White Paper

PQCへの早期移行に向けた ハイブリッド暗号方式の実装

2025/04

ソフトバンク株式会社
先端技術研究所

SoftBank

SANDBOXAQ™

ソフトバンクとSandboxAQのPQC移行に向けた取り組み

実用的な量子コンピューターの登場はサイバーセキュリティーに大きな変革をもたらす可能性があります。現在、広く使用されているRSA暗号や楕円曲線暗号（ECC：Elliptic Curve Cryptography）などの暗号化技術は、量子コンピューターに対して脆弱であることが指摘されており、第三者による通信の傍受やなりすましが懸念されています。

これに対して、政府機関や金融機関など、機密情報を扱う組織は、量子コンピューターでも解読が困難な耐量子計算機暗号（PQC：Post Quantum Cryptography）への移行準備を進めています。

ソフトバンクは、SandboxAQと協力して2021年にPQCに関する検討を開始しました。それ以降、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）によるPQCアルゴリズムの標準化動向を注視するとともに、PQCへの移行に向けた活動を実施してきました。

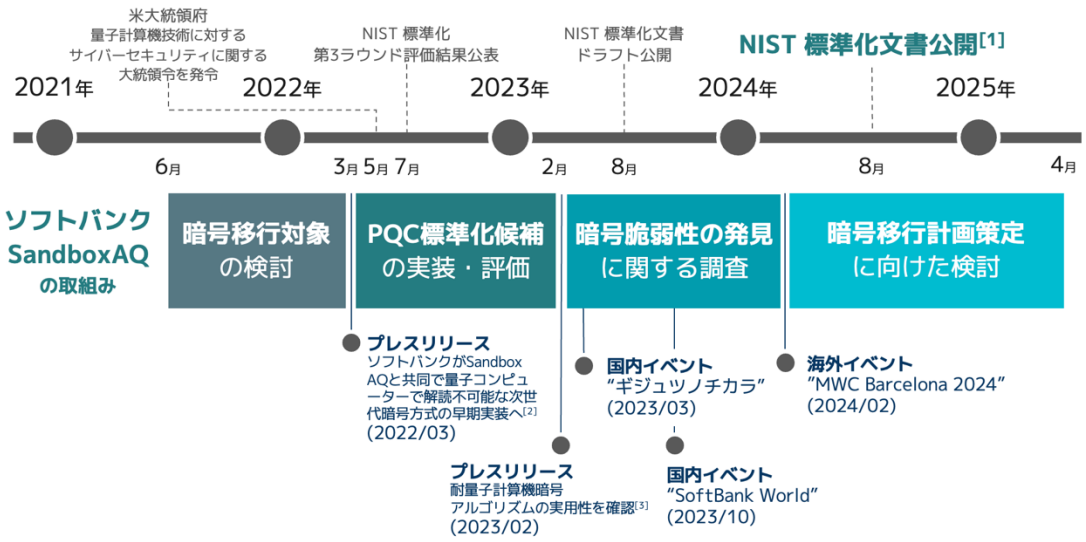

図1：PQC移行に向けたソフトバンクの取り組み

2022年にソフトバンクとSandboxAQは、量子コンピューターによるStore Now Decrypt Later攻撃（SNDL攻撃）からデータを保護するために、既存の暗号アルゴリズムと新たなPQCアルゴリズムを組み合わせるハイブリッド暗号方式の実証実験を行いました。この実験を通じて、移行に伴う技術的課題とその解決策が明らかになりました。

本ホワイトペーパーでは、ハイブリッド暗号方式の必要性と実証実験について解説します。

© SandboxAQ, SoftBank Corp.

量子コンピューターの脅威

量子コンピューターは、重ね合わせや量子もつれなどの量子力学の原理を活用して、従来のコンピューターとは桁違いの速度で複雑な計算を処理します。特に、従来のコンピューターでは解くのが難しいとされる、素因数分解問題や離散対数問題といった数学的問題を効率的に解くことができます。量子コンピューターはまだ開発段階ですが、世界中で研究が進められて急速に発展しており、その驚異的な計算能力は、今日のサイバーセキュリティーにとって深刻な脅威となる可能性も秘めています。

現在、RSA やECCなどの公開鍵暗号方式は、銀行取引や医療記録から国家安全保障上の通信に至るまで、あらゆるものを保護しています。 公開鍵暗号方式は、暗号化と復号に異なる鍵を用いる暗号方式で、非対称暗号とも呼ばれます。公開鍵暗号方式では、送信者が公開鍵を用いてデータを暗号化し、受信者は秘匿された秘密鍵を用いてデータを復号します。この時、第三の攻撃者は公開鍵を知ることはできますが、秘密鍵の情報を持っていないため、暗号化されたデータを解読することはできません。公開鍵暗号方式は、暗号化通信の鍵交換やなりすましを防ぐデジタル署名に用いられています。従来の公開鍵暗号方式では、巨大な数の素因数分解や離散対数問題といった数学的問題を用いて安全性を保証してきました。

しかし、量子コンピューターは、Shorのアルゴリズムとして知られる強力なアルゴリズムを使用して、これらの数学的問題を簡単に解読することができます。Shorのアルゴリズムでは、量子コンピューターが0と1の重ね合わせ状態であるキュービットを使うことで、従来のコンピューターでは指数関数的な計算量が必要であった素因数分解などの問題を効率的に解読することができます。これにより、量子コンピューターでは従来の暗号アルゴリズムに基づく公開鍵の情報から秘密鍵を効率的に計算することができます。

量子コンピューターの実現はまだ先のことと考えられることが多いですが、政府や企業は現在でもその脅威にさらされています。現時点で量子コンピューターへの耐性がない暗号化通信を傍受し、量子コンピューターが実用化されたタイミングで解読し悪用するような攻撃が想定されます。このような攻撃はStore Now Decrypt Later攻撃（SNDL攻撃）やHarvesting攻撃と呼ばれています。このリスクは、データを保護するためには量子コンピューターで解読できない暗号化に早急に移行する必要があることを示唆しています。

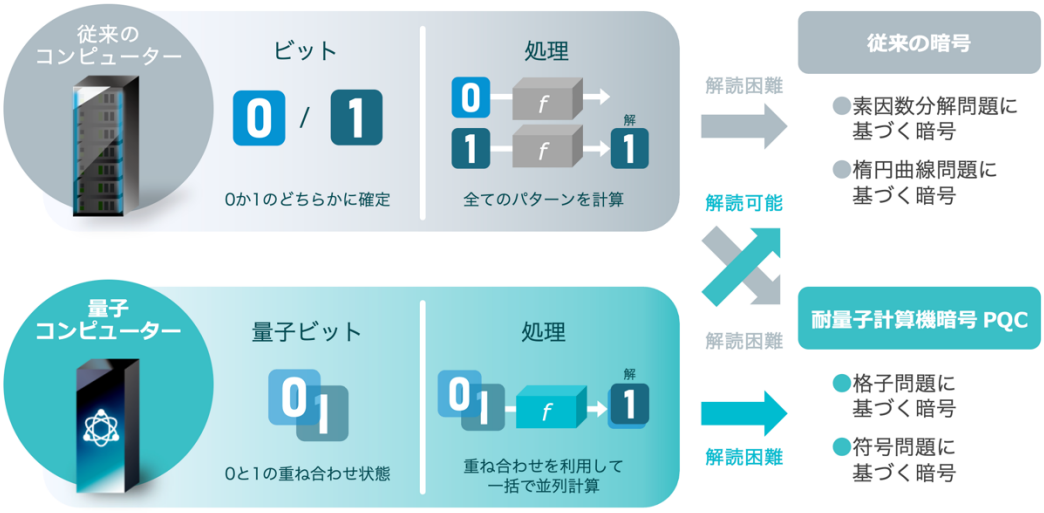

図2：従来のコンピューターと量子コンピューターの違い

© SandboxAQ, SoftBank Corp.

耐量子計算機暗号（PQC）

耐量子計算機暗号（PQC）とは、量子コンピューターの脅威に耐えるように設計された暗号化技術を指します。

RSA や ECC とは異なり、PQCのアルゴリズムは、量子コンピューターによっても解読することが困難な数学的問題に基づいています。根本的に異なる数学的問題に依存しているため、Shorのようなアルゴリズムを使用する量子コンピューターは、PQC で保護されたデータを簡単に解読することができません。

PQCアルゴリズムには複数のアプローチがあります。それぞれのアプローチはベースとなる数学的問題で分類されます。以下では数学的問題による分類をそれぞれ説明します。

構造化格子に基づく暗号

構造化格子暗号方式は、構造化された格子（多次元空間内の点の幾何学的な配置）から導出される数学的問題を採用しています。構造化格子方式は、優れた効率性とバランスの取れたセキュリティを有しています。実用上優れた性能を発揮することが評価され、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）により2024年8月にこの問題に依拠するアルゴリズムの標準化が行われました。後述するML-KEMやML-DSAなどのアルゴリズムがこのカテゴリーに分類されます。

非構造化格子に基づく暗号

非構造化格子暗号方式は、構造化を伴わない格子から導出される数学的問題を採用しています。非構造化格子暗号方式は、より強力なセキュリティを提供する可能性がありますが、大きな鍵サイズと増加した計算リソースを必要とするため、多くの場合、構造化格子暗号よりも広範な展開には適していません。

同種写像に基づく暗号

同種写像暗号方式は、2つの同種の楕円曲線の間の写像から導出される数学的問題を採用しています。 同種写像暗号方式は、鍵サイズが小さいため、当初は有望なアルゴリズムとして期待されていました。しかし、最近の脆弱性の発見と暗号化時の高い計算要求により、セキュリティとパフォーマンスに関する懸念が生じており、2025年4月時点ではNISTによる選定候補から外れています。

符号に基づく暗号

符号暗号方式は、符号問題と呼ばれる数学的問題に基づいています。符号暗号方式は量子コンピューターによる攻撃に対して高い耐性を持っていますが、より大きな鍵サイズを必要とするため、ストレージやデータ転送の効率に影響を与える可能性があります。構造化格子に基づく暗号方式のバックアップとして標準化アルゴリズムへの採用が決まっています。

© SandboxAQ, SoftBank Corp.

特徴	構造化格子暗号	非構造化格子暗号	同種写像暗号	符号暗号
セキュリティー強度	高い 徹底的な分析で信頼されている	非常に高い 理論的な強度が高い	不確実 近年脆弱性が発見された	高い 高い耐性が証明されている
性能（速度）	速い 暗号化・復号を高速に処理できる	比較的遅い 計算資源を多く要する	遅い 計算負荷が大きい	中程度 計算オーバーヘッドが許容範囲内である
鍵サイズ	中程度 管理可能で広範囲に実用化できる	大きい 広範囲の実用化には課題もある	小さい PQCアルゴリズム内では実証上最小	非常に大きい 大規模な鍵管理を必要とする
リソース要件	中程度 今日の端末で適切に動作する	高い 高性能な処理能力が必要である	高い 特定のハードウェア要件がある	適度〜高い 今日の端末で適切に動作する
成熟度	成熟 NISTによってテスト・標準化された	比較的未熟 複雑で採用が限定的	未熟 近年脆弱性が発見された	中程度 長年研究されるも鍵サイズの大きさから採用は少ない

表1：PQCアルゴリズムの特徴

© SandboxAQ, SoftBank Corp.

NISTによるPQCアルゴリズム標準化

NIST は 2024 年に正式な PQC 標準を策定しました。標準化されたアルゴリズムには、1 つの鍵交換アルゴリズム（FIPS203）と2つのデジタル署名アルゴリズム（FIPS204、 FIPS 205）が含まれています。

鍵交換アルゴリズム

FIPS 203 : ML-KEM（Module-Lattice-Based Key-Encapsulation Mechanism）

- ML-KEMは、従来のRSAやECCとは異なり、構造化格子に基づく暗号アルゴリズムであり、量子コンピューターでも解決するのが難しい暗号方式です。具体的には、格子内の最短ベクトル問題を利用して安全性を確保します。効率的なキーの生成と暗号化が可能になり、比較的低い遅延とオーバーヘッドで高いセキュリティーを提供します。

デジタル署名アルゴリズム

FIPS 204 : ML-DSA（Module-Lattice-Based Digital Signature Algorithm）

- ML-DSA は、構造化格子に基づくデジタル署名アルゴリズムです。 ML-DSA は署名の生成と検証の速度が速く、特にセキュリティーとパフォーマンスのバランスに優れています。

FIPS 205 : SLH-DSA（Stateless Hash-Based Digital Signature Algorithm）

- SLH-DSAは、ハッシュ関数を利用したデジタル署名方式で、安全性の高さが特徴です。ただし、計算量と署名サイズが大きいため、通信帯域幅とストレージの負荷が増加します。

また、NISTは、量子コンピューターが最終的に格子ベースのアルゴリズムを解読できるようになった場合に備えて、バックアップとして機能する追加のアルゴリズムを選定してきました。

鍵交換アルゴリズム（候補）

HQC

- HQCは、ML-KEMとは違い、符号問題に基づく暗号方式です。この数学的アプローチの多様性により、ML-KEMの潜在的な脆弱性に対する代替手段として期待されています。HQCは2025年3月に追加の鍵交換アルゴリズムとして選定されました。

デジタル署名アルゴリズム（候補）

FN-DSA（FFT over NTRU-Lattice-Based Digital Signature Algorithm)

- Falconとして知られるFN-DSAは、高速フーリエ変換（FFT）を利用して効率的でコンパクトなデジタル署名を実現します。FN-DSAは、2024年中の標準化文書公開が予定されていましたが、2025年4月時点ではまだ公開されていません。

2025年4月時点で、NISTは上記2つのアルゴリズムの実装ガイドラインと詳細な技術文書のドラフトを作成中です。これらの文書がリリースされた際には、新しい標準に基づいてシステムを更新することをお勧めします。

従来暗号とPQCによるハイブリッド暗号方式

PQCへの移行における課題

現在、構造化格子に基づく暗号化が実用的なソリューションとして有力ですが、PQCへの移行は複雑で困難なプロセスであり、慎重な計画が必要です。PQCへの移行を検討する際には、量子セキュリティを確保するために暗号インフラを移行させる際に発生する課題に対応する必要があります。

技術的および運用上の課題は次のとおりです。

- 多くの組織のレガシーシステムは、RSAやECCなどの従来の暗号化アルゴリズムと統合されています。
- PQCを導入するためには、新しい暗号化方式が現在利用しているソフトウェアやハードウェア上で動作することを確認するための広範なテストが必要です。
- 暗号化標準のアップグレードには、移行中のデータ漏洩や運用の稼働停止を防ぐために、サイバーセキュリティー、IT、コンプライアンスチーム間の慎重な調整が必要です。
- PQCは、標準化されて日が浅いため潜在的な脆弱性が発見されるリスクがあります。移行後に発見された場合には、再度移行プロセスにリソースを割くことになります。

これらの課題への対処の遅れは重大なリスクを生じます。量子コンピューターの脅威が差し迫ったものになるまで実装を遅らせるとデータの侵害にさらされる可能性があります。

現在暗号化されている機密データは、将来のSNDL攻撃により脆弱になる可能性があります。さらに、政府機関や標準化団体がPQCアルゴリズムの採用に向けて迅速に動いており、規制上の圧力も急速に高まると想定されます。

© SandboxAQ, SoftBank Corp.

ハイブリッド暗号方式

既存の暗号アルゴリズムから新しい　PQCアルゴリズムへの移行は簡単ではないため、移行には組織は段階的なアプローチをとる必要があります。

現実的な方法として、従来の暗号アルゴリズムとPQCアルゴリズムをシームレスに融合させるハイブリッド暗号方式の利用が推奨されます。この方式は、従来のコンピューターに対してすでに導入されているアルゴリズムと、将来の量子コンピューターに耐性のあるPQCアルゴリズムを併用することで、安全性と互換性を高めるアプローチです。

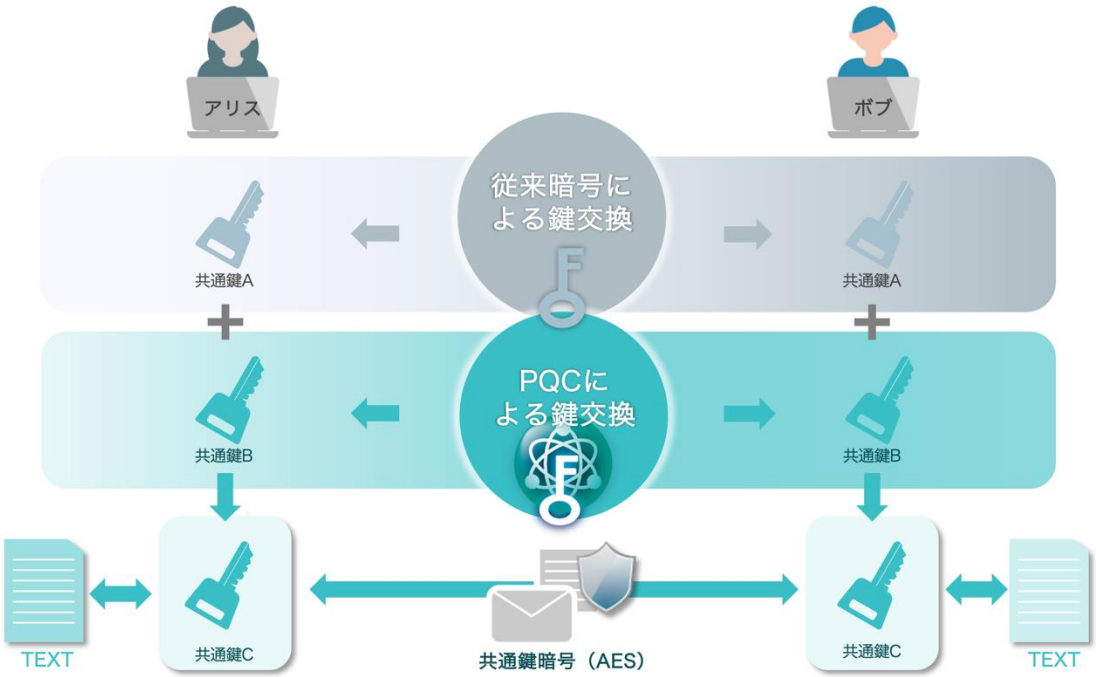

図3：ハイブリッド鍵交換方式

図3は、従来暗号とPQCの両方を組み込んだハイブリッド鍵交換方式を使用して、アリスとボブの 2 者間で安全なデータ通信を確立するプロセスを示しています。

1. 従来暗号による鍵交換：最初に、アリスとボブは、従来暗号方式（ECC）を使用して共通鍵Aを生成します。

2. PQC鍵交換：同時に、アリスとボブはPQC鍵交換を行い、それぞれのPQC鍵ペアを利用して、量子コンピューターによる攻撃に耐性のある安全な共通鍵Bを生成します。

3. 共通鍵暗号鍵の生成：両者はECCにより交換された共通鍵AとPQCにより交換された共通鍵Bを利用して、最終的な共通鍵Cを導出します。

4. 安全なメッセージ交換：共通鍵Cを使用して、アリスはメッセージを暗号化してボブに送信します。ボブはメッセージを復号して安全に読むことができます。

© SandboxAQ, SoftBank Corp.

この方法はハイブリッドアプローチを簡略化して説明したものであり、実際の処理とは異なる場合があることに注意してください。ハイブリッド暗号方式の実装は、2025年4月時点でInternet Engineering Task Force (IETF) による標準化ドラフトで検討されています。

ハイブリッド暗号方式の主な利点は次のとおりです。

- 即時性：機密データを量子対応攻撃から即座に保護することが可能です。
- 互換性：既存のインフラストラクチャを統合することで中断を最小限に抑え、コストのかかるダウンタイムを防ぎます。
- 安全性：PQCの潜在的な脆弱性が発見された際に、従来暗号によりデータを保護することができます。

ソフトバンクとSandboxAQによる広範な実環境検証により、ハイブリッド暗号方式がユーザーエクスペリエンス、パフォーマンス、またはネットワークの遅延に悪影響を与えることなく、堅牢なセキュリティーを提供することが確認されています。

特徴	ハイブリッド暗号方式	PQC単独暗号方式
量子攻撃への耐性	☑ 即時性のある量子安全性	☑ 即時性のある量子安全性
統合複雑性	☑ 既存インフラに容易に統合可能	ⓘ インフラを大きく変更する必要あり
レガシーシステムとの互換性	☑ 現在の標準と互換性あり	ⓘ 互換性が低く大きな更新の可能性あり
移行時の運用リスク	☑ 段階的な導入が混乱を軽減	ⓘ 急な全体の見直しによる混乱のリスク
規制上のコンプライアンス	☑ 容易にFIPS等の要件を満たす	☑ 将来的な量子関連標準を満たす
コスト・リソースへの影響	☑ 既存の投資の範囲内で可能	ⓘ 多大な新規のリソースを要する
実装までの時間	☑ 段階的で短期間の導入が可能	ⓘ 広範なテストと展開が必要

表2：ハイブリッド方式の利点

© SandboxAQ, SoftBank Corp.

ソフトバンクと SandboxAQによるハイブリッド暗号方式の検証

ソフトバンクは2022年にSandboxAQ と提携して、実際のユーザーシナリオでハイブリッド暗号方式を検証しました。

この検証では、PQCアルゴリズムが通信パフォーマンスに影響を与えずに、信頼性の高い実用的なセキュリティーを提供できることを確認することを目的としています。

検証の構成

本検証環境は、1組のLinuxサーバー、Cisco WiFi-6アクセスポイント、および数台のAndroid端末で構成されました。トラフィックはAndroid端末で生成され、各種測定をLinuxサーバ上で行いました。本検証では、通信環境で広く使用されている次のようなネットワークを介して性能の検証を行っています。

- 5G接続
- LTE 接続
- SmartVPNを経由した接続
- WiFi接続

また、本検証では、オンラインゲーム、高解像度ビデオストリーミング、標準的なWebブラウジング、VPN接続といったシナリオを想定したトラフィックを流し検証を行っています。このアプローチにより、ユーザーが利用する実ネットワークトラフィックを想定した暗号化方式の評価が可能になりました。

図4：検証に用いたネットワークシナリオ

© SandboxAQ, SoftBank Corp.

この調査では、各シナリオで重要な指標を測定しました。

- **遅延**：暗号化により目立った遅延が生じないこと
- **接続速度**：接続が安定しており、信頼性が高いこと
- **パフォーマンス**: CPU 使用率への影響が最小限であること

実証実験で使用されたアルゴリズムを次の表に示します。検証を行った2022年の時点でNISTによる標準化プロセスの第3ラウンドで評価中のアルゴリズムを選定しています。

鍵交換

- 従来の暗号方式（Elliptic curve Diffie–Hellman key exchange; ECDH）
- 構造化格子に基づく暗号方式（ML-KEM、NTRU、Saber）
- 非構造格子に基づく暗号方式（FrodoKEM）
- 符号に基づく暗号方式（BIKE、HQC）
- 同種写像に基づく暗号方式（SIKE）

デジタル署名

- 従来の署名方式（ECDSA）
- 格子に基づく署名方式（ML-DSA、FN-DSA）

主要な調査結果と考察

ソフトバンクとSandboxAQが実施した実証実験では、ハイブリッド暗号方式の実用性を裏付ける結果が得られています。

構造化格子に基づくPQCアルゴリズム、特にML-KEMおよびML-DSAが与える端末のパフォーマンスへの影響は小さいことがわかりました。ハイブリッド暗号方式を用いた場合でも、遅延、CPU使用率、同時コネクション数などの指標が従来の暗号方式（ECC）と近い結果を得ることができました。

ただし、すべてのPQCアルゴリズムで同等の結果が得られたわけではありません。同種写像に基づく暗号化は、鍵サイズが小さいため当初は有望であると考えられていましたが、パフォーマンスが大幅に低下しました。

これらの結果は、2024年8月のNIST標準化アルゴリズムの結果を反映していると言えます。

遅延

PQCのベースとなるアルゴリズムごとにグループ化された全体の遅延を対数スケールで比較しました。図5に示すように、従来暗号（ECDH）が最も高速で、次に構造化格子暗号（ML-KEMなど）が続きます。

非構造化格子暗号（FrodoKEM）はそれほどパフォーマンスは良くありませんが、それでも同種写像暗号（SIKE）よりも大幅に優れています。符号暗号（HQCなど）は全体に分散されていますが、そのピーク遅延は非構造化格子暗号や同種写像暗号と同様です。結果は理論値とほぼ一致しており、構造化格子暗号が全体的に最高のパフォーマンスを発揮することを示しています。

同種写像暗号の計算時間は実際は、構造化格子よりも長いことがわかっています。図6の遅延には、鍵交換部分だけでなく、デジタル証明書を使用するTLSハンドシェイクの他の部分も含まれるため、鍵交換部の視覚的な違いが小さくなります。

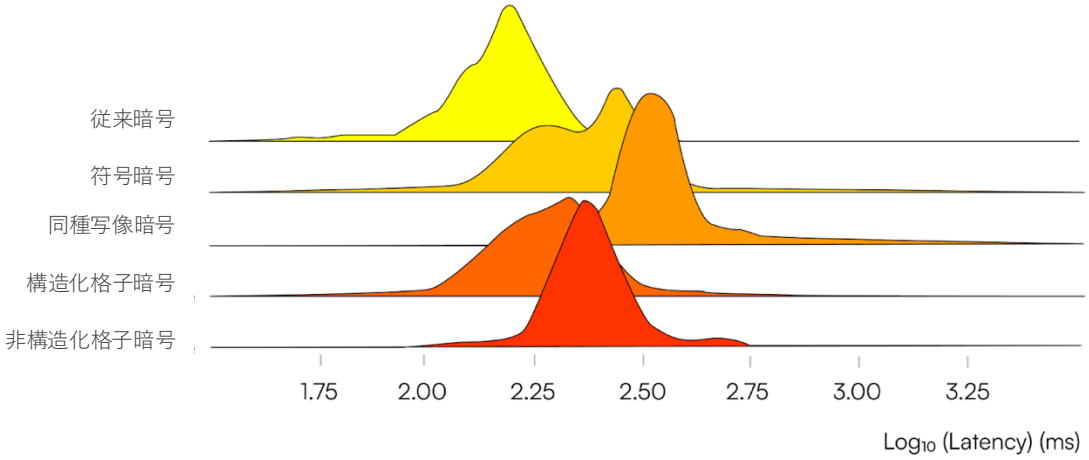

図5：WiFi接続におけるTLSハンドシェイクの遅延（ミリ秒）。
結果を視覚的に理解しやすくするために分布は対数スケールで図示。

© SandboxAQ, SoftBank Corp.

同時接続数

また、同時接続の許容数に対する鍵交換アルゴリズムの影響も比較しました。図6に示されているように、PQCアルゴリズムを使用したハイブリッド暗号方式により、従来暗号（ECC）と比較して同時接続数が減少しました。その中で、構造化格子暗号（ML-KEMなど）は最小限の劣化を示しました。対照的に、同種写像暗号（SIKE）では、同時接続に関して大幅なパフォーマンスの低下が見られました。

符号暗号（HQCなど）は、パフォーマンスは多少低下しますが、同種写像暗号および非構造化格子暗号（FrodoKEM）と比較して、優れたコネクション数を示します。この結果は、現在PQCの標準と考えられている構造化格子暗号の代替手段としての可能性を示唆しています。

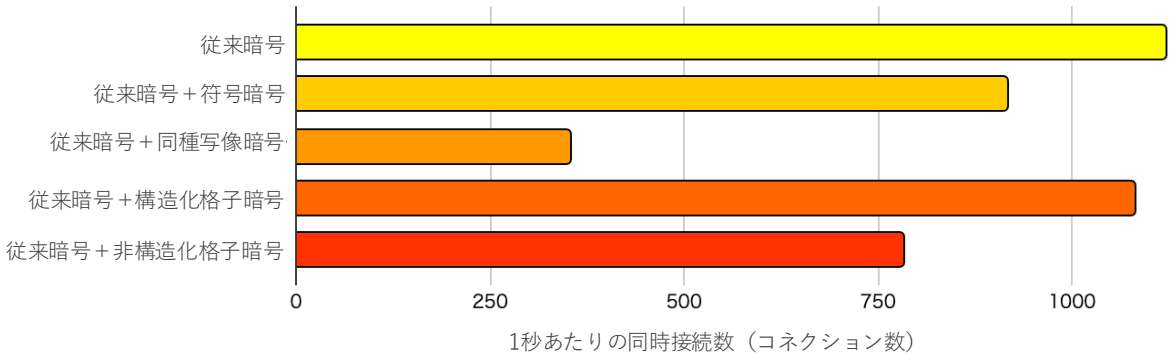

図6：アルゴリズムごとの同時接続数

CPUとメモリの使用量

図7は、各アルゴリズムの平均 CPU およびメモリ使用量の散布図を示しています。黒色で示された同種写像暗号（SIKE）は、鍵長が小さいためメモリ要件は低くなりますが、計算に時間がかかり、遅延が大きくなっていることがわかります。

一方、赤色で示された非構造化格子暗号（FrodoKEM）は同種写像暗号よりも必要な計算量は少なくなりますが、サイズが大きいためメモリ使用率が高くなります。これは、特定の帯域幅でネットワーク上で大規模な鍵交換をすると、遅延が長くなるためです。 CPU使用率の分布はさまざまな PQC アルゴリズムを正確に表しますが、メモリ使用率の分布は基礎となるOSのメモリ管理動作の影響を受けることに注意することが重要です。

ここでも、緑色で示された構造化格子暗号（ML-KEMなど）は黄色で示された従来暗号（ECC）と比較的近い値であることがわかります。

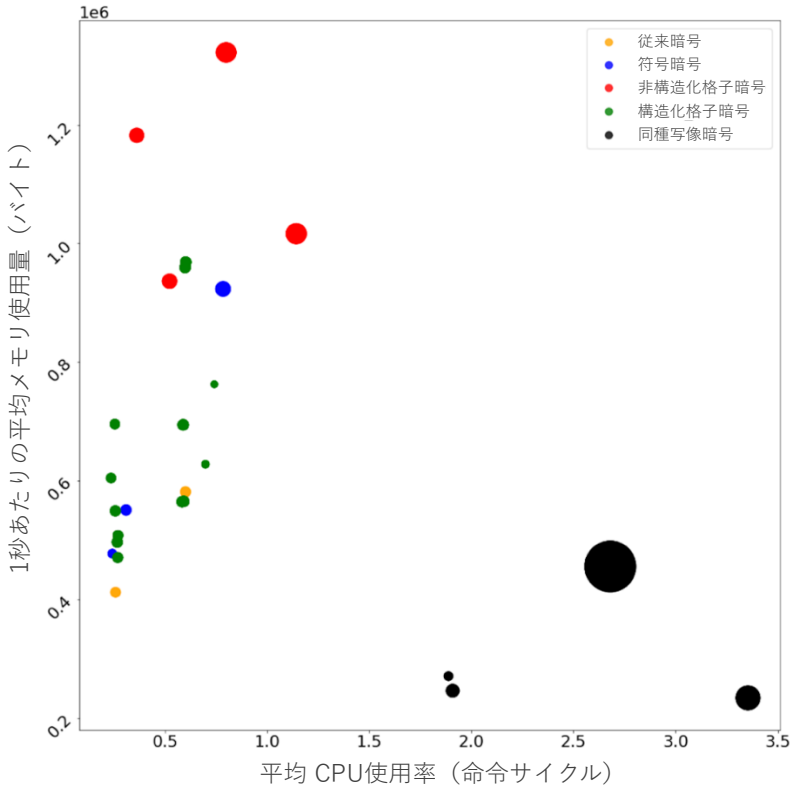

図7：平均 CPU使用率（命令サイクル）と平均メモリ使用率（バイト）。
色はベースとなる数学的問題を表し、円のサイズは鍵交換の相対的な遅延を表す。

デジタル署名のハンドシェイクデータ量

図8は、PQCハイブリッドデジタル署名アルゴリズムのハンドシェイクのデータ量を示しています。従来の署名アルゴリズム（ECDSA）のデータ量は非常に小さいですが、ML-DSAやFN-DSAといったPQCアルゴリズムのデータ量は大きくなります。従来のアルゴリズムとPQCアルゴリズムを組み合わせたハイブリッド方式では、データ量がさらに増加します。

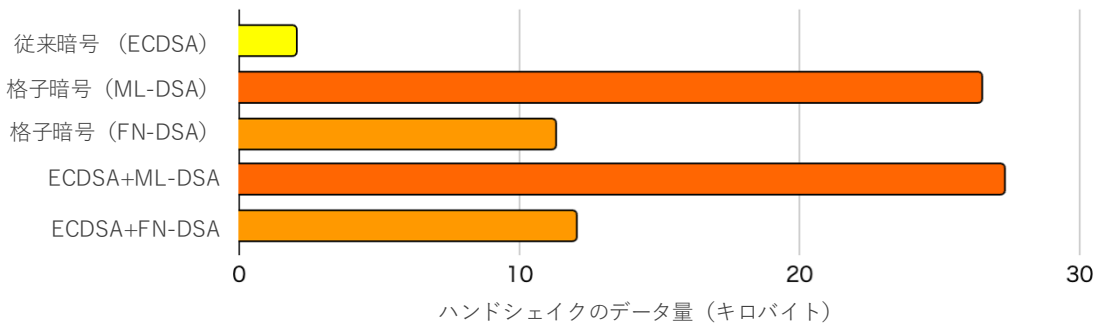

図8：TLSハンドシェイクのデータ量（キロバイト）

© SandboxAQ, SoftBank Corp.

デジタル署名の遅延

データ量を考慮すると、デジタル署名アルゴリズムの実装は一見すると難しいように思えるかもしれません。しかし、遅延の観点から見ると、PQCが非常に効率的であることがわかります。PQCアルゴリズムによるデジタル署名にかかる時間は、従来の署名アルゴリズムの遅延の4分の1未満であることを示しています。また、ML-KEMの場合、計算は10分の1以下の非常に短い時間で完了するため、遅延への影響は最小限であることがわかります。

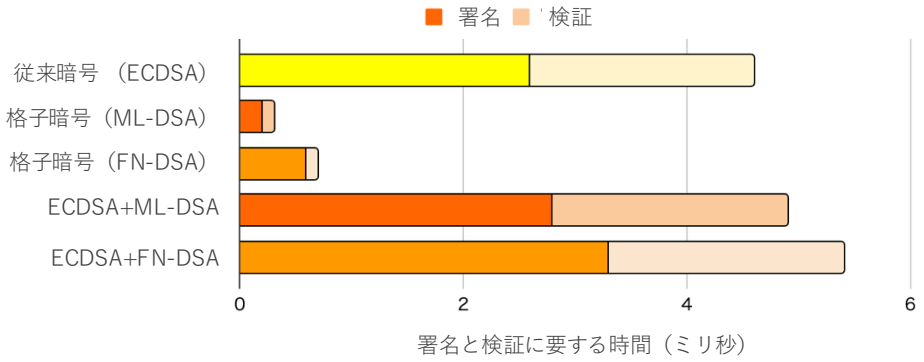

図9：デジタル署名の署名と検証の処理時間（ミリ秒）

考察

以上の実証実験では、適切なアルゴリズムを選定することで、PQCがパフォーマンスに与える影響を最小限にすることができることがわかりました。 特に、ML-KEM や ML-DSA のような構造化格子に基づくPQC　アルゴリズムの性能が高いことを裏付けています。この結果は、量子コンピューターによる攻撃に対して効果的にデータを保護することを目指す組織にとって、ML-KEM　や　ML-DSAのように標準化されたPQCアルゴリズムを用いたハイブリッド暗号方式が明確で実行可能な道筋であることを示しています。

一方で、デジタル署名におけるハンドシェイクサイズは、ハイブリッド方式を用いることで悪化する場合があります。これらは今回検証したユーザーシナリオでは、通信のハンドシェイク時のみに発生することから大きな影響はありませんが、多量のデジタル署名を一度に受けるようなユースケースでは通信負荷として顕在化する可能性があります。PQC移行に際しては、ユースケースに合わせてネットワークへの影響を検証することが重要です。

© SandboxAQ, SoftBank Corp.

PQC の早期移行に向けたアクション

PQC早期移行の利点

ソフトバンクとSandboxAQによる実証実験は、量子コンピューター時代に備える組織にとって、ハイブリッド暗号方式が実用に耐えうるソリューションであることを示しました。

ハイブリッド暗号方式は、組織の機密情報を現代のサイバー脅威から保護し、量子コンピューティングの進歩に備えるための強力な手段です。一方で、署名アルゴリズムの通信サイズや鍵交換におけるCPU負荷などを考慮し、要件を満たすアルゴリズムを慎重に選択し、検証する必要があります。

量子コンピューターに耐性のある暗号化アルゴリズムへの移行に向けて積極的な措置を講じることで、組織は持続的なセキュリティーと競争上の優位性を得ることができます。

ハイブリッド暗号方式を早期に導入することで、次のようなメリットが得られます。

- 能動的なデータ保護：組織は、新たな量子脅威から機密情報を即座に保護でき、特にSNDL攻撃に対して脆弱なデータを保護できます。
- コンプライアンスの保証とリスク軽減：FIPS（Federal Information Processing Standards）、PCI-DSS（Payment Card Industry Data Security Standard）、EU一般データ保護規則（GDPR：General Data Protection Regulation）などにより定められる規則では、堅牢な暗号化保護の必要性がますます高まっています。早期に移行に着手することで、 規制によりPQCへの対応が求められた際に、規制に違反するリスクを軽減することができます。
- コスト：早期に移行することで、事後対応的にアップグレードすることに伴う長期的な財務的および運用上の負担が軽減されます。ハイブリッド暗号方式を使用すると、組織は既存の暗号化を維持しながら、段階的にPQC 標準に移行できます。
- 信頼と評判の向上：先進的なセキュリティーを早期に実証することで、組織は顧客、パートナー、規制当局からの信頼を獲得することができます。

企業は早期に行動することで、将来のリスクを軽減し、コンプライアンスの取り組みを簡素化し、重要なデータを長期的に保護することができます。

© SandboxAQ, SoftBank Corp.

組織の PQC 移行のベスト プラクティス

量子安全な暗号化への移行を成功させるには、慎重な計画と実行が必要です。組織は、PQC をスムーズに導入するために、明確で実践的な手順に従う必要があります。

ステップ #1: 暗号化インベントリの構築

まず、現在使用されているすべての暗号化システムを徹底的にカタログ化することから始めます。それぞれのシステム内でどの暗号化方式（RSA、ECC、デジタル署名など）が機密データを保護するかを正確に記載する詳細な文書を作成します。組み込みの暗号化、証明書、キー管理プロセス、HSM、サードパーティーサービスを見落とさないことが重要です。

ステップ #2: 優先順位の決定

データの機密性、法規制への準拠、将来の量子脅威に対する脆弱性に基づいて移行対象の優先順位を決定します。インフラと、長期的な機密保持が必要な財務記録、健康情報、知的財産などの価値の高いデータを優先します。移行を進める上で、早急に対応する必要があるもの、また移行に際して多くの労力が必要となるシステムを特定します。

ステップ #3: Crypto-agility（暗号俊敏性）のあるシステムの構築

Crypto-agilityとは暗号化アルゴリズムやプロトコルを迅速に切り替える能力を指します。新しい暗号化アルゴリズムの採用には、多くの場合、技術的なハードルが伴います。新しいアルゴリズムを迅速かつシームレスに統合可能な柔軟なフレームワークを作成して準備することが重要です。ライブラリの抽象化または集中暗号管理サービスは、将来のアップグレードやアルゴリズムの切り替えが必要になった場合に、必要な労力を最小限に抑えるのに役立ちます。また、フレームワークまたは API を採用することで、アーキテクチャーを大幅に変更することなく、複数の暗号化標準をサポートすることもできます。

ステップ #4: ハイブリッド暗号方式の実装

現在および将来のデータを保護するために、PQCと従来の暗号化を組み合わせたハイブリッド暗号方式を実装します。この二重の暗号化により、データを即座に保護しながら、将来的なPQC単体の実装に段階的に移行できる柔軟性が提供されます。これにより、将来的に一部の PQC アルゴリズムに脆弱性が発生した場合でも組織のデータは保護され、リスクが大幅に軽減されます。

© SandboxAQ, SoftBank Corp.

PQCへの早期移行に向けて

量子コンピューターが新たな緊急の脅威を生み出す中、量子安全な暗号化ソリューションの必要性がかつてないほど明確になっています。 RSA や ECC などの従来の暗号化手法は、将来の量子コンピューターの飛躍によってその安全性が破られ、機密性の高いビジネス、政府のデータが危険にさらされることになります。

構造化格子に基づくPQCと従来暗号による ハイブリッド暗号方式は、組織にこれらの課題に対処する実用的で効果的な方法と考えられます。ハイブリッド暗号方式を早期に導入することで、即時にセキュリティが確保され、SNDL攻撃から重要な情報が保護されます。

ソフトバンクとSandboxAQの実証実験は、このアプローチの実行可能性だけでなく、様々なシナリオでのネットワークへの影響が最小限であることも確認しました。

ソフトバンクとSandboxAQは、今後も組織のPQC対応への移行をサポートするソリューションの開発、またその導入に向けた活動を推進していきます。

参考文献

[1] “NIST Releases First 3 Finalized Post-Quantum Encryption Standards.” National Institute of Standards and Technology, August 2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[2] 「ソフトバンクがSandbox AQと共同で量子コンピューターで解読不可能な次世代暗号方式の早期実装へ」. SoftBank Corp, 23 March 2022, https://www.softbank.jp/corp/news/press/sbkk/2022/20220323_01/.

[3] 「耐量子計算機暗号アルゴリズムの実用性を確認」. SoftBank Corp, 28 February 2023, https://www.softbank.jp/corp/news/press/sbkk/2023/20230228_01/

© SandboxAQ, SoftBank Corp.