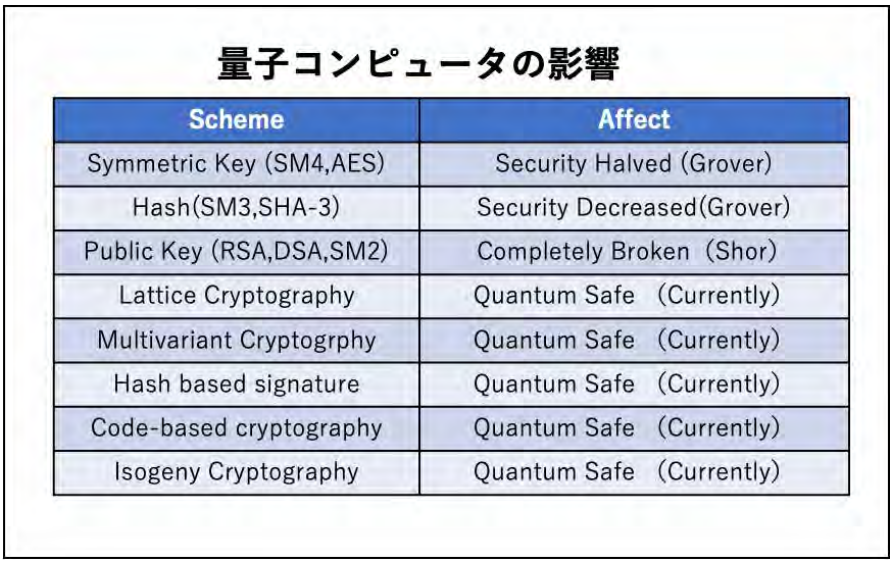

図 5-7　中国の講演資料２

しかし、量子コンピュータが実用になると共通鍵（対象鍵）暗号（SM4、AES 等）の安全性は半減し、ハッシュ暗号（SM3、SHA-3）の安全性は低下する。また、公開鍵（非対称鍵）暗号（RSA、DSA、SM2 等）は、完全に破られる。一方、Lattice、Multivariant、Hash based signature、Code-based、Isogeny は、現時点では耐量子コンピュータの安全性を保てると考えている。

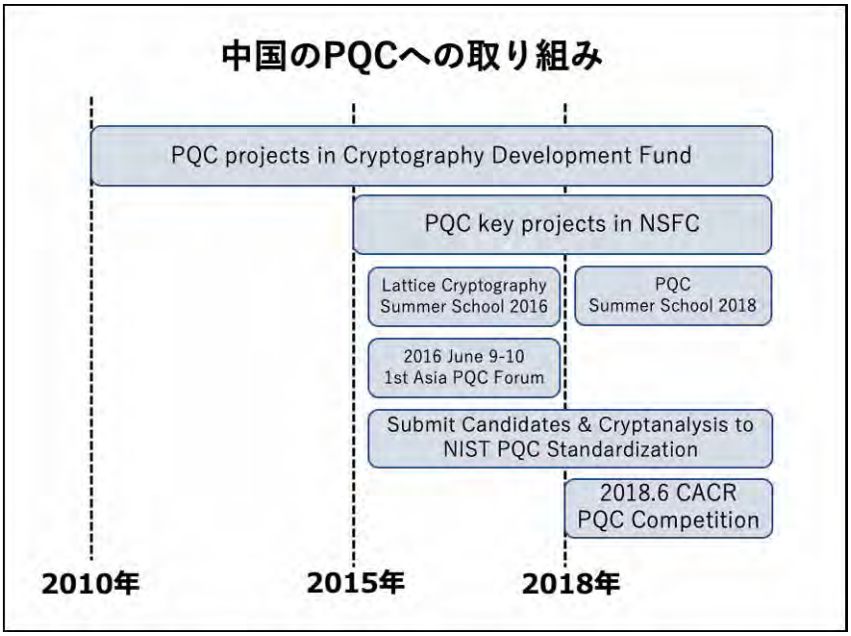

図 5-8　中国の講演資料３

CACR（中国暗号研究協会）では、2018 年 6 月に PQC 公募を開始している。

図 5-9　中国の講演資料４

また、中国は、NIST の標準化の公募に対しても上図のような候補で提案している。

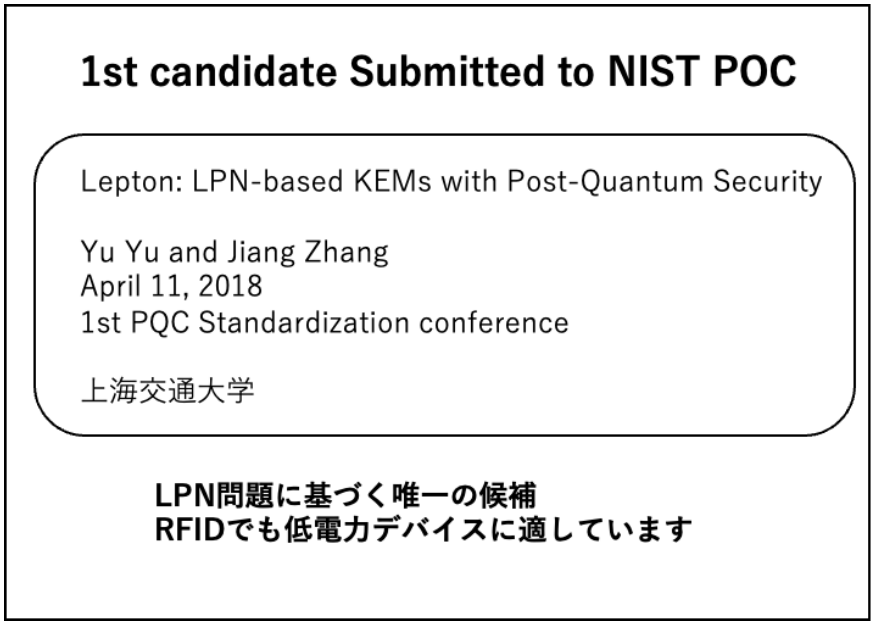

図 5-10　中国の講演資料５

NIST PQC に提案された最初の候補は、LPN 問題に基づく唯一の候補であり、RFID でも低電力デバイスに適することができる。

図 5-11　中国の講演資料６

また、国際標準化委員会である ISO/IEC SC27 WG2 SD8 の PQC プロジェクトに参加している。

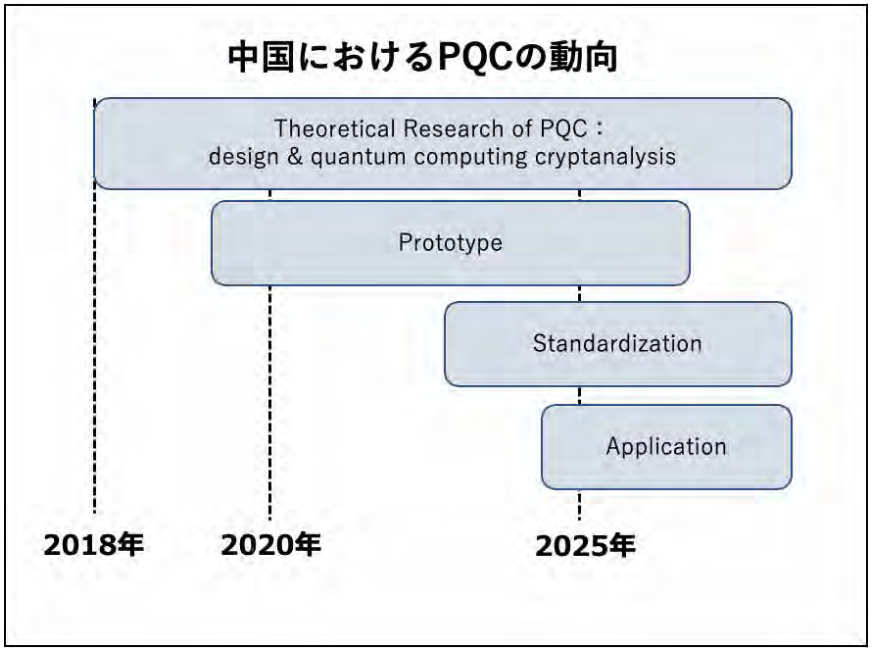

図 5-12　中国の講演資料７

一方、中国国内に向けた PQC 開発の取り組みは、2018 年より PQC の理論研究として設計と量子コンピューティングの暗号解読の研究を始めており、2023 年ごろまでに標準化、2025 年前に商用移行としている。上記のように、量子コンピュータを利用した暗号解読の研究も同時に進められており、中国では、量子技術に対して莫大な投資を行っていることを考えると、量子コンピュータを利用した暗号の解読における脅威は大きいと考えられる。

https://docbox.etsi.org/Workshop/2018/201811_ETSI_IQC_QUANTUMSAFE/EXECUTIVETRACK/JING_CHINESEACCADEMYOFSCIENCE.pdf

Research of Post-Quantum Cryptography in China　Jiwu Jing （Data Assurance and Communications Security Research Center　Chinese Academy of Science）

【ロシアの PQC 開発状況】

ロシアも PQC の国家標準を策定している。モスクワ通信情報技術大学(MTUCI) 量子センタ　Konstantin Panko　ポスト量子暗号部門責任者によると、「現在、既に量子コンピュータ耐性のある次世代の情報セキュリティシステムを構築する完全に独創的な暗号ソリューションを持っている」と発言している。彼らのチームは、現在の国際的な慣行と独自の科学的成果の研究に基づいて、情報セキュリティの 2 つの基本的な問題を解決するため、新しい国家標準の草案を準備していると強調した。「共有鍵を生成するための時代遅れの Diffie-Hellman アルゴリズムと GOST 34.10-2018 電子署名標準の代わりに、初めて代数幾何学暗号に基づく Classic McEliece タイプのシステムを提案した。そのパラメータは計算能力に応じて変更でき、また、保護されたシステムと必要な情報セキュリティの程度によって変更することができる。これは、世界の慣行と比較して優位性がり、先行していると考えている。新しい標準は、国内の情報インフラのデジタルデータプラットフォームで使用される。」と発言している。

https://digitnews.in/russia-develops-national-standards-for-post-quantum-cryptography/

第６節 PQC と量子暗号（QKD）

現在、各国における暗号通信の耐量子コンピュータの対策における考え方は、以下の通りである。

① 米国（NSA：National Security Agency） 2020/10/26

NSA は、QKD に対して以下の問題点を指摘し懸念を抱いており、QKD の下記の課題が解決されない限り、セキュリティシステムでの使用の推奨や認定はしない方針である。

A) 送信者と受信者の間の初期認証がない
QKD は、送受信者間の初期認証手段を持たないので双方の安全を保証するために非対称暗号（RSA 等は既に危険なので、PQC 等と考える）か、または事前配置された鍵で認証が必要になる。
→以下の各国ともに PQC だけで十分であり、QKD は、現時点で必要ないと考えている。

B) 量子鍵配送は専用の機器が必要であり、現在の通信に適さない通信速度と距離の限界である。
QKD は物理特性に基づいており、ユーザーは専用のファイバ接続や自由空間での送信機を物理的に管

理する必要があるため、既存のネットワーク機器に簡単に統合することができない。また、通信速度や距離の限界が現在の通信環境に適さない（通信速度は遅く、伝送距離は短い）。

C)　堅牢な中継施設（trusted node） が必要のため新たな多額の投資が必要
QKD ネットワークでは､信頼できる中継設備が必要であり､新たに大規模な設備コストが必要であり、また内部脅威への安全対策も必要になるためユースケースに制限がある。

D)　現在実現可能なシステムは、現代技術で限定的なため、無条件安全の理論には達していない
実用的な QKD システムの実際の安全性は、物理法則の理論的な無条件安全性ではなく、実装と工学設計で達成する限定的な安全性である。暗号化の安全性誤差の許容度は非常に小さく検証が困難であり、QKD の実装は脆弱性をもつ可能性が考えられる（市販の QKD 装置を使った実験的な盗聴事例も報告されている）。

E)　セキュリティ確保のため通信を停止しているため、「通信の可用性」を維持できない
QKD の安全性の根拠は、盗聴者検知でのサービス停止（通信停止）であり、これ自体が QKD の重大な脅威となる。（通信の可用性が侵される脅威）

これらの QKD の課題は、以下の他国も同様に考えており、実用化においては、その対策が急務である。
https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

② 英国（NCSC：National Cyber Security Centre 英国国家安全保障局）2020/3/24
NCSC は、従来の暗号の鍵配送に対し、QKD の特殊なハードウェア要件と全てのユースケースで認証の要件を考えると、政府または軍事アプリケーションでの QKD の使用は推奨しない方針である。NSA の指摘と同様に、QKD プロトコルは、初期認証を考慮していないため、物理的な中間者攻撃に対して脆弱である。この攻撃方法は、盗聴者が送信者と受信者間の間に入り、送信者―盗聴者、盗聴者―受信者のそれぞれで偽の鍵を共有させる。送信者と受信者は互いの通信を疑う術はないので、通信する相手を信じて通信を開始する。盗聴者は、成りすましによる盗聴行為が可能になる。この成りすましを回避するためには、QKD の実行前に送受信者間での確実な認証が必須である。
→米国と同様に NCSC が推奨する量子コンピュータの脅威に対する最善の緩和策は、PQC であるとしている。
https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

③ フランス（ANSSI：Agence nationale de la sécurité des systèmes d ‘information） 2020/5/4
QKD は、現在および将来の脅威に対する必須のソリューションではないとしている。理論的には数学的攻撃に対しては安全だが、実際のハードウェアを理論通りに実装することは不可能であり、安全を達成することはできないと指摘しおり、攻撃者により QKD デバイスが異常な動作をする可能性がある(なりすましなど)と言及している。
QKD は、現在の実装によるサービスを展開する上で、技術的に大きな制約がある。また、QKD を共通鍵暗号（既存の数理暗号：AES 等）の鍵配送に使用方式は、情報理論的安全ではない（数理暗号の計算量的安全性）。情報理論的安全なのは OTP（One Time Pad）を実現したときだけであり、暗号伝送速度は QKD の鍵配

送速度で律速されるため非常に遅く、伝送距離も短く適用できるアプリケーションは非常に限定的になる。長距離化のための縦列接続（中継）型の QKD による通信では、中継施設の条件によりシステムの安全性保証が損なわれ、膨大な投資が必要になる（各国と同様の指摘）。

④ ドイツ（BSI：Bundesamt für Sicherheit in der Informationstechnik）

ドイツにおいては、BSI（連邦 IT セキュリティ局）が QKD 利用におけるガイドラインを出しており、他国のように切り捨てるのではなく、QKD の不完全さ、脆弱性を理解した上での利用について正しく詳細に説明し、その可能性とリスクについて言及している。

https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-MeldungenNews/Meldungen/Leitfaden_quantensichere_Kryptografie_211216.html

⑤ オーストラリア（Australian Army）

オーストラリア陸軍においては、2021 年 9 月に「Army Quantum Technology Roadmap」の中で、「量子通信と暗号」のセクションの中で「オーストラリア陸軍にとって量子鍵配送（QKD）の価値を認めていない。これは、QKD 自体が十分に安全である可能性が低いからであり、更に、より簡単に統合できる PQC が出現したためである。」としている。また「利用の可能性ある QKD 対応ネットワークとしては、技術的な制約とその脆弱性により、少数のリンクに限定されるだろうと結論付けている。

https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf

第７節　QRC と量子暗号（QNSC）

表 5-5 は、ISO（International Organization for Standardization：国際標準化機構）の OSI（Open Systems Interconnection）参照モデル（現在のネットワークをその機能ごとに階層化しまとめたもの）の各ネットワーク階層に対応した脅威やセキュリティ技術を纏めたものである。ここからわかるように、各層ごとに様々なセキュリティ技術が構築されているが、物理層においては、本質的に伝送路等のインフラアクセスに対する盗聴を想定したセキュリティ技術はない。現在の情報通信においては、物理層を直接守ることはできず、上位のレイヤかもしくは、伝送直前で、データに暗号化（数学的複雑性で計算量的安全を根拠とする現代暗号）をした暗号データを流すだけである。

表 5-5 国際標準化機構（ISO）の OSI 参照モデルにおける各階層のセキュリティ技術の考え方

階層	層名	定義	プロトコル例	セキュリティの脅威	ソリューション
L1	アプリケーション層	アプリケーション、サービス	HTTP、FTP、電子メール	Static Password, SNMP Private Community Strings	Anti Virus software, OS Hardening, Patching
L2	プレゼンテーション層	データの表現形式	文字コード、圧縮	Viruses, Worm	Intrusion Detection, Auditing
L3	セッション層	接続制御と管理	TLS	Personal Information Retrieval, Root Privilege Access, Net Bios, DOS	Patches, Encryption, Authentication
L4	トランスポート層	データ通信の制御	TCP/IP、UDP	Endpoint Identity	Firewall access control list
L5	ネットワーク層	アドレス管理とルーティング	IPv4、IPv6	Preventing unauthorised access to internal system	VPN network based intrusion detection and content filtering
L6	データリンク層	通信区間のデータ送受信	Ethernet、Wi-Fi	ARP spoof, MAC Flooding	Private VLANs, Static ARP (address resolution protocol) entries, STP (Spanning Tree Protocol) root priority
L7	物理層	電気尊号、無線信号	有線ケーブル、無線	Inadequate Power, Unfettered access, Open wall ports	Managed Power through UPS, Restricted Access, Close down open wall ports

出展：International Journal of Electrical Electronics & Computer Science Engineering Special Issue - TeLMISR 2015, ISSN : 2348-2273