プレスリリース
2022 年 11 月 17 日

国立研究開発法人情報通信研究機構
国立大学法人京都大学
株式会社東芝
株式会社 ZenmuTech

量子セキュアクラウドによる高速安全なゲノム解析システムの開発に成功

～従来不可能だった情報理論的安全で高速な処理を実現～

【ポイント】

- 量子セキュアクラウドによるゲノム解析を情報理論的安全かつリアルタイムに実施できるシステムを開発
- フィルタリング機能により、解析・治療に不必要な個人情報の保護が可能
- 今後、患者の MRI 画像などの重要データを安全に利活用できるデータプラットフォームとして期待

国立研究開発法人情報通信研究機構（ＮＩＣＴ、理事長: 徳田　英幸）、国立大学法人京都大学（総長: 湊 長博）、株式会社東芝（代表執行役社長　CEO: 島田　太郎）、株式会社 ZenmuTech（代表取締役社長　CEO: 田口　善一）は、量子セキュアクラウド[*1]（量子暗号[*2] ネットワーク上に秘密分散[*3] を組み合わせた分散ストレージシステム）にゲノム解析専用装置を装備し、全ゲノムデータの安全な伝送・保管・解析をリアルタイムで実施できるシステムの開発に成功しました。

安全なデータの解析手法として開発されている準同型暗号[*4] を用いたものやマルチパーティ計算[*5] では扱うことがほぼ不可能であった全ゲノムデータに対し、情報理論的安全な暗号化処理を施すことにより、ゲノム解析専用装置の処理速度を損なうことなく、情報理論的安全なデータ解析を実現しました。また、解析や治療に不必要な個人情報に対し、フィルタリング機能を実装しており、個人情報を保護しつつゲノム解析を実施できるシステムが完成しました。

今後、本技術は、超長期に保管が必要な患者の MRI 画像データなどの安全な利活用を可能とするデータプラットフォームとして活用されることが期待されています。

なお、本成果は、2022 年 11 月 2 日（水）に、英国科学雑誌「*Scientific Reports*」に掲載されました。

【背景】

個人のゲノムデータは究極の個人情報であり、超長期に秘匿性を担保しつつ利用する必要があります。しかし、現時点では従来の暗号技術での秘匿化に留まっており、2030 年頃に実現されるといわれているフルスケール量子コンピュータを用いれば解読されるおそれがあります。今、解析が困難としても、保管されているデータも将来攻撃されるリスクがあり、十分な対策が取られていないのが現状です。

例えば、従来から知られている安全なデータ処理方法として、秘密計算が挙げられます。秘密計算は、データを一切復号することなく秘匿したまま処理し、その出力も秘匿したまま得られるので、入力から出力まで一貫して安全なデータ処理を実現できる一方、計算リソースや通信リソースを多く必要とするという欠点がありました。秘密計算の一手法であるマルチパーティ計算では、データを秘密分散した状態で各種演算を実行可能ですが、複数サーバ間で大量の通信が必要となります。また、別の秘密計算手法である準同型暗号を利用した手法において

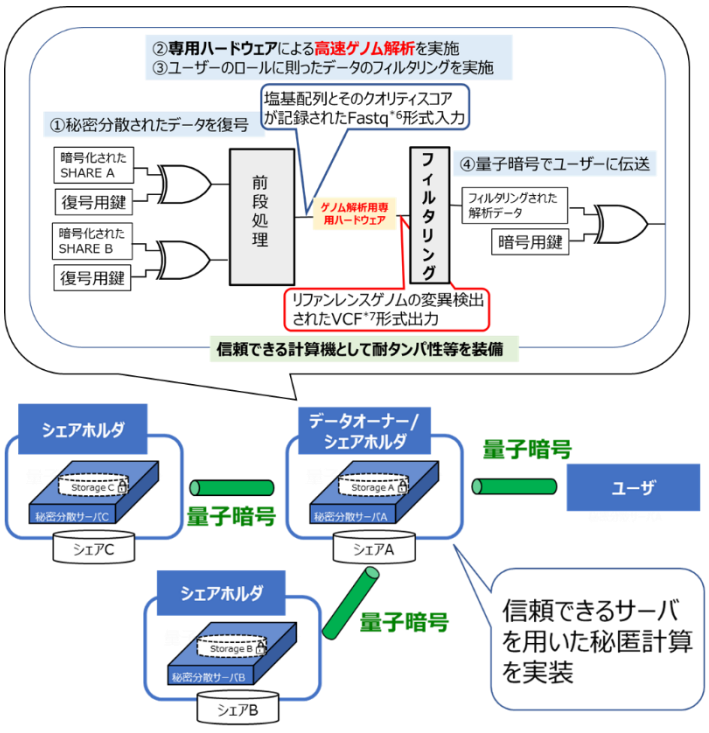


図 1　今回開発した“信頼できるサーバ”を実装した量子セキュアクラウド

は、その処理に大量の計算リソースが必要となります。そのため、いずれの秘密計算の手法においても、全ゲノム解析などの大容量かつ非構造化データに対し、四則演算よりも複雑な処理を可能とする実装は現時点において実現していません。

【今回の成果】

今回、本研究グループは、将来どのようなコンピュータが出現しても盗聴のリスクのない情報理論的安全な通信を可能とする量子暗号ネットワーク上に、情報理論的安全なデータ保管を可能とする秘密分散プロトコルを実装した量子セキュアクラウドを形成、さらに、ゲノム解析専用装置（全ゲノム解析を高速処理する専用ハードウェア）を物理的安全に実装し、情報理論的安全なデータ解析ができるシステムを開発しました。解析専用装置を“信頼できるサーバ”として取り込み、サーバ内での処理以外でのデータを情報理論的安全な形式に変換することで、安全な全ゲノム解析が可能となりました（図 1 参照）。

また、解析結果に関し、研究や治療に不要な個人情報をフィルタリングする機能も実装しました。この機能を付加しても、ゲノムデータ解析者（研究者や医師）は、ゲノムデータを遅延なく利用することが可能です。これにより、ゲノムデータ所有者（ゲノムデータを提供した個人、データ保管組織）及びゲノムデータ解析者の双方が安心して提供・解析できる環境が実現できます。

【今後の展望】

今回、量子セキュアクラウドに“信頼できるサーバ”を物理的に安全な環境に組み込み、大容量非構造化データの処理も安全かつ高速に実施できることを実証しました。このようなサービスは、専用ハードウェアのような計算リソースを有効活用でき、また、超長期に秘匿性を必要とする情報の保管・利活用も容易になります。

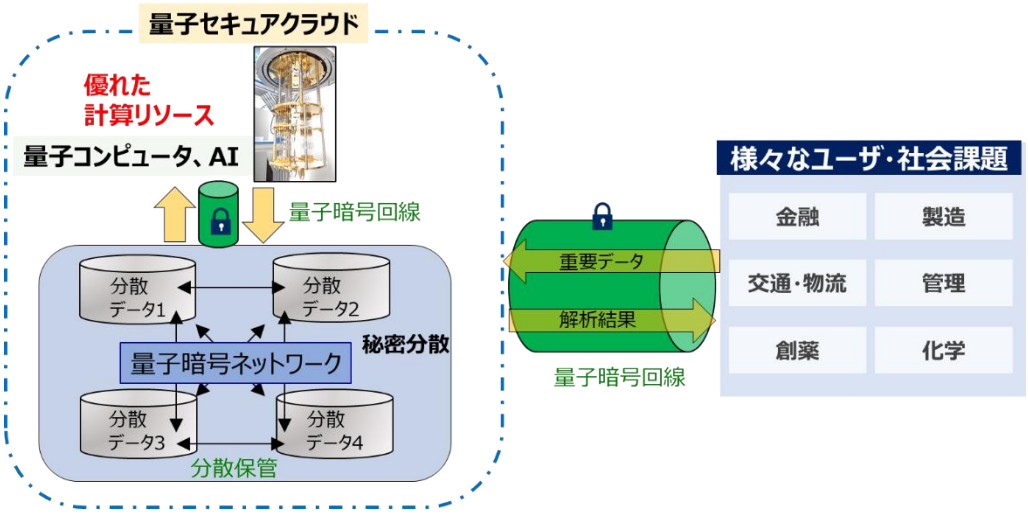


図 2 様々な計算エンジンを取り入れた量子セキュアクラウドの将来イメージ

今後、図 2 に示すように、様々な計算リソースや複数ユーザによる相互参照を可能とする仕組みを量子セキュアクラウドに実装し、リーズナブルなコストで、ゲノムデータや医療現場における患者の MRI 画像データを安全に利活用できる新しいデータプラットフォームとしての機能実証を目指します。

＜各機関の役割分担＞

・情報通信研究機構: 高速秘密分散、高速 OTP[*8] 暗号化装置、フィルタリング機能の実装
・京都大学: ゲノム解析手法、ユーザインターフェース設計、解析デモ
・東芝: 高速量子鍵配送[*9] 装置及び、ゲノム解析専用ハードウェアを含む実証環境構築・運用
・ZenmuTech: 準同型暗号、マルチパーティ計算周辺分野の調査、秘密分散ソフトウェア開発への協力

＜論文情報＞

掲載誌: *Scientific Reports*
DOI: 10.1038/s41598-022-22804-x
論文名: Secure secondary utilization system of genomic data using quantum secure cloud
著者: Mikio Fujiwara*, Hiroki Hashimoto, Kazuaki Doi, Mamiko Kujiraoka, Yoshimichi Tanizawa, Yusuke Ishida, Masahide Sasaki, and Masao Nagasaki*
Correspondence: *fujiwara@nict.go.jp, *nagasaki@csml.org

本研究の一部は、内閣府が主導する戦略的イノベーション創造プログラム（SIP）[*10]「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）の一環として実施しました。

＜用語解説＞

***1 量子セキュアクラウド**

量子セキュアクラウドシステムは、量子暗号技術と秘密分散技術を融合し、データの安全な流通・保管・利活用を可能とするクラウドシステムのこと。本技術の確立により、改ざん・解読が不可能な高いセキュリティ性を担保するだけでなく、例えば、金融、製造、交通・物流、管理、創薬、化学分野で蓄積された個人情報や企業情報など秘匿性の高いデータの収集・分析・処理・利用を可能とする。

***2 量子暗号**

光子を使って暗号鍵共有を行う量子鍵配送（QKD）装置、及びその暗号鍵を使い、ワンタイムパッド（OTP）方式により、情報の暗号化・復号を行う暗号技術のこと。量子コンピュータを含むあらゆる計算機で原理的に解読できない極めて安全な通信を実現できる（図 3 参照）。

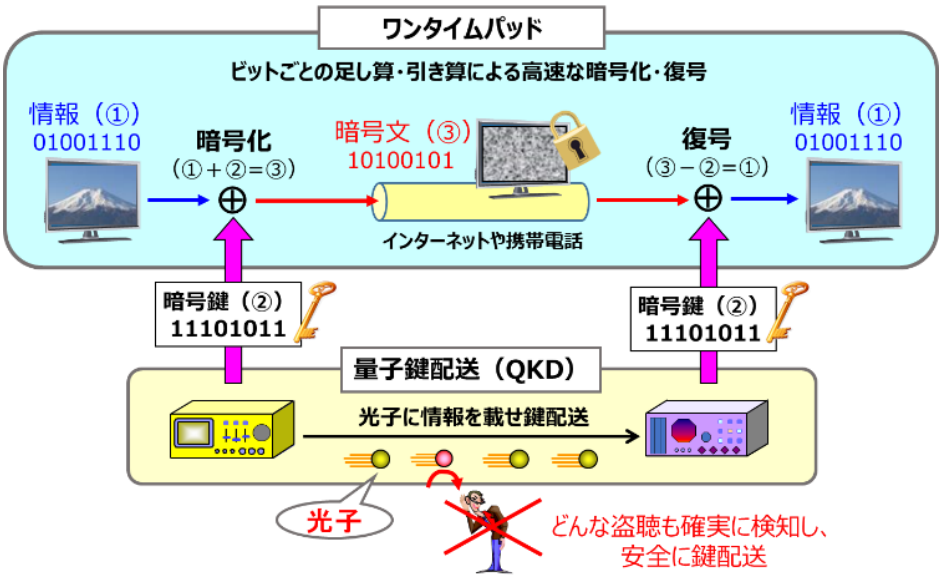


図 3 量子暗号回線の構成

***3 秘密分散**

元のデータを n 個の分散片に変換し、n 個の分散片のうち、k 個がそろわなければ元の情報を復元することができないという符号化手法。

***4 準同型暗号**

鍵を用いて暗号化されたデータに対してある種の演算を行い、さらに、それを復号したものは元々のデータの演算結果となっている暗号を用いて行う秘密計算のこと。

***5 マルチパーティ計算**

データを秘密分散を用いて分割し、物理的に情報を隔離したサーバに格納した状態で計算を行うことで、データの秘匿性を担保する秘密計算の手法。

***6 Fastq**

ゲノム塩基配列とそのクオリティスコアを 1 つのファイルにテキストベースで保存されるデータフォーマット。

***7 VCF**

バリアントコールファイル。ゲノム配列の変異情報を保存するためのデータ形式。

***8 OTP（One Time Pad）方式**

一度使用した暗号鍵を何度も使い回さずに、一度使用したら破棄する方式。情報理論的安全性が得られる。

***9 量子鍵配送**

量子鍵配送（Quantum Key Distribution, QKD）は、通信を行う二者間でのセキュア通信を保証するために、量子力学を用いてランダムな秘密鍵を共有し、それを基に情報を暗号・復号するためのものであり、現在、東芝が製品化を行っている。

https://www.global.toshiba/jp/products-solutions/security-ict/qkd.html

***10 内閣府が主導する戦略的イノベーション創造プログラム（SIP）**

内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。

https://www8.cao.go.jp/cstp/gaiyo/sip/

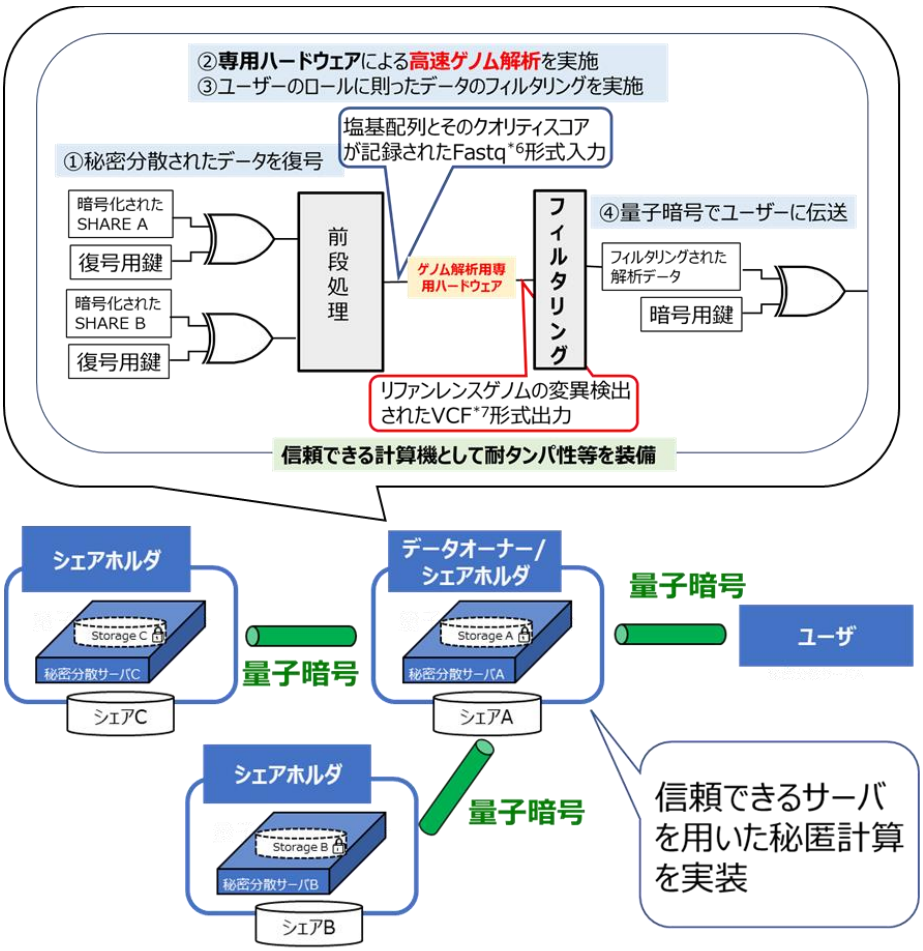
補足資料

今回開発した量子セキュアクラウドシステム

“信頼できるサーバ”を実装した量子セキュアクラウドシステムでは、全ゲノム解析専用サーバを量子暗号ネットワーク上の“信頼できるノード”内に設置し、さらに、認証付きラックなど物理的に厳重にアクセス管理された環境に設置することで、物理的な攻撃に対しての安全性を確保しました（図 4 参照）。また、このサーバの入出力データは OTP 暗号化され、情報理論的安全な秘匿化が施されています。今回は、高速処理を重視し、情報理論的安全性を持ちつつ、高速処理が可能な排他的論理和ベースの秘密分散プロトコルを採用しました。この結果、秘密分散処理では 700 Mbps を超える処理速度を実現しています。また、高速 OTP 装置では 2 Gbps の処理速度を実現しています。

排他的論理和ベースの秘密分散の定義:

R(random number)=$R_U||R_L$, S(secret data)=$S_U||S_L$



$$A = (S_U \oplus R_U \oplus R_L) \| (S_L \oplus R_L)$$
$$B = (S_U \oplus R_U) \| (S_L \oplus R_U \oplus R_L)$$
$$C = R_U \| R_L$$

図 4 量子セキュアクラウドの構成図

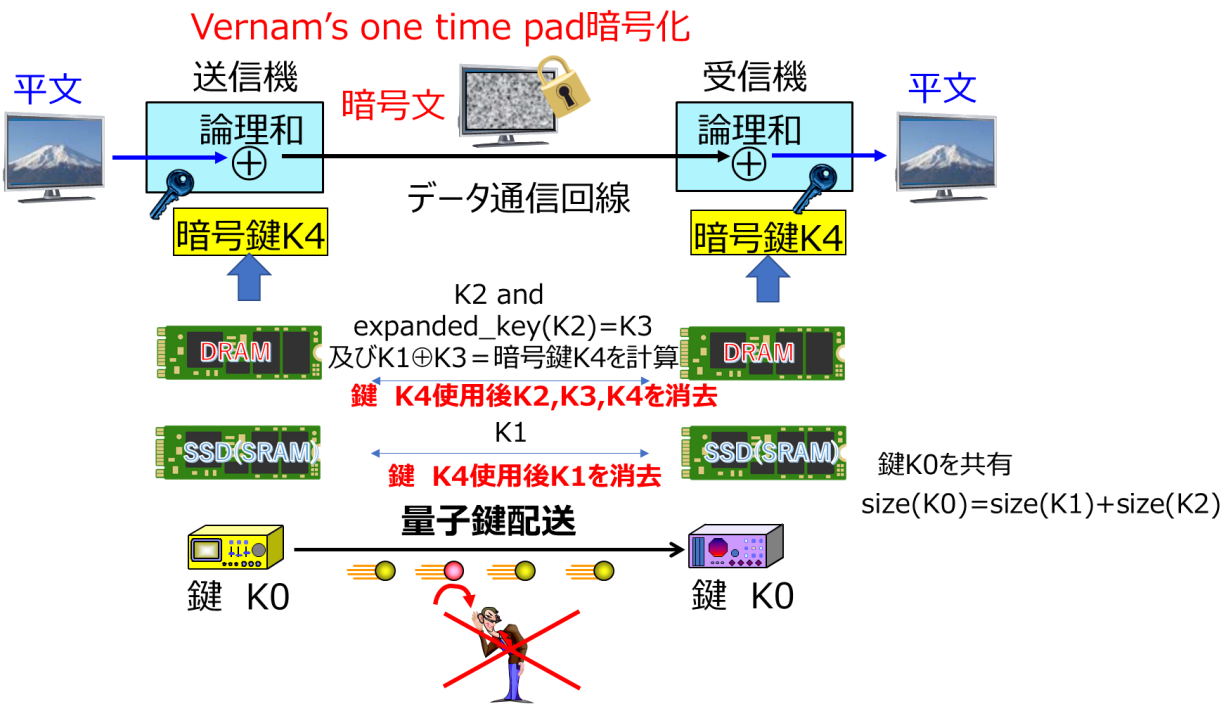


図 5 鍵データの安全な消去システム

さらに、OTP 暗号化用鍵データを保管する長期記憶媒体への直接的なプロービング攻撃に備え、使用後の鍵データを完全に消去できるシステムも採用しています。図 5 に示すように、暗号用の鍵を確実に消去できる DRAM 上に生成し、確実な消去を実現しています。

＜ 本件に関する問合せ先 ＞
国立研究開発法人情報通信研究機構
未来 ICT 研究所 小金井フロンティア研究センター
量子 ICT 研究室
藤原 幹生
E-mail: fujiwara@nict.go.jp

京都大学 学際融合教育研究推進センター
スーパーグローバルコース医学生命系ユニット
京都大学大学院医学研究科附属ゲノム医学センター
長﨑 正朗
E-mail: nagasaki@csml.org

株式会社東芝
研究開発センター
E-mail: inquiry@rdc.toshiba.co.jp

株式会社 ZenmuTech
広報・マーケティング担当
松倉 泉
E-mail: info@zenmutech.com

＜ 広報（取材受付）＞
国立研究開発法人情報通信研究機構
広報部 報道室
E-mail: publicity@nict.go.jp

京都大学
総務部広報課国際広報室
E-mail: comms@mail2.adm.kyoto-u.ac.jp

株式会社東芝
コーポレートコミュニケーション部
メディアコミュニケーション室
E-mail: media.relations@toshiba.co.jp

株式会社 ZenmuTech
広報・マーケティング担当
松倉 泉
E-mail: press@zenmutech.com