているが、PQC および QKD の研究ではすでに一定の成果を収めている。どのようにして先進国の歩みに遅れず付いていくかは、課題であると同時にチャンスでもある。国外ではすでにこの技術が銀行業に応用されている事例もあるので、この技術に関連する商業化ソリューション市場も、台湾の情報セキュリティスタートアップが掴むべきビジネスチャンスであるといえる。PQC の決勝に選出されたチームには、台湾から計 4 名の専門家や学者が参加しているが、彼らはすでに 20 年以上にわたってこの分野に深く関わっている上、国外の最高峰の専門家とも長期的な協力関係にあり、今後先進国の後を追うために有望な人材である。

TAcc+プログラムが指導する台湾のスタートアップチームの中にも、PQC 分野に参入する情報セキュリティスタートアップの池安量子資安（Chelpis）社がある。同社は量子暗号をコアに、ゼロトラストアーキテクチャを基盤に据えて、企業レベルの Edge-to-Cloud 情報セキュリティソリューションおよび製品の提供、IT/OT インフラおよびアプリケーションの保護および強化を行っており、認証を受けた同社開発のチップは、IoT のエンドポイントセキュリティに応用することが可能である。また、エンドツーエンドの量子セキュリティテクノロジー、クラウドとエンドポイントのデータ送信セキュリティ、ポスト量子暗号技術、ならびにゼロ知識証明などのソリューションも発表している。

現在の QKD 技術の最大のボトルネックは、既存の基本アーキテクチャにいかにして高速かつ効果的に光子を割り当てるかであるが、関連分野に参入する者たちは、その打開に懸命に取り組んでいる。例えば、カナダのスタートアップ企業 Quantropi 社は、世界で初めてクラウドプラットフォームおよびネットワークを通じて QKD 技術を実現し、かつそのモデルが既存の QKD システムより 10 万倍も高速であることを証明した。同社の共同創業者兼 CEO である James Nguyen 氏は、「当社のソフトウェアプラットフォーム『QiSpace™』の本質は 100%のアルゴリズムであり、線形代数で表現される量子力学に基づいている。光子がないということは、光子の速度や距離の制限がないことを意味する」と述べている。台湾の科学技術部は 2018 年から、量子技術を優先補助項目の 1 つとしており、2019 年には 25 キロメートルの屋内光ファイバー量子暗号通信および 4 キロメートルの屋外光ファイバー量子暗号通信の実験に成功した。関連する情報セキュリティスタートアップは、技術の発展および関連の商業化ソリューションによるビジネスチャンスに目を向けるべきである。

間もなくやって来る量子時代に備えるため、台湾政府も積極的に関連する人材を育成しており、「汎用的な量子コンピュータハードウェア技術」、「光量子技術」、「量子ソフトウェア技術およびアプリケーション開発」という 3 大分野に焦点を当て、省庁を超えた産学官の研究チームを結成して、台湾の量子テクノロジー産業チェーンの構築のための、リソース投入と指導とを行っ

ている。中央研究院の廖俊智院長は、「量子テクノロジーの敷居は高いものの、台湾としては、開発の初期段階で先進国に肩を並べ、集中化、提携および統合などといった方法を通じて、量子テクノロジーの発展過程で直面する技術的なボトルネックや重要なポイントを実際に理解し、それらの部分で台湾の産業が果たせる役割をできるだけ早く認識して、量子テクノロジーのサプライチェーンの重要な参加者となることが必要である」と述べている。

出典：

- "量子電腦為何比傳統電腦強大？量子運算的發展又有哪些挑戰呢？" 泛科學, 2018.
- "【臺灣資安大會直擊】為對抗量子電腦攻擊手法，後量子加密 PQC 演算法有望變成未來全球加密與數位簽章新標準," iThome, 2020.
- "資安關鍵字：網路加密技術｜量子加密通訊】抵抗量子電腦問世的威脅，以光子傳送密碼或金鑰," iThome, 2020.
- "從 4 大關鍵問題搞懂 PQC 與密碼學競賽," iThome, 2020.
- "是否有密碼之盾能夠擋住量子電腦之矛？後量子密碼學的前世今生——匯智安全科技陳君明董事長專訪," 泛科學, 2021.
- "量子電腦問世後的密碼學主力戰場「後量子加密技術」," 科技大觀園, 2021.
- "Google、IBM 都來競爭！英國實驗室突破量子電腦新成就，將比超級電腦更厲害？" 數位時代, 2022.
- "量子國家隊成軍，17 項團隊底定，聚焦未來量子世代臺灣產業鏈," iThome, 2022.
- "首批 NIST 認可的 PQC 演算法出爐，美 CISA 建議即刻做好六大準備," iThome, 2022.
- "量子運算能夠協助未來 AI 系統的安全性，讓 AI 演算法運用在更多方面," iKnow 科技產業資訊室, 2023.
- "IBM 聲稱量子電腦大突破，且進入實用階段，兩年後有機會打敗傳統超級電腦," iKnow 科技產業資訊室, 2023.
- "IBM 推出新量子運算晶片和處理器　探索科學新領域," 科技島, 2023.
- "Google 展示量子霸權：僅幾秒完成的任務最強超級電腦要花 47 年," 鉅亨網, 2023.
- "臺灣資安產業開始推動 PQC 遷徙，池安成立量子安全遷移中心," iThome, 2023.
- "中研院研發 5 位元量子電腦 年底推出／台灣首次自製量子晶片 將放到雲端提供學術研究單位試用," 自由時報, 2023.

- "矽谷科學家：量子電腦有望實現通用人工智慧," 中央通訊社, 2023.
- "重要趨勢！量子跟你想的不一樣！量子電腦將掀起超級運算大革命！將如何引領科技發展？ft.台灣量子電腦協會理事長 張慶瑞教授！" 曲博科技教室, 2023.
- "新一代 IBM 量子處理器「蒼鷺」Heron 與 IBM Quantum System Two 亮相," IBM, 2023.
- "「量子日」最快明年降臨？量子運算恐顛覆全球軍經安全," 聯合新聞網, 2024.
- "Quantropi 使用現有網絡基礎設施展示量子熵的量子安全分布," 頭條匯, 2024.
- "台灣自製超導量子電腦 成少數完成研發國家," 中央通訊社, 2024.
- "連台積都只看 5 年內技術　一家法國量子新創，給台灣電子業的警示," 天下雜誌, 2024.