プレスリリース
2023 年 12 月 18 日

国立研究開発法人情報通信研究機構
野村ホールディングス株式会社
TOPPAN デジタル株式会社
株式会社大和証券グループ本社
株式会社みずほフィナンシャルグループ

複数の企業間を結ぶ量子暗号ネットワークテストベッドの運用試験を開始

【ポイント】

- 国内初の企業間量子暗号ネットワークの試験環境を構築
- 企業間でデータを安全にやり取りし、保管するための運用試験を開始
- 民生分野での量子暗号技術の効果的な活用法・運用法に関する知見を蓄積し、利用者の拡大を目指す

国立研究開発法人情報通信研究機構（ＮＩＣＴ、理事長: 徳田 英幸）、野村ホールディングス株式会社（代表執行役社長 グループ CEO: 奥田 健太郎）、TOPPAN デジタル株式会社（代表取締役社長: 坂井 和則）、株式会社大和証券グループ本社（執行役社長: 中田 誠司）、株式会社みずほフィナンシャルグループ（執行役社長: 木原 正裕）は、NICT が運用する東京 QKD ネットワーク[*1] 上に新たに整備された企業間量子暗号ネットワークテストベッドを用いて、データの送受信やバックアップ保管など安全に共有・利活用する運用試験を開始します。

本運用試験を通じて、多くの企業が量子暗号ネットワークを共通基盤として利活用する際の課題を抽出し、民生分野（金融・医療など）における量子暗号技術[*2] の効果的な活用法・運用法に関する知見を蓄積するとともに、本テストベッドをより使いやすくなるよう改良しながら利用者の拡大を目指します。

なお、本テストベッドの構成や利用可能なアプリケーションについては、12 月 20 日（水）に開催される量子暗号技術セミナー（オンライン形式、主催: 一般社団法人量子 ICT フォーラム）にて紹介します。

【背景】

様々な重要情報がデジタル化されてデータセンターなどに半永久的に保存され続ける時代となり、それがハッカーの格好の攻撃対象になるという新たな状況に直面しつつあります。現時点では解読できなくても、データを盗聴・保存しておき、将来、高度な計算機が登場したときに過去に遡って全データを解読するという脅威が現実のものとなっています。さらに、予期せぬ災害で重要情報が消失する事案も起こっています。

暗号解読技術が年々高度化し続けている一方で、近年、高度に秘匿すべきデータも、複数の企業や組織間でデータを共有し、新たな技術開発やビジネス創出につなげるデータ連携の動きが加速しています。

将来の解読に脅かされることのない情報理論的安全性[*3] を備え、かつデータ消失の危険性も少なく、安心してデータを流通・保管・共有・利活用できる新たなセキュリティシステムの構築が求められています。

【企業間量子暗号ネットワーク及び運用試験の概要】

NICT では、2010 年に安全な鍵供給を可能とする量子鍵配送ネットワークとして東京圏に QKD ネットワーク（「東京 QKD ネットワーク」）を形成、運用を続けてきました。さらに、重要情報を安全に長期保管し利活用する仕組みとして、東京 QKD ネットワーク上に秘密分散技術[*4] を組み込んだ量子セキュアクラウドを開発し、以降、現在に至るまで運用しながら様々な技術実証やアプリケーションの開発を行ってきました。

今回、様々な社会課題の解決に向け、複数の企業拠点を結んで東京 QKD ネットワークを拡張するとともに、量子インスパイアードコンピュータ[*5] と呼ばれる計算エンジンも組み

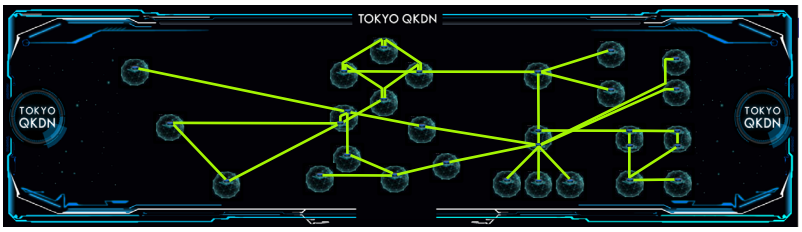


図 テストベッドのネットワーク監視画面

込み、安全に試験利用できる環境を企業間量子暗号ネットワークテストベッドとして整備しました。これらの試験環境を複数の企業で連携し活用していくための運用試験を開始します。運用試験を通じて、企業が活用する際の課題及び多くの企業が連携活用する際の課題を抽出するとともに、従来インフラとの親和性/責任分界点のバランスなどの設計についても検証を行います。

【今後の展望】

民生分野における量子暗号技術、量子セキュアクラウド技術の効果的な活用法・運用法に関する知見を蓄積するとともに、本テストベッドをより使いやすくなるよう改良しながら利用者の拡大につなげます。将来的には、極めてセキュリティレベルの高いデータセンターネットワーク技術に発展させ、個別企業でのセキュリティ対策コスト削減に貢献し、長期秘匿化を必要とするデータを安全に利活用することを目指しています。

＜発表情報＞

・量子暗号技術セミナー（オンライン）

・発表日時: 2023 年 12 月 20 日（水） 13:30～15:30

・主催: 一般社団法人量子 ICT フォーラム

＜研究支援＞

なお、本研究の一部は、量子暗号通信ネットワークの社会実装加速のための広域テストベッド整備[*6] の成果及び総務省「ICT 重点技術の研究開発プロジェクト（JPMI00316）」「グローバル量子暗号通信網構築のための研究開発」の支援を受けて実施した成果も活用しています。

＜用語解説＞

***1 東京 QKD（Quantum Key Distribution）ネットワーク**

NICT が 2010 年から東京圏に構築・運用を続けている量子鍵配送（QKD）ネットワークのテストベッド。NEC、東芝、NTT-NICT、学習院大学などの様々な産学機関で開発された QKD 装置が導入され、装置改良の研究開発、長期運用試験、相互接続やネットワーク運用試験など、QKD ネットワーク技術の実用化に向けた研究開発のほか、QKD ネットワークを現代セキュリティ技術と融合した新しいセキュリティアプリケーションの研究開発などを進めている。

***2 量子暗号技術**

量子暗号は、「量子鍵配送」による暗号鍵の共有と、それを用いた「ワンタイムパッド暗号」から構成される。
量子鍵配送では、送信者が光子を変調（情報を付加）して伝送し、受信者は届いた光子一個一個の状態を検出し、「鍵蒸留」と呼ばれる情報処理により、盗聴の可能性のあるビットを排除して、絶対安全な暗号鍵（暗号化のための乱数列）を送受信者間で共有する。変調を施された光子レベルの信号は、測定操作をすると必ずその痕跡が残る（ハイゼンベルクの不確定性原理）ため、この原理を利用して盗聴を見破る。
ワンタイムパッド暗号では、送信情報のデジタルデータを、それと同じ長さの暗号鍵（0 と 1 のランダムなビット列）と足し算することで暗号化し、復号は更にもう一度足し算をすることで行う。パッドとは暗号鍵を意味する。一度使用した乱数列は二度と使わないというのがワンタイムパッド暗号の規則である。ワンタイムパッド暗号は、解読が絶対的に不可能であることがシャノンにより証明されている。

***3 情報理論的安全性**

一般的な暗号技術に用いられる、「特定の数学的な問題を解くことが難しい」という仮定に依存した安全性（計算量的安全性）とは異なり、攻撃者・盗聴者が得られる情報と、秘密情報との確率論的な独立性をもって安全性が保証される性質。理論上、いかなる盗聴攻撃によっても、情報が漏えいすることはない。

***4 秘密分散技術**

原本データを無意味化された複数（n 個）のデータ（シェア）に分割し、異なるデータサーバに分散保管する技術。危殆化するデータサーバの数は、ある閾値（k 個）未満であり、かつ、データサーバ間は完全秘匿回線で結ばれていると仮定した場合、どんな計算機でも破れない機密性を実現できる。n-k 個以下のサーバが棄損しても、残った k 個のサーバからシェアを集めることで、原本データを復元できる。一方、k 個以上のシェアがそろわないと原本データは復元できない。

***5 量子インスパイアードコンピュータ**

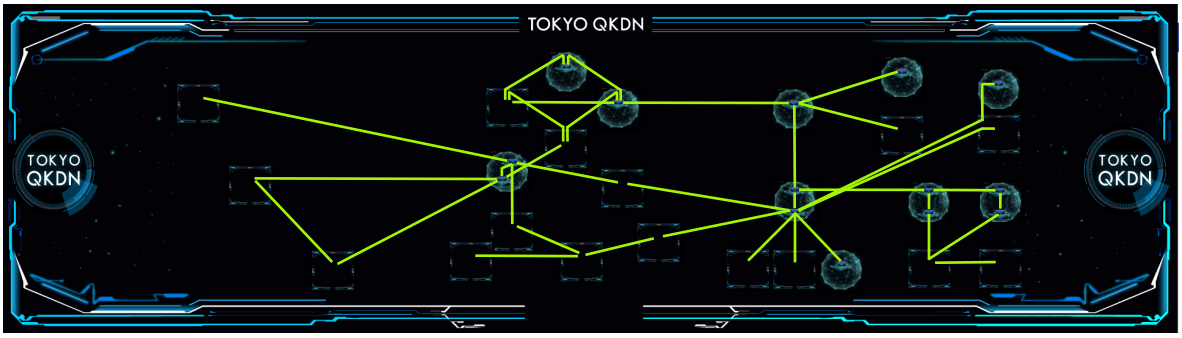
量子インスパイアードコンピュータは、従来の計算のシステム堅牢さと、量子コンピュータの能力の一つである「アニーリング技術」をデジタル回路で実現するシステムで、全体から複数のアプローチをしていくことで、汎用コンピュータでは解くことが難しい「組合せ最適化問題」を高速で解くコンピューティング技術である。

***6 量子暗号通信ネットワークの社会実装加速のための広域テストベッド整備**

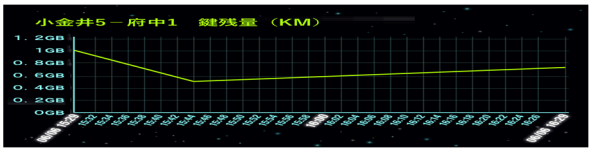
東京 QKD ネットワークを令和 3 年度補正予算により拡張整備中の事業。

補足資料

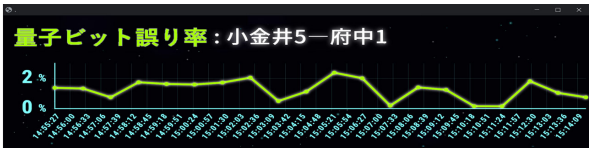
企業間量子暗号ネットワークテストベッドの構成



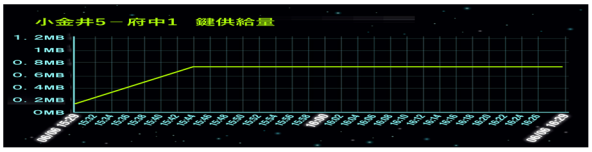
ネットワーク監視画面



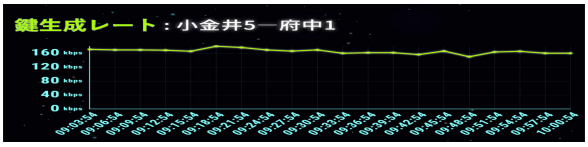
鍵残量



量子ビット誤り率



鍵供給量



鍵生成レート