TOSHIBA

ホワイトペーパー

量子暗号通信と金融ブロックチェーン

安全な金融取引の将来について

はじめに

ブロックチェーン技術は、間違いなく過去10年間に出現した最も破壊的で革新的な技術のひとつですが、このブロックチェーンが約束するセキュリティを損なうかもしれない別の技術があります－量子コンピューティングです。量子コンピューティング技術の能力は、現在のブロックチェーンを含めた、特定の数学的アルゴリズムに依存するあらゆるセキュリティシステムへの挑戦となり得ます[1]。

任意の2拠点間でデータを電子的に送信することは傍受に対して脆弱であり、今日の公開鍵暗号方式を使用して転送中のデータを暗号化することでさえ、「今収集して後で解読」攻撃に対して脆弱になる可能性があります。これは、攻撃者が将来量子コンピューターが現在の暗号化標準を破れるほど強力になってからデータを解読することを目的として、いま流れている暗号化されたデータを体系的に記録しておくものです。公開鍵暗号方式で保護されたデータの解読にかかる時間を大幅に短縮できるかもしれないほど量子コンピューターの進化のスピードは速まっており、この脅威はますます喫緊なものとなっています。

量子鍵配送＝Quantum Key Distribution（QKD）技術は、量子力学の法則を利用することで、二者間で同じ秘密鍵を共有し、第三者が鍵共有プロトコルを盗聴しようとしていることを検出できます。QKDは、今日の大都市圏でのミッションクリティカルなアプリケーションへ適用可能であり、耐量子計算機暗号とのハイブリッドアプローチにも応用できます。ハイブリッドソリューションの一部としてのQKD利用は永続的なセキュリティを提供し、基盤となる公開鍵暗号化データに対する「今収集して後で解読」攻撃が成功しないことを保証します。

このホワイトペーパーでは、これらの技術の進化とJPモルガン・チェース、シエナと共同で東芝アメリカ社が実施した実際のアプリケーション調査研究およびQKDの将来について説明します。

ブロックチェーンとは

ブロックチェーンは、情報をブロックに格納する分散型の不変で安全な[2]電子データベースです。従来、データはテーブルに保存されていました。しかし、（ブロックチェーンの）名前が示すように、ブロックは、前のブロックの数字と文字に基づいてランダムに生成された数字と文字からなる長い文字列としてデータを保存します。各ブロックにはあらかじめ決められた容量があり、情報は変更の内容と日時を記録する一意のハッシュコードと共に、線形かつ時系列に保存されます。ブロックが容量に達すると、ブロックは閉じて前のブロックにリンクされることでブロックチェーンが形成されます。各ブロックは時系列でチェーンに追加されるため、トランザクションを記録するための優れた元帳になります。

ブロックチェーンのセキュリティは、完全性とコンセンサスという2つの原則によって支えられています。完全性とは、誰かが他の誰かに代わって取引を行うことができないということです。すべてのデジタル署名は、所有者だけが知っている一意の秘密鍵で生成され、所有者の公開鍵を使用して照合されるため、偽造は不可能です。最終的に、コンセンサスがブロックへの新しいエントリがどのように受け入れられ、検証されるかを規定します。これにより、変更はネットワーク全体として検証され、承認されてからブロックに追加されるので、ブロックチェーンレコードに「嘘をつく」ことは不可能になります。この全体的な承認（「コンセンサス」）がなければ変更は記録されず、データが悪意を持って改ざんされる可能性がなくなります。

ブロックチェーンはセキュリティと忠実度のレベルが高いため、金融業界で特に役立ちます。ブロックチェーンにより、金融機関はカスタムアプリケーションを介して支払情報を転送する、より効率的な手段を開発するという最終目標に向けて、支払関連情報を迅速かつ安全に交換できます。このプロセスの簡素化により、金融機関間の支払速度と精度の向上、返送可能性の低減、支払処理時間の短縮が可能になります。

暗号化とは

暗号化とは、意図する受け手だけが秘密のデータにアクセスできるよう、符号により情報と通信[3]を保護する手段です。暗号化技術はアルゴリズムを使用してメッセージを変換（または「暗号化」）し、許可されていない者がメッセージを解読できないようにします。アイデンティティ（本人性）に加えて、暗号化手法は真正性と完全性を保護します。真正性はあなたの本人性（身元）を証明し、完全性は不正な変更からデータを保護します[4]。暗号化アルゴリズムには、対称鍵（または単一鍵）暗号化と非対称鍵（または公開鍵）暗号化の2種類があります。

- 対称鍵暗号化[5]は、電子情報の暗号化と復号を1つの鍵のみに依存しています。対称鍵暗号化を介して通信する送受信者双方は、共有鍵について合意する必要があります。

- 非対称鍵暗号化[6]を使用すると、送受信者ごとに2つの異なる、しかし数学的には関連する鍵（1つは公開鍵、もう1つは秘密鍵）が生成されます。コンテンツの作成者は両方の鍵を知っています。公開鍵を使用して暗号化されたメッセージは対応する秘密鍵を使用して復号でき、その逆も可能です。公開鍵を自由に共有することで他者は送信内容を暗号化でき、それは公開鍵と秘密鍵の両方を所有する者のみが復号できます。デジタル署名は、所有者が秘密鍵を使用して署名し、受信者が公開鍵を使用して照合することによって実現されます。

ブロックチェーンを使用する利点は、主に以下の5点です[7]。

1. **強化されたセキュリティ**：ブロックチェーンの不変性は、不正行為事象を減らすのに役立ちます。その分散性により、データの変更が困難になり、分散されたデータのビューの信頼性を確保します。匿名化機能と制御されたアクセスポイントにより、エンドツーエンドの暗号化と組み合わせることで、データのプライバシーを保護するための優れた選択肢になります。

2. **透明性の向上**：ブロックチェーンデータの分散性のおかげで、トランザクションは複数の場所で同じように記録されます。ネットワークのすべてのメンバーは、常に同じデータを同時に見ることになります。厳密な時系列の記録により、メンバーはトランザクションの履歴全体を確認できるため、詐欺の可能性を減らすことができます。

3. **即時の追跡可能性**：ブロックチェーンの強力な日付と時間管理により、資産の出所を秒単位で証明できる監査証跡が作成されます。これは詐欺が蔓延している業界や、製品の出所に懸念を持つ消費者にとって特に重要です。

4. **効率と速度の向上**：ブロックチェーンにより、手作業による事務処理の効率と速度が向上します。ドキュメントとトランザクションの詳細はブロックチェーンに保存されるため、紙でやりとりしたり、複数の元帳を調整したりする必要がありません。

5. **自動化**：自動化は、特にスマートコントラクトを使用する場合に、この速度と効率の向上の重要な側面です。これらのコントラクトでは、所定の要件が満たされると、トランザクションプロセスの次のステップが起動されます。これにより、人間の介入やサードパーティでの検証の必要性が減ります。

新しい技術による脅威

強力で効果的で広く利用可能な量子コンピューターは、数年先には実現する見込みです。ただし、この技術は、短期的にも長期的にもサイバーセキュリティに課題をもたらし続けています。先に述べたように、当面の懸念の1つは、「今データ収集して後で解読する」攻撃の蔓延です[8]。今日の長期保存すべき情報は、特定の悪意ある者によるこの種の攻撃に対して特に脆弱です。

マクロの視点では、量子コンピューターの処理能力が指数関数的に増加すると、現在のデジタル通信と情報全体が危険にさらされます。量子コンピューターが十分に強力になると、既存の公開鍵暗号標準を破り、デジタルシステムへの脅威となり得ます。

この脅威に対抗するには、QKDなどの耐量子性のある暗号化標準を世界規模で実装する必要があります。政府と重要な機関（銀行やIT企業を含む）は、これらがまだ理論上の脅威に留まっているうちに、量子セキュリティ計画を策定し、量子に対応出来る人材を育成する必要があります。

現在の暗号化レベル

公開鍵暗号は、Web上のいくつかのアプリケーションで広く使用されています。この暗号化方式は、電子通信の機密性、完全性および信頼性を保証します。現在使用されている一般的な公開鍵暗号アルゴリズムには、RSA、Diffie-Hellman、楕円曲線暗号化などがあります[9]。これらのアルゴリズムのセキュリティは、コンピューターが特定の数学的問題－非常に大きな数の素因数分解など－を解くのが非常に困難であるという仮定に基づいています。

そのような仮定は何十年もの間当てはまっていました。しかし、量子コンピューターの台頭は、現在の暗号化システムのセキュリティを脅かしています。量子コンピューターとその演算能力の元となる量子ビットは一度に複数の計算を実行できるため、対応する公開鍵から任意の送受信者の秘密鍵を計算でき、現在のコンピューティングよりもはるかに短い時間で一般の暗号化方法を解読できます。大規模な商用量子コンピューターはまだ広く利用可能ではありませんが、技術が初期段階にある今のうちに、企業は防御を強化する必要があります。この目的のために企業が取り得る2つの選択肢は、①既存の（異なる仮定に基づく）計算量的暗号化方法を既存の方法よりも安全であろう新しい方法に置き換える、または、②仮定は一切行わず、未来の量子に対しても安全なQKDを導入する、です。

QKDを導入するという選択肢は、計算上の仮定ではなく物理法則により送受信者間の通信を保護するものであり、最も有望です。この量子暗号[10]は、粒子自体の性質を変更せずに粒子の状態を観測することは不可能であることが確立されている、量子力学の観測および複製不可能の原則に基づいています。QKDシステムでは、対称暗号鍵は最初に光子の形で表され、観測と複製不可能の原則に従います。これは、第三者（「盗聴者」）がQKDで生成された鍵を傍受しようとすると光子自体が変化し、鍵として使うことができなくなるので、盗聴者による干渉を発見し警告できることを意味します。鍵を傍受出来なければ盗聴者は鍵を使用して暗号化されたメッセージを復号できず、システムの機密性が確保されます。

米国National Institute of Standards and Technology（NIST）[11]は現在、NISTサイバーセキュリティフレームワークの利用を通じてサイバーセキュリティリスク管理を改善しようとしている組織に方向付けとガイダンスを提供しています。業界や政府と協力して作成されたフレームワークは、重要なインフラストラクチャの保護を促進するための標準、ガイドラインおよび事例で構成されています。フレームワークの優先順位が付けられ、柔軟性があり、再現性があり、費用効果の高いアプローチは、重要なインフラストラクチャの所有者と運営者がサイバーセキュリティ関連のリスクを管理するのに役立ちます。

QKD鍵生成の利点

データを安全に保つことは、今日の情報技術の急速な発展によってもたらされる最大の課題の1つです。ますます多くの機密データがリモートのクラウドベースのサーバーに保存されるため、このデータへの安全なアクセスが主な関心事になっています。データ伝送の保護はパブリックネットワークを介して送信される情報の暗号化に依存しています。QKDを使用してデータを安全に共有することは、ビジネスにとって不可欠な考慮事項になっています。

金融機関には、最も厳しいITおよびデータセキュリティ要件がいくつかあります。彼らは、銀行取引やアプリケーションのデータのリアルタイムの可用性を確保すると同時に、機密性の高いクライアントや社内情報を保護する必要があります。さらに、コンプライアンスおよび規制要件のレベルは上がる可能性があります。

これらの機関は、リアルタイムの取引とトランザクションデータ交換のために、データ処理およびリカバリセンターからキャンパスネットワークにデータを安全に転送できる必要があります。データは、広域ネットワーク上の勘定系アプリケーションとビデオ会議ツールによって処理されます。

QKDは、ブロックチェーンアプリケーションから公開鍵の仮定をなくすための最初のステップです。これは、多くの業界にとって必須である機密性の高いデータを保護するために重要な秘密鍵を配布するために使用されます。金融、防衛、公益事業、医療セクターのデータ機密性と、スマートシティとスマートエネルギー送配電網を支える重要なインフラストラクチャを保護します。

QKDセキュリティの本質は、たとえば通常の光ファイバーを介して送信される単一の光子（光の粒子）に基づいて鍵の各ビットをエンコードすることに依存しています。光子を読み取ったりコピーしたりしようとするとエンコーディングが変更されるので、それぞれの鍵の機密性を検証し、保証できます。単一の光子を小さな粒子に分割したり、その中にエンコードされている情報を変更せずにコピーしたりすることはできません。後者は、前述の複製不可能定理によって禁止されています。これにより、QKDが提供する高レベルのセキュリティが可能になります。

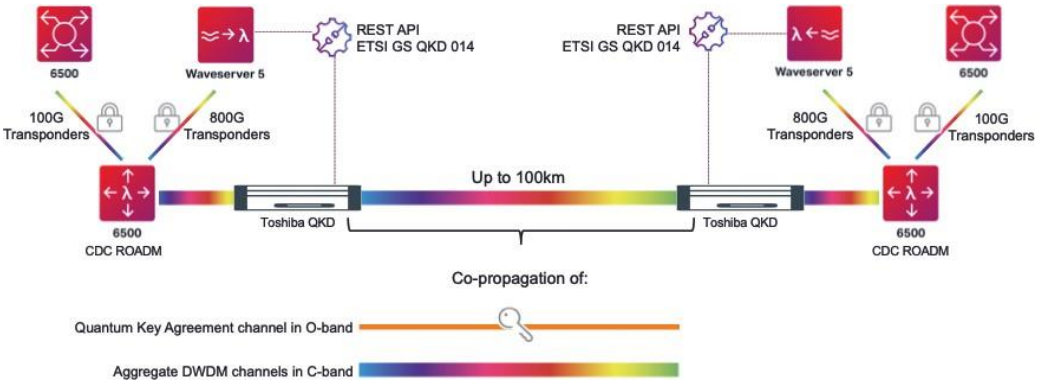
QKDを採用することで、組織は通信インフラストラクチャを、今日の膨大な数のサイバー脅威と将来の脅威から保護できます。すでにハッカーはスーパーコンピューターの進歩、量子コンピューターの実現、または暗号解読の新しい技術の発見を通じてデータを解読することを目的として、「今収集し後で復号する」などの手法を用いデータを集め保存しています。QKDにより、長期的な保護が必要なデータは今日のIT環境で安全であるだけでなく、もう目の前に迫っている量子の時代にも保護され続けることが将来にわたって保証されます。

実世界のアプリケーション：JPモルガン・チェース、シエナおよび東芝アメリカ社のQKDテストベッド

東芝アメリカ社は、JPモルガン・チェース、シエナと協力して、オハイオ州コロンバスにあるJPモルガン・チェースの光伝送ラボで共同実験研究を実施し、ミッションクリティカルな大都市規模の運用環境において、QKDで保護された800Gbpsの耐量子光通信チャネルの実行可能性を実証しました。これは業界で初めての暗号化であり、QKD鍵の生成と、QKDで保護された非常に大量の情報の送信が単一のファイバーで可能であることを確認しました。この調査研究のテストベッドは実際の環境を模倣するように注意深く設計されています。

研究チームは、新たに開発されたQKDネットワークが、盗聴者を即座に検出して防御する能力を実証しました。また、量子チャネルの品質に対する現実的な環境要因の影響についても研究しました。この共同研究には、ミッションクリティカルなブロックチェーンアプリケーションを保護するQKDの業界初のデモンストレーションも含まれていました。

この研究の結果は、データセンター間相互接続など、大容量、大都市規模、ミッションクリティカルな運用環境でのQKD技術に基づく量子セキュア光チャネルの展開への道を開きます。研究論文の全文は**このリンク**（https://doi.org/10.48550/arXiv.2202.07764）から入手できます。



この図は、AES暗号化装置が多重化QKDシステムから秘密鍵を取得して、高帯域幅のデータストリームを保護するユースケースの例を示しています。.

QKDを使用したブロックチェーンの利点

許可型ブロックチェーンネットワークは、多くの場合、大量の機密情報を処理します。この情報はネットワーク内の他の関係者に読まれることを目的とする一方で、データの転送中はデータの機密性を保持することが重要です。現在、このデータの機密性は標準の公開鍵暗号方式を使用して保護されていますが、これは、将来の量子技術を使った盗聴者に対して十分ではありません。

次に来るのは?

東芝グループ、JPモルガン・チェースやシエナなどの企業は、実世界のアプリケーション技術開発の最前線にいます。量子コンピューティングの時代が近づくにつれ、堅牢な暗号化が非常に重要になります。ますますQKDは、ヘルスケアや国家安全保障などの他の分野で、金融セクターで実証されたのと同様の応用が展開されるでしょう。

研究者は、他の事象に同様にQKDを適用することを次の2つの主要な方向で想定しています。まず、今回行ったように、機密性の保証を強化するためにQKD秘密鍵を使用して通信チャネルを保護する手法に用いること。次に、ブロックチェーンの完全性とコンセンサスの場合のように、公開鍵暗号の他のインスタンスをQKDによって可能となる対称鍵暗号に置き換えることです。目標は、量子コンピューターと将来の暗号解読にさらされる潜在的な攻撃対象領域を減らすために、可能な限り公開鍵の仮定への依存を減らすことです。

それほど遠くない将来、QKDは量子インターネット上での安全な通信のための基盤技術になるでしょう。

参照先

1. “Quantum Computing Will Break the Blockchain and QKD Can Save It ” *Quantum Xchange,* https://quantumxc.com/blog/quantum-computing-will-break-the-blockchain-and-qkd-can-save-it/
2. Hayes, Adam. “Blockchain Explained.” *Investopedia,* Investopedia, 15 Apr. 2022, https://www.investopedia.com/terms/b/blockchain.asp
3. Richards, Kathleen. “What Is Cryptography?” *SearchSecurity,* TechTarget, 27 Sept. 2021, https://www.techtarget.com/searchsecurity/definition/cryptography
4. Saylor Academy. “Confidentiality, Integrity, and Authenticity: Attributes of secure communication” *Saylor Academy,* 5 May, 2022, https://learn.saylor.org/mod/book/view.php?id=29682&chapterid=5263
5. Smirnoff, Peter, and Dawn Turner. “Symmetric Key Encryption – Why, Where and How It’s Used in Banking.” Cryptomathic, https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking
6. Brush, Kate, et al. “What Is Asymmetric Cryptography?” *SearchSecurity,* TechTarget, 27 Sept. 2021, https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography
7. Pratt, Mary K. “Top 10 Benefits of Blockchain Technology for Business.” *SearchCIO,* TechTarget, 2 June 2021, https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business
8. ISARA Corporation. “Protect against Harvest & Decrypt.” *ISARA Corporation,* https://www.isara.com/solutions/use- cases/protect-against-harvest-decrypt.html
9. Lake, Josh. “What Is RSA Encryption and How Does It Work?” *Comparitech,* 22 Mar. 2021, https://www.comparitech.com/blog/information-security/rsa-encryption/
10. “Quantum Encryption vs. Post-Quantum Cryptography.” *QuantumXC,* 22 Mar. 2022, https://quantumxc.com/blog/quantum-encryption-vs-post-quantum-cryptography-infographic/
11. Nicole.keller@nist.gov. “Cybersecurity Framework: Getting Started.” *NIST,* 14 Apr. 2022, https://www.nist.gov/cyberframework/getting-started

このホワイトペーパーは、東芝アメリカ社が発行したWhite Paper「Quantum Key Distribution and Blockchain Securing the Future of Financial Transactions」を基に、東芝デジタルソリューションズ株式会社によって日本語翻訳したものです。

TOSHIBA

東芝デジタルソリューションズ株式会社
ICTソリューション事業部　QKD事業推進室
〒212-8585 神奈川県川崎市幸区堀川町72番地34

量子暗号通信に関するお問い合わせ先：Mrkt-InfoQKD@ml.toshiba.co.jp
https://www.global.toshiba/jp/products-solutions/security-ict/qkd.html