資料4－5

量子通信・量子暗号の動向と展望

光子の状態を制御
⇒
・微弱光でも超長距離通信を実現（量子通信）
・どんな計算機でも解読できない暗号通信を実現（量子暗号）

情報通信研究機構 未来ICT研究所
主管研究員　佐々木雅英

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

技術の現状

・中国が低軌道衛星(600kg)で
量子暗号を実証
・NICTが50kgの低軌道衛星で
量子通信を実証
・ドイツが静止軌道衛星で
超高感度コヒーレント通信を実証

・中国が2000km量子暗号網を構築、
国営企業が利用開始
・大手通信キャリアが実証試験を開始
（韓国SKT、英国BT、スペインTelefonica等）
・韓国SKTがベンチャー企業のIDQを買収
・東芝、NECが世界最高速の装置を開発済

（補足資料、参照）

量子暗号、量子通信の
長距離化に向けて基礎
研究を各国が推進中

量子中継

衛星による量子
通信・量子暗号

量子暗号

“Struggle for Life” in a Sea of Technical and Entrepreneurship Risk, L. M. Branscomb

量子暗号に関する日本の現状

ü **世界最高速の量子暗号装置を開発済み**

海外製の10倍高速、2倍長距離

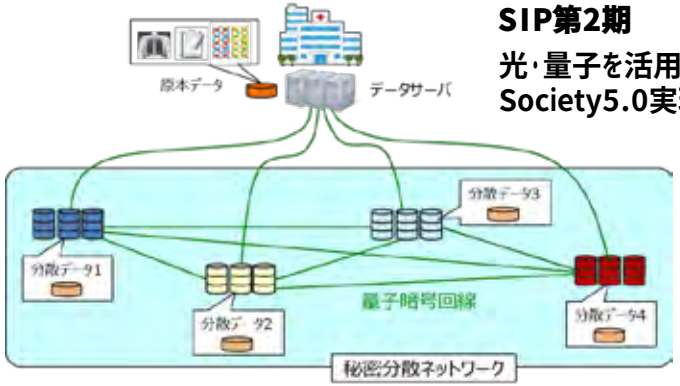
NEC
100kbps@45km

送信機　受信機

東芝
300kbps@45km

送信機　受信機

ü **新たなキラーアプリ『量子セキュアクラウド技術』を開発中(量子暗号x秘密分散)**



SIP第2期

光･量子を活用した
Society5.0実現化技術

ü **国際標準化を主導中**

国際電気通信連合(ITU)において日本、韓国、スイス、中国などが量子暗号ネットワークの勧告草案を編纂中

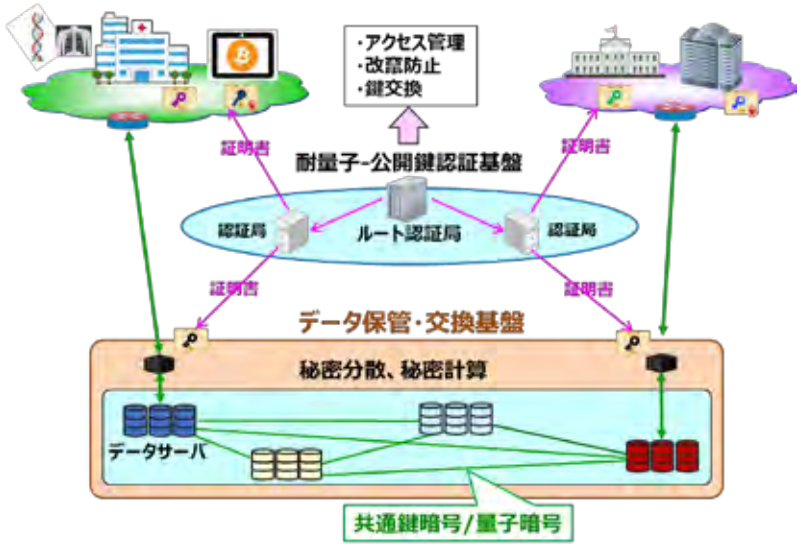
まずすべきこと

Ø 装置の市場投入と量子暗号サービスの開始

政府がアーリーアダプターとして、機密情報をやり取りする部署間に導入を検討すべき時期

今後の課題

Ø 量子暗号、秘密分散、秘密計算、耐量子-公開鍵暗号を統合する**分野横断的取り組み**を推進し新たな『**量子セキュリティ技術分野**』を創出



Ø SINET等を活用し拠点化、試験運用、人材育成
Ø 重要インフラ技術と融合し輸出産業化
Ø 安心・安全『日本ブランド』で市場シェア拡大

衛星量子通信・量子暗号

・宇宙は真空なので、遥か彼方まで光子が届く ⇒ 大陸間での量子暗号
・光は電波の10万倍の帯域を持ち、ライセンスフリー

衛星通信網、地球観測網を支える技術としてこれから市場が拡大

・米国、中国、カナダ、ドイツ、スイス、オーストラリア、シンガポールの各国、及び欧州宇宙機関が関連プロジェクトを推進中
・日本では総務省プロジェクトで衛星向け量子暗号技術の研究開発を推進（2018年から5年間、 NESTRA, SONYコンピュータサイエンス研究所、スカパーJSAT、NICT、東大が、航空機で実証試験を計画）

- **今後、光通信・量子暗号・光学センサを搭載した衛星を開発し、複数機打ち上げ ⇒ 2025年頃までに実現できれば、衛星コンステレーション市場で主導権を握れる**
- **2030年頃、衛星網と地上網を統合、量子セキュリティインフラをグローバル化**

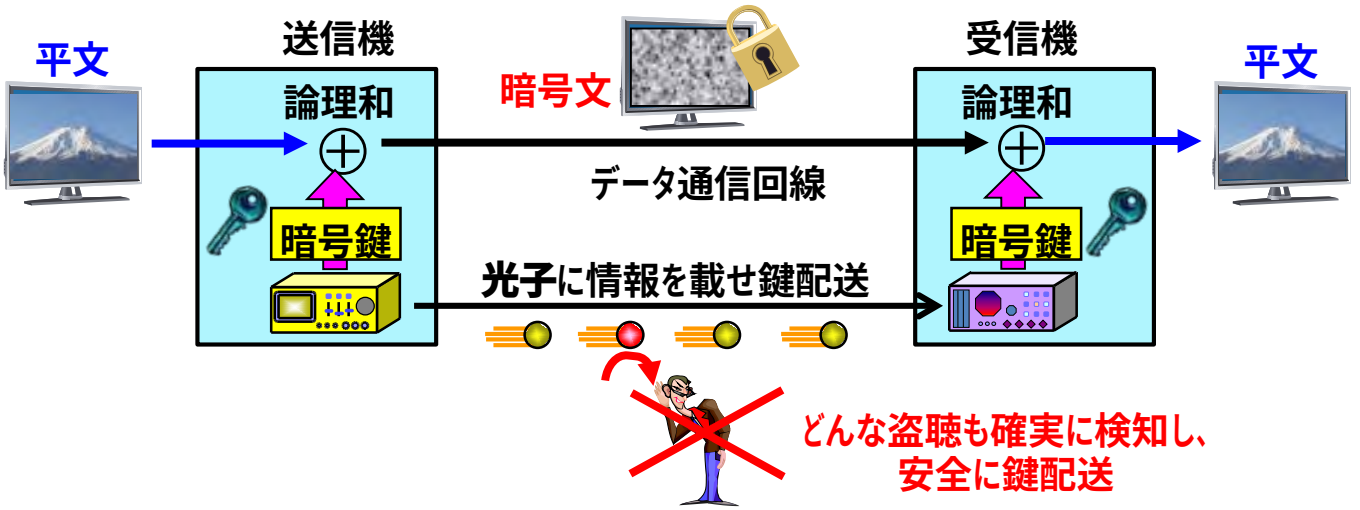
補足資料

量子暗号とは

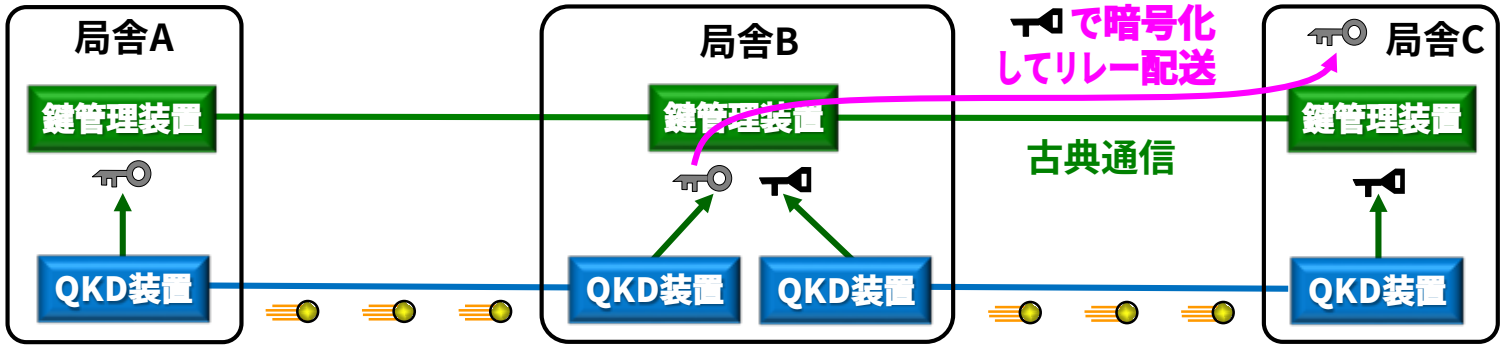
①光子一個一個に乱数情報を載せて伝送、2地点間で同一の鍵を共有
量子鍵配送（Quantum Key Distribution: QKD）

②平文と同じサイズの鍵で暗号化、一回一回使い捨て：**ワンタイムパッド（OTP）**

⇒どんな計算機でも解読できない暗号通信を実現（情報理論的安全性）



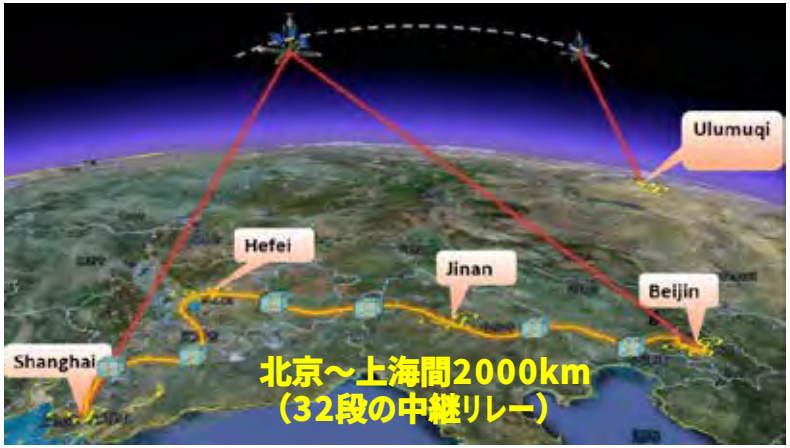
ネットワーク化は『**信頼できる局舎**』を介した鍵のバケツリレーで実現



量子暗号分野の動向

中国の躍進

・2017年7月、衛星量子暗号を世界で初めて実証
・2018年3月、世界最大の量子暗号ネットワークを構築
⇒新華社通信、中国工商銀行、国家電網公司などが利用。
重要インフラ網を他国のサイバー攻撃から防御する狙い
Q. Zhang et al., Opt. Express 26, 24260 (2018).



図は中国科学技術大学, Q. Zhang氏のご好意による

2018年、大手通信キャリアが投資を開始

・2月、SK Telecom（韓国）がジュネーブ大発のベンチャーID Quantique社に$65M（71億円）出資。５Gのセキュリティインフラ市場を狙う。
https://www.idquantique.com/id-quantique-sk-telecom-join-forces/

・3月、ブリティッシュテレコムが英国初の量子暗号網をCambridge ~ Ipswich間に構築。
https://www.advaoptical.com/en/newsroom/press-releases/20180613-adva-fsp-3000-powers-uks-first-quantum-network

・6月、テレフォニカ，ファーウェイ，マドリード工科大学が商用網で量子暗号の実証試験を開始。
https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S01_WORLD_TOUR/UNIofYORK_SPILLER.pdf

・6月、米Quantum Xchange社がWall Street金融市場向けに量子暗号サービスを発表。
https://quantumxc.com/

・7月、ドイツテレコムの実証通信網にSK Telecom、IDQが量子暗号システムを提供。
https://www.zdnet.com/article/sk-telecom-applies-quantum-key-to-deutsche-telekom-network/