量子計算機でも破れない耐量子セキュリティ技術

Cryptographic Technologies for Protection of Networks with Security Vulnerability against Cryptanalytic Attacks with Advent of Quantum Computers

秋山　浩一郎 AKIYAMA Koichiro　　谷澤　佳道 TANIZAWA Yoshimichi

量子計算機の出現により，これまで情報セキュリティを支えてきた暗号技術の危殆（きたい）化が始まっている。そこで，量子計算機でも破れない暗号技術（耐量子セキュリティ技術）への置き換え（耐量子化）に向けた準備が，世界的に進められている。

東芝グループは，この社会的課題に対し，高度な機密性を保ってデータを送信でき，高速性・安定性・相互運用性などを備えた量子鍵配送（QKD）装置を用いた暗号通信技術，及びローエンドデバイスにも搭載でき，公開鍵長が短く軽量な耐量子計算機暗号（PQC）技術を開発した。これらの技術を駆使することで，セキュアネットワークの実現を目指している。

Conventional cryptographic technologies supporting information security have begun to be compromised in recent years with the advent of quantum computers. Efforts toward the development of new cryptographic technologies are therefore being actively promoted in Japan and other countries.

As a solution to this social issue, the Toshiba Group has developed the following two cryptographic technologies as measures against cryptanalytic attacks with the advent of quantum computers: a cryptographic communication technology using quantum key distribution (QKD) equipment, which enables the transmission of highly confidential data while also offering high-speed performance, stability, and interoperability; and a lightweight post-quantum cryptography (PQC) technology with a small public key, which can be implemented even in low-end devices. We are aiming to realize highly secure networks by making full use of these technologies.

1. まえがき

1994年に米国の理論計算機科学者ピーター・ショアが，量子計算機を使うことで，素因数分解問題と離散対数問題が効率的に解けることを示したことにより，量子計算機による暗号技術の危殆化が始まっている。公開鍵暗号として広く利用され，ネットワークの安全を支えているRSA暗号（注1）と楕円（だえん）曲線暗号の安全性が，これらの問題の計算困難性に基づいているからである。

2022年1月現在，量子計算機はまだ研究開発段階で，暗号を解読できるほど長いビット長の計算はできないため，直ちにネットワークの安全性が損なわれるわけではない。しかし，2030年代半ば以降には現行方式の暗号を破る量子計算機が出現するとの見方もあり[1]，社会を長年支えているインフラシステムなどから順次，量子計算機でも破れない暗号への置き換え（耐量子化）が必要となっている。

実際，量子計算機開発の活発な動きに呼応するように，米国国家安全保障局（NSA）は2015年8月に現行の公開鍵暗号のPQCへの移行を発表した。更に，2017年12月には米国国立標準技術研究所（NIST）によってPQCの標準化が開始され，標準方式の選定が行われるなど，耐量子化に向けた動きが加速している。

PQCと独立に開発され，耐量子化を支える技術に量子暗号通信がある。量子暗号通信の基盤となる技術は，1984年に二人の物理学者によって発表された量子鍵配送（QKD）のプロトコルでBB84と呼ばれる[2]。以降，プロトコル・理論・実装に関する研究開発が進み，量子計算機を含むあらゆる解読・盗聴が不可能な暗号通信技術であり，同時に，実用性の高い量子技術として注目されている。近年，欧州，米国，中国，日本でもそのネットワーク実証が行われており[3]，ETSI（欧州電気通信標準化機構），ITU-T（国際電気通信連合-電気通信標準化部門），ISO/IEC JTC1（国際標準化機構／国際電気標準会議 第一合同技術委員会）といった，国際標準化団体における標準化を巡る議論も活発である。このような状況の中，東芝と東芝デジタルソリューションズ（株）は2020年に量子暗号通信システム事業の開始を発表した[4]。2021年には当社を含む民間企業11社で“量子技術による新産業創出協議会”を発足[5]し，量子暗号通信を含む量子技術の産業化を加速・リードしている。

（注1） 暗号化と復号に異なる鍵を使う暗号方式の一つ。

ここでは，量子暗号通信とPQCを耐量子セキュリティ技術と呼び，耐量子セキュリティ技術を駆使して実現する，量子計算機出現以後のセキュアネットワークの姿を描くとともに，それに向けた当社の取り組みについて述べる。

2. 量子計算機の脅威とその対策技術

インターネット上のサイトで初めてショッピングをする際は，そのサイトからクレジットカード番号などの信用情報が要求される。信用情報は重要な個人情報であり，ユーザーは特段に意識しないが，通常は他人から見られないように公開鍵暗号で暗号化して送信されている。公開鍵暗号は，このようにあらかじめ鍵を共有していない相手でも暗号通信ができ，デジタル署名を用いることで送信相手の認証も可能となるといった優れた特性を持っている。一方で，一旦送信相手と鍵の共有ができれば，暗号化や復号に掛かる時間は共通鍵暗号の方がはるかに高速である。このため，情報の暗号化は共通鍵暗号で行い，そこで利用する共有鍵を公開鍵暗号で暗号化して送信するといった，ハイブリッドな利用方法が主流となっている。

2.1 量子計算機が引き起こす脅威

量子計算機は，現行の公開鍵暗号（RSA暗号と楕円曲線暗号）の安全性の基盤となっている問題を効率的に解くことによって，その安全性を脅かす。また，同様に量子計算機によって，公開鍵暗号と同じ計算困難な問題に基づくデジタル署名（RSA署名やECDSA（Elliptic Curve Digital Signature Algorithm）など）の安全性も脅かされる。デジタル署名の安全性が損なわれるとデジタル署名の偽造が可能となるため，認証局が発行する公開鍵証明書はその効力が失われ，データの改ざんや他者への成り済ましが可能となる。

共通鍵暗号も量子計算機を用いた暗号解析の影響を受けるが，鍵長を2倍にすれば耐量子性を実現できることが知られている。この節では，量子計算機出現以降も安全な通信を実現する耐量子セキュリティ技術について，具体的な技術を示す。

2.2 量子暗号通信

QKDは，量子性を持つ“光子”の位相・偏光に暗号鍵の情報を書き込んで送信することで，通信路上で起こり得る盗聴（観測）を光子の量子状態変化として物理的に検知し，盗聴されていないことが確かめられた情報に基づいて暗号鍵を共有する。量子暗号通信は，QKDにより共有した暗号鍵を共通鍵として利用した暗号通信を指す。物理的な性質を安全性の根拠としているため，従来の公開鍵暗号とは異なり，理論上，無条件に安全な通信が実現でき，現時点で最も安全性の高い通信手段といえる。

QKD技術は，光子の送受信に基づく技術であることから，利用できる距離・通信形態に制約があるが，安全な中継拠点（トラステッドノード）を設けてネットワークを構築することで，広域でも利用可能なプラットフォームが構築可能となる。光子の送受信を行うQKD装置，光ファイバー通信網，トラステッドノード，といった大規模・高価なインフラが必要となることから，例えば，医療・ゲノムや，金融，政府機関などの分野における，特に高い機密性を必要とするユースケースから利用され始めることが想定される。ただし，量子暗号通信自体はデジタル署名・本人認証などの認証機能を持たないため，次に述べるPQCなどを利用した認証基盤との組み合わせが必要となる。

2.3 PQC

PQCは，量子計算機でも計算困難な計算問題に基づく公開鍵暗号である。多くの研究者が長い年月を掛けても効率的な解法を見いだせなかった計算困難な問題を安全性の根拠とすることで，実用上は十分な安全性が主張できることや，現行の暗号方式と同様に従来の計算機や通信環境で処理やデータ通信が可能であり，システムを大きく変更することなく現行の暗号方式から移行ができることなどから，PQCは幅広いシステムの耐量子化に用いられると期待されている。

PQCのうち有力な方式は絞られてきている。例えば，格子の最短（最近）ベクトル問題に基づく暗号は格子暗号，線形符号の復号問題に基づく暗号は符号暗号とそれぞれ呼ばれ，NIST標準最終候補にもなっている。特に，格子暗号は，同じ問題からデジタル署名が構成でき，量子計算機時代の認証機能を実現する技術としても期待されている。

その一方で，これらの暗号は総じて，現行の公開鍵暗号よりも安全性を担保するために必要な公開鍵サイズが大きくなる。このため，メモリー容量に限界がある組み込みマイコンなどのローエンド機器に実装する際には，公開鍵がメモリーに格納できず，計算の都度外部から読み込むことで著しいオーバーヘッドが生じる可能性が指摘されている。また，狭帯域ネットワークにおいては公開鍵が1パケットに収まらず，複数パケットに分割されるため，パケットロスの影響が大きくなるという問題が生じる。

3. 量子計算機出現以降のセキュアネットワーク

2章で述べた量子暗号通信とPQCの特性をまとめると，**表1**のようになる。

これを踏まえると，量子計算機出現以降の量子セキュアネットワークは，量子暗号通信とPQCのそれぞれの特長を

表1. 量子暗号通信とPQCの特性比較

Comparison of characteristics of QKD and PQC

項　目	量子暗号通信	PQC
秘匿性	無条件安全	計算量的安全
認証	なし	あり
通信距離	制約あり	制約なし
通信装置	専用装置が必要	現行のネットワーク機器で可能

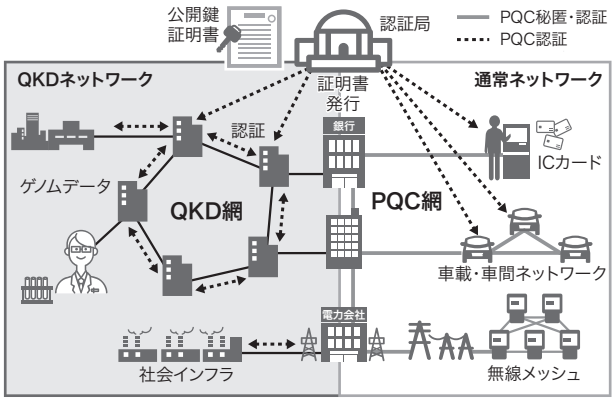


図1. 量子計算機出現以降の量子セキュアネットワークの概要

量子計算機でも破れないセキュアネットワークとしては，量子暗号通信とPQCのそれぞれの特長を生かして安全性を実現するハイブリッド構成が考えられる。

Overview of secure network after advent of quantum computers capable of breaking current public-key cryptosystems

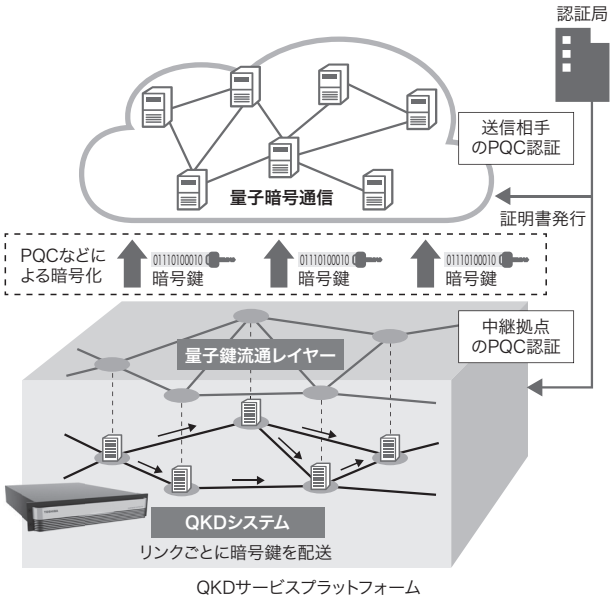


図2. QKDサービスプラットフォームの概要

QKDシステムと量子鍵流通レイヤーとを組み合わせ，暗号鍵配送サービスを実現するプラットフォームとして整備することで，多様な分野でのユースケースへと広がっていくことが想定される。

Overview of QKD service platform

生かしたハイブリッド構成が望ましい（**図1**）。コストを掛けても確実に機密性を保持したいデータ（ゲノム情報などの機微な個人データ，社会インフラデータなど）を取り扱う専用網やネットワークインフラなどでは，無条件安全の特性を生かした量子暗号通信が利用される（図1左側の“QKD網”）。一方，個人の決済情報や移動情報など，コストを掛けずに機密性を守りたい情報が流通する通常のネットワークにおいては，PQCの利用が想定される（図1右側の“PQC網”）。特に，現時点ではモバイル機器やIoT（Internet of Things）機器などへの量子暗号通信技術の実装は困難であり，このような機器ではPQCが利用される。また，車載用組み込み機器などのローエンド機器への導入には，より軽量化されたPQCが望まれている。

図1中のQKD網部分は，実際には，**図2**に示すようなQKDサービスプラットフォームとして実装される。QKDサービスを実現するプラットフォームとして整備され，多様な分野でのユースケースへと広がっていくことが想定される。ここで，QKDサービスプラットフォームにおいても，耐量子性を考慮し，認証においてはPQCを用いることが考えられる。例えば，暗号鍵の配送先が正しい受信者であることの確認や，暗号鍵を中継する拠点が信頼できるノード（トラステッドノード）であることの確認には，認証局が発行する公開鍵証明書をベースとする認証基盤が必要であり，PQC認証の利用が想定される。また，共有した暗号鍵をアプリケーションユーザーに受け渡すための通信インターフェースの認証・暗号化にも，PQC若しくは耐量子性を持つ共通鍵暗号が用いられると考えられる。

4. 東芝グループの量子暗号通信技術

ここでは，当社の持つ量子暗号通信技術とその特長について述べる。量子暗号通信をバックボーンネットワークとして使う場合，大量のトラフィックを扱う高速性，インフラとしての高い安定性，そして既存ネットワークへの組み込みの容易さが求められる。以下で，東芝グループの量子暗号通信技術の特長である，高速性，安定性，通信インフラ親和性，及び相互運用性について述べる。

(1) 高速性　　QKDにおいて，単位時間当たりに生成できる暗号鍵の量（鍵配信速度）は，量子暗号通信で利用できる暗号鍵の量を決定する最も重要な指針である。当社は，光子検出時に発生するバックグラウンドノイズを除去する自己差分型回路技術を開発し，1 GHzクロック駆動時においても高精度で安定な光子検出を

行うことを可能とした。また，光子検出処理後の鍵蒸留処理アルゴリズム（処理負荷の高い大規模行列演算などから成る）を高速で実行する並列計算アルゴリズムを考案・実装した。これらの光子制御技術と高速信号処理技術の融合により，10 Mビット/sを超える世界最速の鍵配信速度を達成している[6]。

⑵　安定性　　敷設光ファイバーの振動や温度変化などの外乱によって生じる，光子の位相や偏光の変化の影響を，フィードバック制御によって抑制し，外乱の影響を極小化して安定動作する技術を確立・実証した[7]。

⑶　通信インフラ親和性　　QKDのための光子通信を，通常のデータ通信と同一の光ファイバーに光波長多重化する技術を確立した[8]。これにより，QKD光子通信のための専用光ファイバー敷設が不要となり，導入コストの低減や既設ファイバー回線の利用，既存ネットワークインフラとの統合も可能となる。

⑷　相互運用性　　QKDによって生成した暗号鍵を，統一的なインターフェースで利用できるように，暗号鍵提供のためのAPI（Application Programming Interface）を開発した。このAPIを利用することで，QKDシステムのプロトコル・実装の詳細や差異を意識することなく，QKDのアプリケーション開発を容易に行うことが可能となる。API仕様はETSIにおいて標準化され[9]，複数の実証で用いられ始めている。

上記以外にも例えば，長距離化や小型化に向けた研究開発も進めており，それぞれ，Twin-field QKDプロトコルと複数波長を用いた安定化技術による600 kmを超える通信距離の実証[10]，QKDの主要機能を光集積回路化した開発チップを用いて小型化した量子暗号通信システムの実証[11]，などの成果を挙げている。

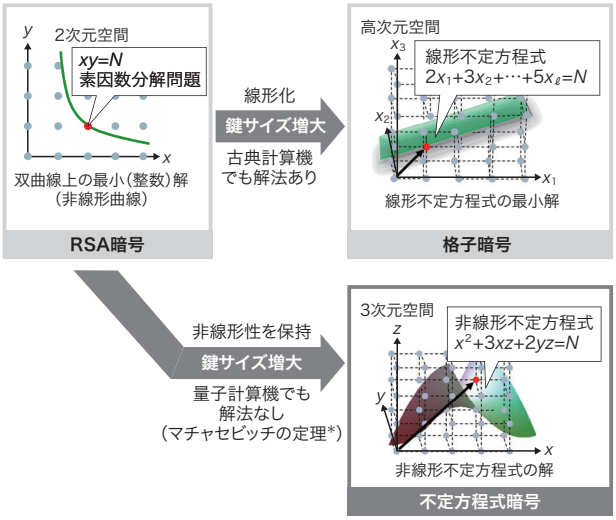
5. 東芝グループのPQC技術

ここでは，当社の持つPQC技術の狙いと特長について述べる。まず，ローエンド機器への実装が懸念される原因となっている従来技術のPQCにおける公開鍵サイズが現行方式より大きいという特性上の理由について，PQCの中で最も有力視されている格子暗号を例に説明し，当社の取り組む軽量なPQCである不定方程式暗号の有効性について述べる。

RSA暗号が安全性の根拠とする素因数分解問題は，Nを大きな合成数とするときに$xy=N$という方程式の整数解を求める問題と解釈できる（**図3**）。このような，変数の数が制約（式）の数よりも多い不定方程式は，解の自由度が大きく，整数解，原点に最も近い解（最小解）などといったような特別な制約条件がなければ解を見いだすことは容易である。実際，不定方程式$xy=N$において実数解を認めれば，双曲線上の点は全て解となるが，整数解を求めるという制約を課すと，素因数分解問題となり計算困難となる。一般に，整数係数の非線形不定方程式から整数解を見いだす問題（ディオファントス問題）は，汎用的な解法アルゴリズムが存在しない非可解問題であることが証明されている。

一方，PQCの中で有力視されている格子暗号は，格子という離散的な線形空間上で原点に一番近い点を求める問題（最小ベクトル問題）を安全性の根拠としている。格子暗号の場合，この線形空間は線形不定方程式$\boldsymbol{A}\cdot\boldsymbol{s}+\boldsymbol{e}=\boldsymbol{b}$の解空間である。ここで，$\boldsymbol{A}$は$n\times n$行列，$\boldsymbol{s}$，$\boldsymbol{e}$，$\boldsymbol{b}$は$n$次元ベクトルで，$\boldsymbol{A}$と$\boldsymbol{b}$は既知，$\boldsymbol{s}$と$\boldsymbol{e}$は未知である。したがって，この方程式は変数の数が$2n$で，式の数が$n$となり，不定方程式となる。この解空間は$n$次元で，解の中で最も原点に近い解を見付ける問題は計算困難な問題となる（最小ベクトル問題）。しかし，これは線形方程式であるため，線形代数に基づく有力な解法が利用できる。この問題の計算をより困難にするには問題自体のサイズを大きくして次元数nを上げなければならず，これが公開鍵サイズの増大をもたらしている。

これに対して当社が研究開発を行っている不定方程式暗号は，非線形不定方程式の求解問題をベースとする公開鍵暗号である。その非可解問題としての計算困難性から，安



ℓ：高次元空間の次元数
＊非線形な不定方程式には一般的な解法が存在しないことを証明した定理

図3．不定方程式暗号の特長と狙い

非線形不定方程式の求解問題をベースにしており，その非可解問題としての計算困難性から，安全性の高い公開鍵暗号を構成でき，公開鍵サイズの削減が可能となる。

Features and objectives of indeterminate equation cryptosystem

全性の高い公開鍵暗号を構成することができ，このことが公開鍵サイズの削減につながる。求セクション問題と呼ばれる非線形不定方程式の求解問題に基づいた方式は，公開鍵サイズがRSA暗号の約50％以下となっており[12]，ローエンドデバイスへの実装に道を開く可能性を持つ。

6. あとがき

セキュリティにおける量子計算機の脅威が迫ってきている。これに対抗できる耐量子セキュリティ技術の導入は，社会インフラや機密保持年数の長いデータを扱うシステムなどから順次社会的な要請となってゆく。当社は，高度な機密性を持つデータを安全・確実に伝送できるネットワークを整備するとともに，ローエンド機器まで含めてトータルにセキュリティを担保するための技術開発を進め，これらの要請にタイムリーに応えていく。

謝　辞

この研究の一部は，内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「光・量子を活用したSociety 5.0 実現化技術」（管理法人：国立研究開発法人 量子科学技術研究開発機構（QST））によって実施されたものである。また，この研究の一部は，総務省「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の援助の下に行われている。ここに謝意を表します。

文　献

(1) Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready?. IEEE Security & Privacy. 2018, **16**, 5, p.38–41.
(2) Bennet, C. H.; Brassard, G. "Quantum Cryptography: Public Key Distribution and Coin Tossing". Proceedings of IEEE International Conference on Computers Systems and Signal Processing. Bangalore, India, 1984-12, IEEE. 1984, p.175–179.
(3) Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD Network. Optics Express. 2011, **19**, 11, p.10387–10409.
(4) 東芝. “量子暗号通信システム事業を開始”. ニュース&トピックス. <https://www.global.toshiba/jp/news/corporate/2020/10/pr1901.html>, (参照 2022-02-04).
(5) 東芝. “「量子技術による新産業創出協議会（Q-STAR）」の設立について～産業界が主体となり「量子産業の創出」を目指す～”. ニュース&トピックス. <https://www.global.toshiba/jp/news/corporate/2021/09/news-20210901-01.html>, (参照 2022-02-04).
(6) Yuan, Z. et al. 10-Mb/s Quantum Key Distribution. Journal of Lightwave Technology. 2018, **36**, 16, p.3427–3433.
(7) Dynes, J. F. et al. Stability of high bit rate quantum key distribution on installed fiber. Optics Express. 2012, **20**, 15, p.16339–16347.
(8) Dynes, J. F. et al. Ultra-high bandwidth quantum secured data transmission. Scientific Reports. 2016, **6**, 35149.
(9) ETSI GS QKD 014:2019. Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.
(10) Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilization. Nature Photonics. 2021, **15**, p.530–535.
(11) Paraïso, T.K. et al., A photonic integrated quantum secure communication system. Nature Photonics. 2021, **15**, p.850–856.
(12) 秋山浩一郎，ほか. “近似イデアルGCD問題に基づく不定方程式暗号”. 2021年 暗号と情報セキュリティシンポジウム．オンライン開催，2021-01，電子情報通信学会 情報セキュリティ研究専門委員会．2021，3A4-1.

秋山　浩一郎　AKIYAMA Koichiro, Ph.D.
研究開発センター サイバーセキュリティ技術センター
博士（工学）
電子情報通信学会会員・応用数理学会会員
Cyber Security Technology Center

谷澤　佳道　TANIZAWA Yoshimichi
研究開発センター 情報通信プラットフォーム研究所
コンピュータ&ネットワークシステムラボラトリー
Computer and Network Systems Lab.