量子暗号・量子通信研究開発の最前線

情報通信研究機構 未来ICT研究所
量子ICT先端開発センター
武岡 正裕

国立研究開発法人
情報通信研究機構

量子暗号・量子通信

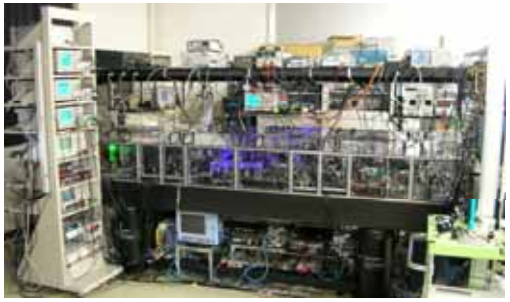
量子通信

本日の話

- 量子暗号
  - 超秘匿セキュリティ技術
- 量子中継ネットワーク（量子通信）
  - 大規模量子暗号ネットワーク
  - 分散量子情報処理プロトコル
  - 超精密時刻同期・・・
- 量子符号化通信
  - 超大容量通信
  - 深宇宙大容量通信

フィールド実証
～実用フェーズ

基礎研究フェーズ



内容

1. 導入：暗号の役割と現代暗号の安全性

2. 量子暗号の仕組みと安全性

3. 国内外の研究開発動向

4. 量子暗号の応用
   → 現代セキュリティ技術との融合

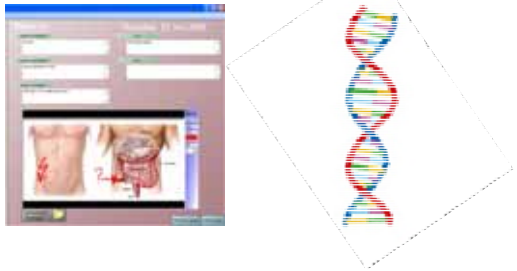
5. まとめ：社会実装に向けて

背景

様々な重要情報がデジタル化されて、
データサーバ上に永遠に保存され続ける時代

・企業競争力の源泉となる製造
ノウハウ、技術情報、経営情報

・個人の生体認証データ、
医療・ゲノム情報



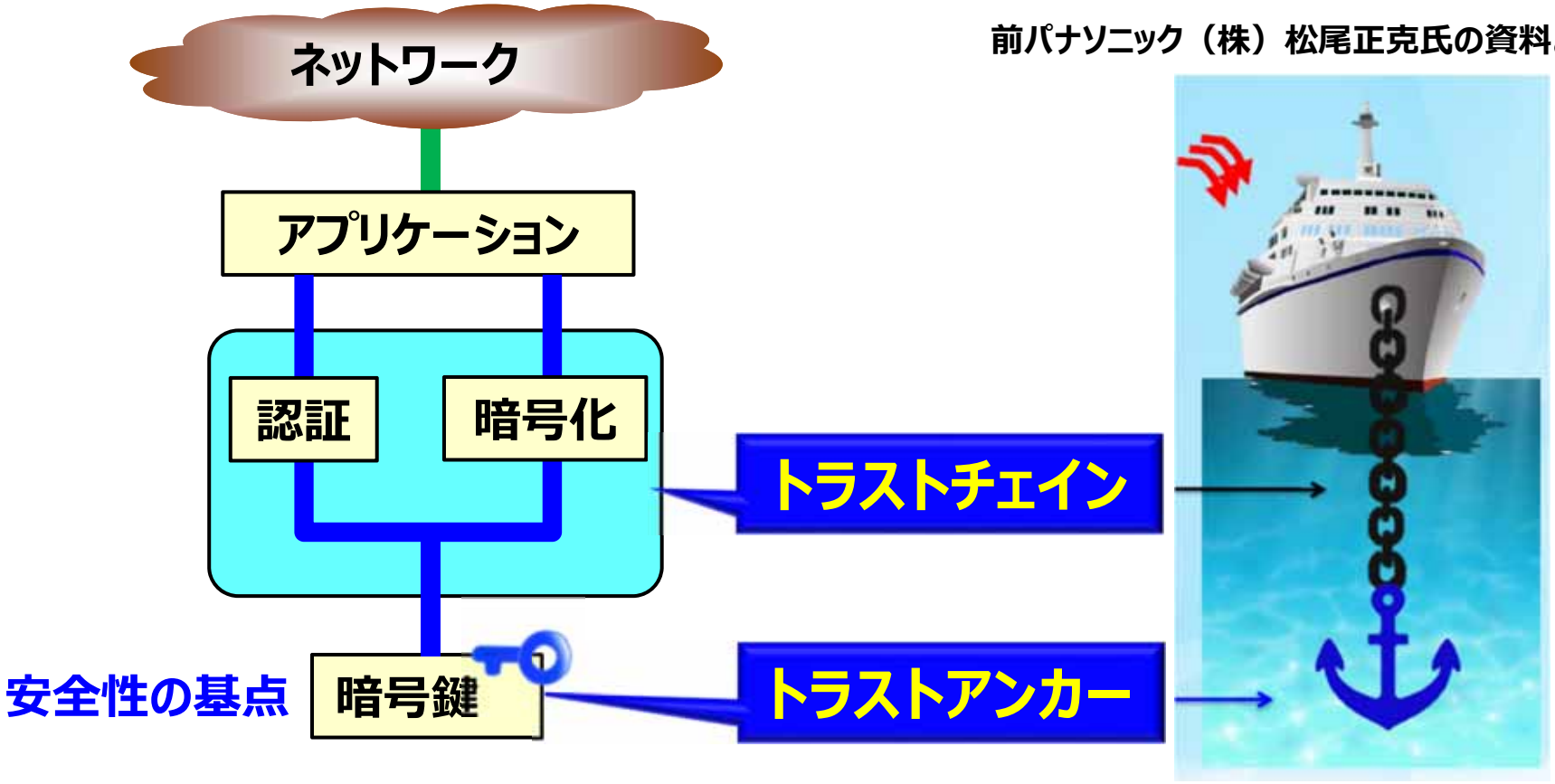
一度漏洩すれば
・複数の世代、複数の家系にわたり生命を脅かすリスク
・社会・経済活動に深刻な影響を及ぼすリスク

世紀単位の安全性確保が必要

安全性の基点

暗号とは相手を認証，文書の改竄を防止，情報を秘匿化

サイバーセキュリティ対策の骨格を形成



前パナソニック（株）松尾正克氏の資料より転載

トラストアンカー，トラストチェインの明確なシステムは
ハッカーにとって攻撃しづらい！

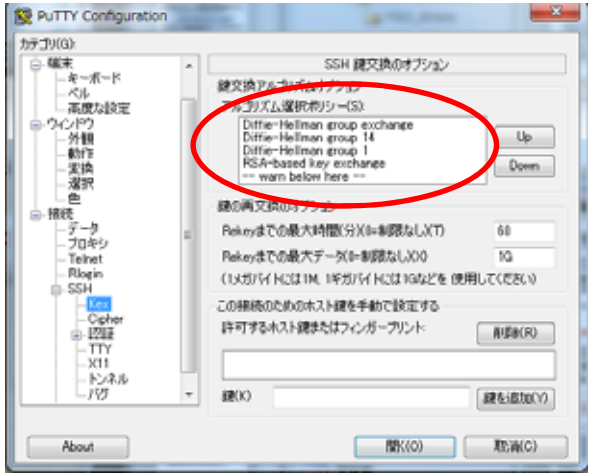
現在の暗号方式

○現在の主流暗号システムにおけるトラストアンカー（暗号鍵）
⇒ 計算アルゴリズムに立脚

・擬似乱数
・公開鍵暗号 ⇒ **「計算量的安全性」**

計算量的安全性：解読の計算困難さにより
安全性を保証する方式

例：RSA暗号・・・素因数分解の困難さ



公開鍵暗号
使用の例

○計算機能力・アルゴリズムの進歩による危殆化の恐れ

・量子計算機が実現すれば瞬時に解読可能に
・スパコン等の進歩により、各方式の寿命は１０～１５年程度
・数学アルゴリズムの進化により

量子コンピュータ開発の活発化

○1994年、Shorが素因数分解アルゴリズムを提案

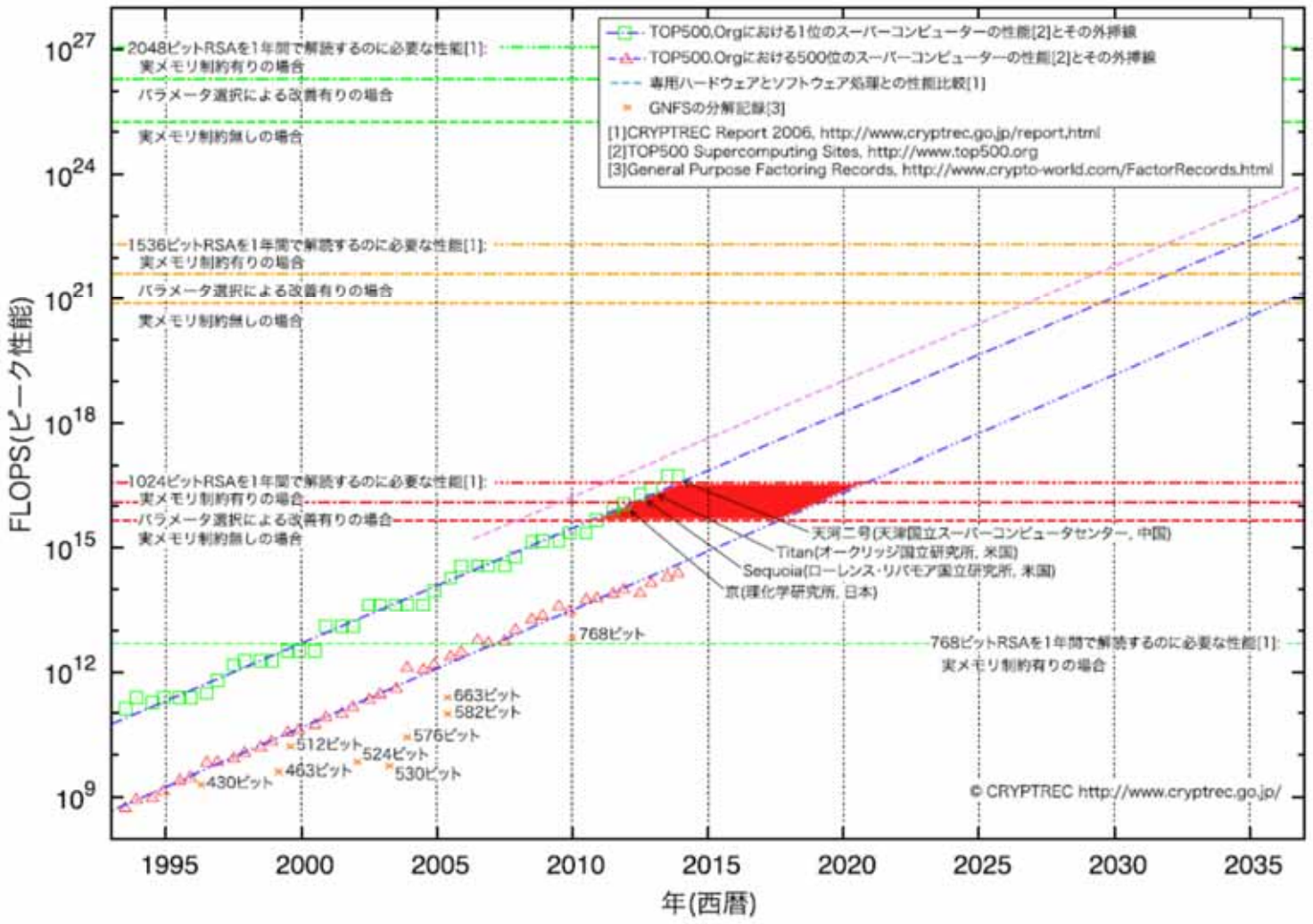
⇨ 実現すれば現代暗号の脅威に

○最近では、世界各国の産学官が積極的に開発を推進

最新動向と展望は本セミナー前半の通り

スーパーコンピュータの進展

例：RSA暗号解読に必要な計算量



CRYPTREC report 2013

内容

1. 導入：暗号の役割と現代暗号の安全性

2. 量子暗号の仕組みと安全性

3. 国内外の研究開発動向

4. 量子暗号の応用
   → 現代セキュリティ技術との融合

5. まとめ：社会実装に向けて

量子暗号とは

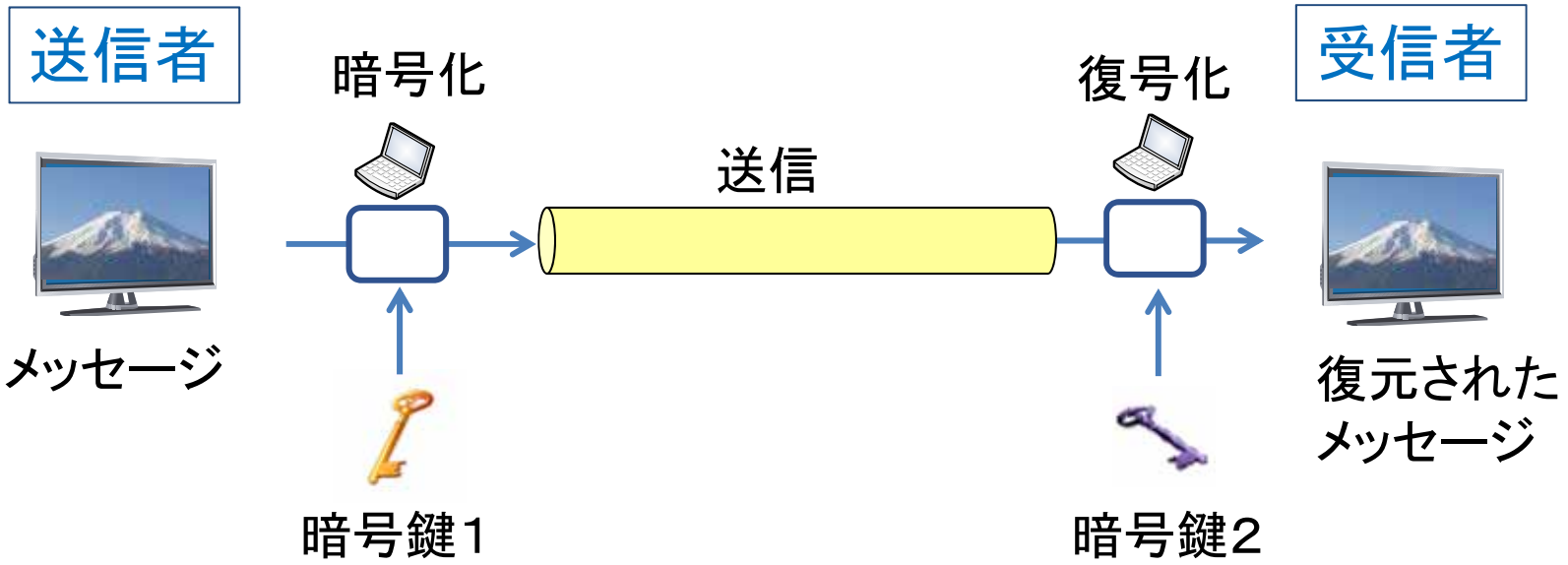
「（量子計算機を含む）どんな計算機でも解読できない」ことを証明できる現在唯一の暗号方式*

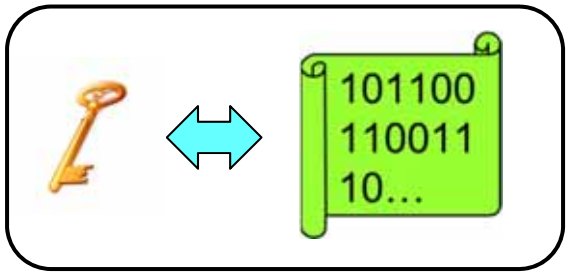
1．情報理論的安全性
→ あらゆる計算機を使っても解読不可
（例え量子計算機を使ったとしても）

2．（鍵共有）通信路への盗聴攻撃に対する安全性
→ あらゆる盗聴攻撃を検知

*ただし直接手渡しを除く

暗号化通信





暗号鍵 ＝ ランダムビット列

**暗号：離れたユーザー間で
いかにして安全な鍵
（ランダムビット列）を作るか**

（暗号鍵1と2が同一：対称鍵暗号
暗号鍵1と2が異なる：非対称鍵暗号）

暗号の安全性

暗号の安全性 ⇔ 鍵（ビット列）の乱数性

従来暗号（数理アルゴリズム）で作られる鍵：

擬似乱数列：　0100111001001110・・・

なんらかの周期性・規則性を持つ

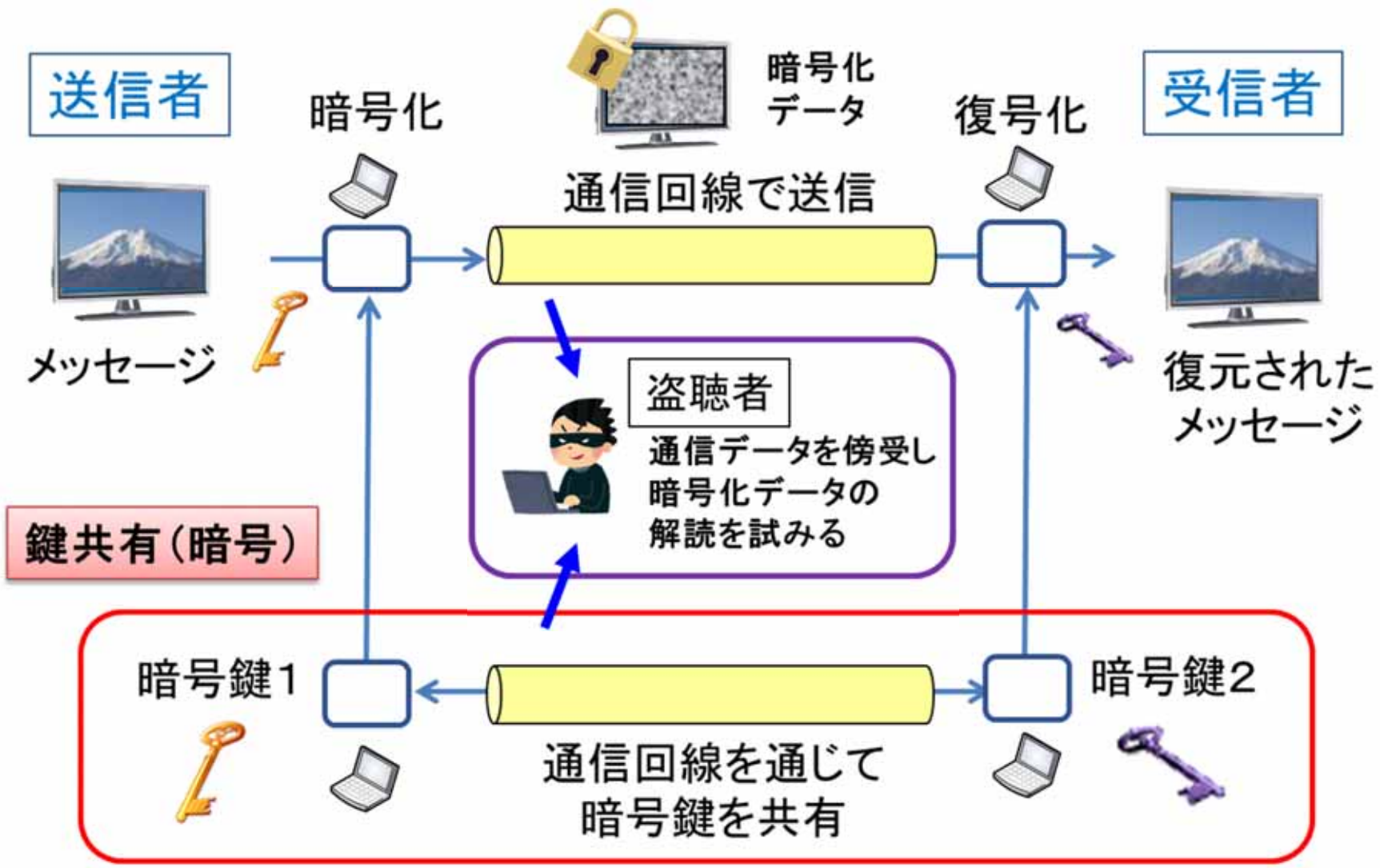
⇒ コンピュータによる解読で鍵を予測される可能性
（例：RSA暗号の解読 ⇔ 素因数分解）

量子暗号で作られる鍵：

真性乱数（物理乱数）：100101001001110・・・

物理現象から作られる真の乱数 ⇒ 原理的に解読（予測）不可能！

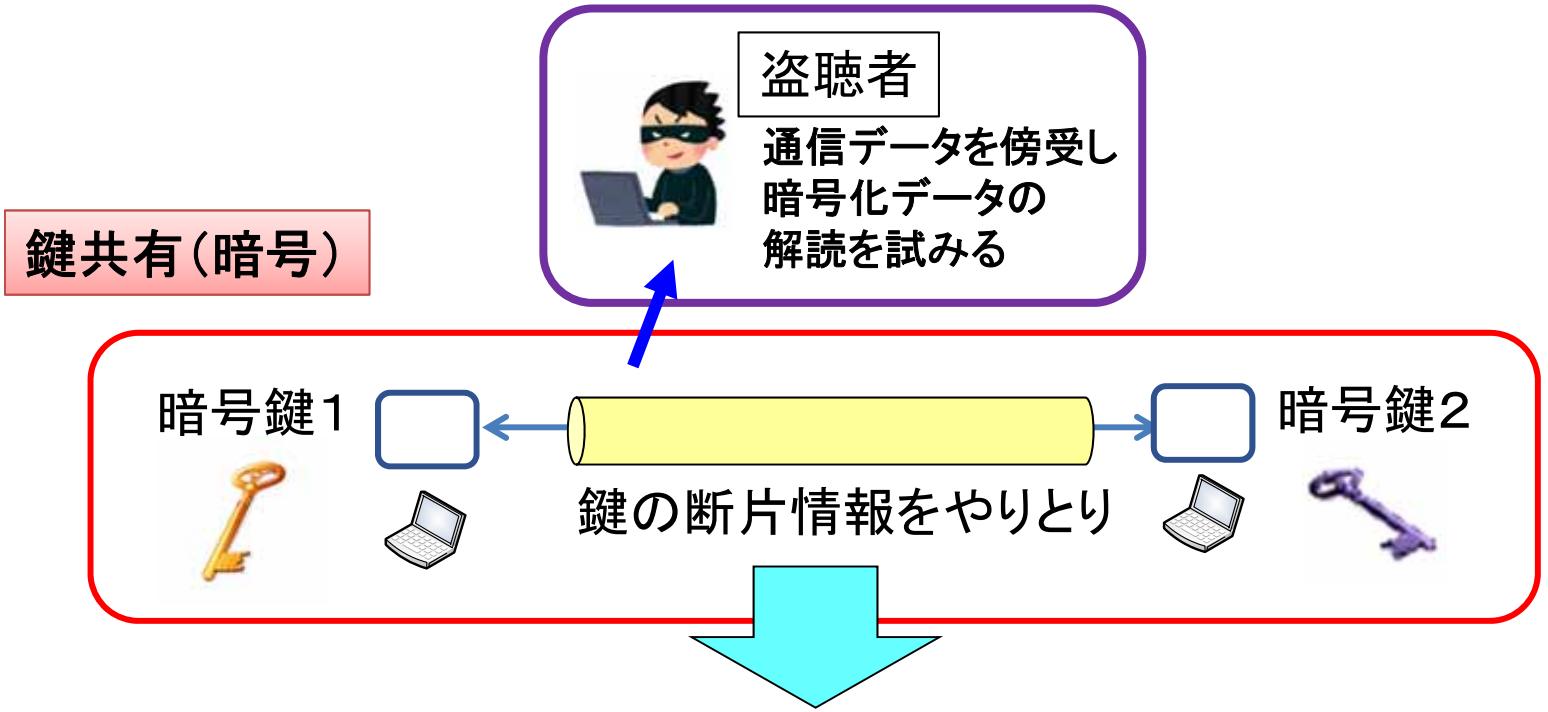
暗号と盗聴者



（暗号鍵1と2が同一：対称鍵暗号
暗号鍵1と2が異なる：非対称鍵暗号）

従来暗号（公開鍵暗号）

従来暗号：鍵共有する際の通信を盗聴されても構わない



鍵の断片情報を通信して鍵を共有

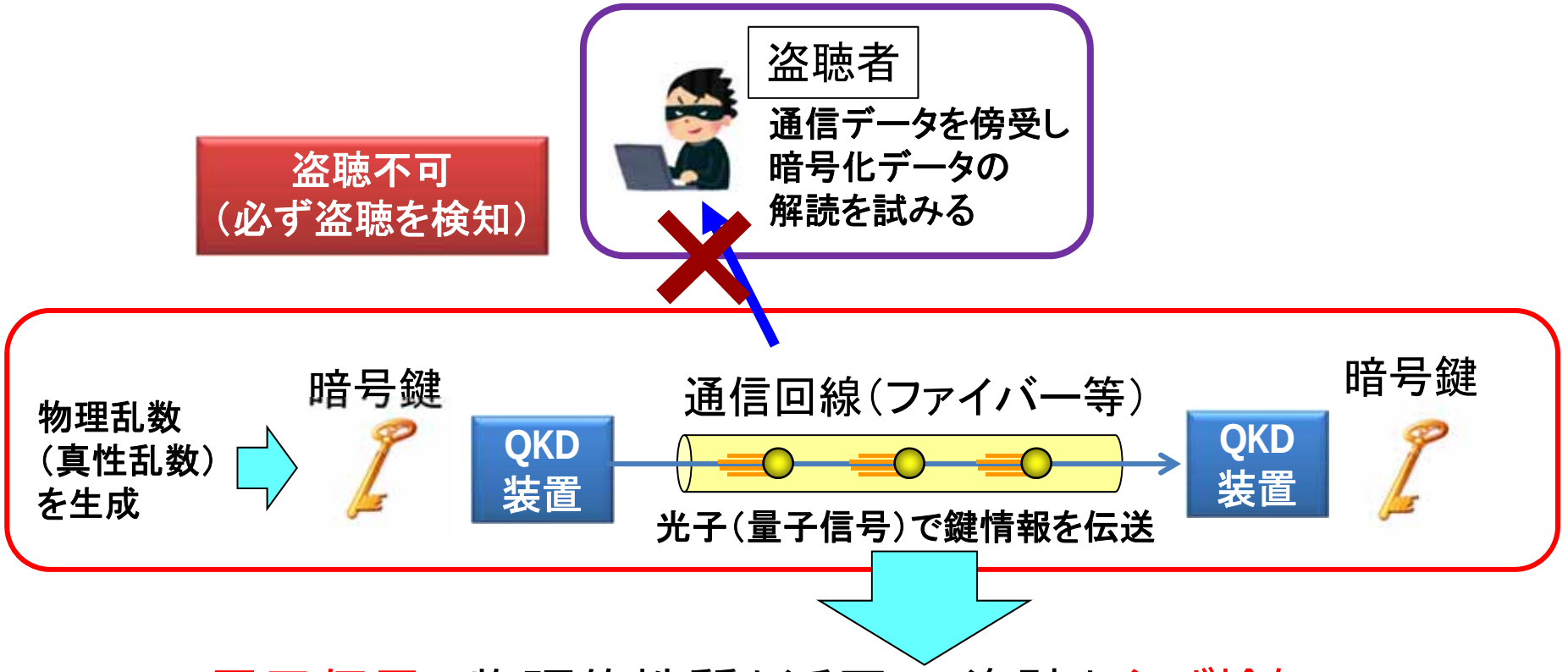
鍵情報の推測は計算量的に困難

例：素因数分解の困難さ

→ 次世代スパコン、量子コンピュータ等による解読の危険性

量子暗号の場合

「量子鍵配送装置（QKD）」により鍵を共有
→ 鍵共有する際の通信の盗聴を許さない　QKD: Quantum Key Distribution

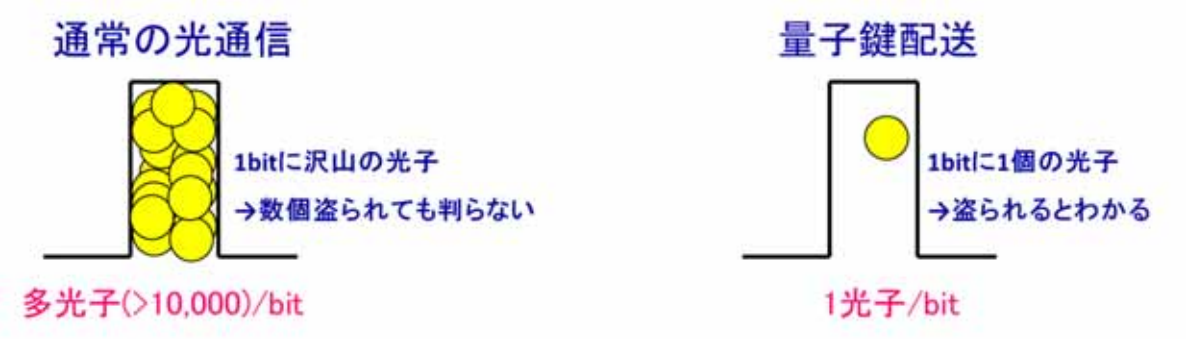


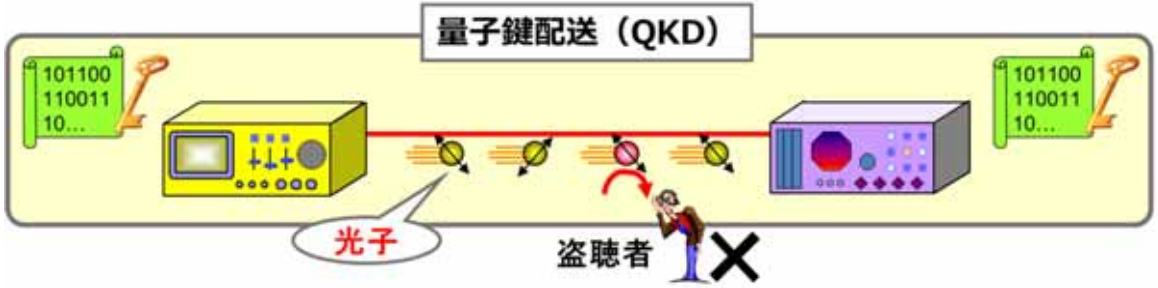
量子信号の物理的性質を活用し、盗聴を必ず検知

盗聴の恐れの無い真性乱数を鍵として使用

QKD:盗聴検知の仕組み

- 光通信技術の延長
- 光子を伝送することにより盗聴を検知



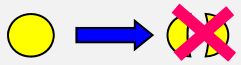


- あらゆる物理的な盗聴攻撃を検知できる
  (光子の分割不可能性、不確定性原理を活用)
  → *盗聴者は鍵を秘密裏に盗むことが不可能*

- QKDの鍵で暗号化されたデータは、
  あらゆる計算機を使っても解読不可能
  (物理的に作られた乱数は「真の乱数性」を持つ)
  → *計算機による解読は不可能*

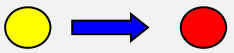
光子の量子力学的性質

1. 光子は粒子の最小単位（量子）
   （これ以上分割が不可能）



⇒光子を盗むと受信側に届かない

2. 光子の観測・増幅等の作用は
   光子状態を必ず変化させる
   （不確定性原理）



⇒盗み見る行為による状態変化を
受信側で検知できる

量子暗号の誕生からフィールド実証へ

1984年、BennettとBrassardが量子暗号を初めて提案

BB84方式：単一光子を使った方式

物理学分野を中心に基礎研究が進展

実装の問題点：単一光子の生成は技術的に難しい
（レーザー光は光子数がポアソン分布で直接は使えない）

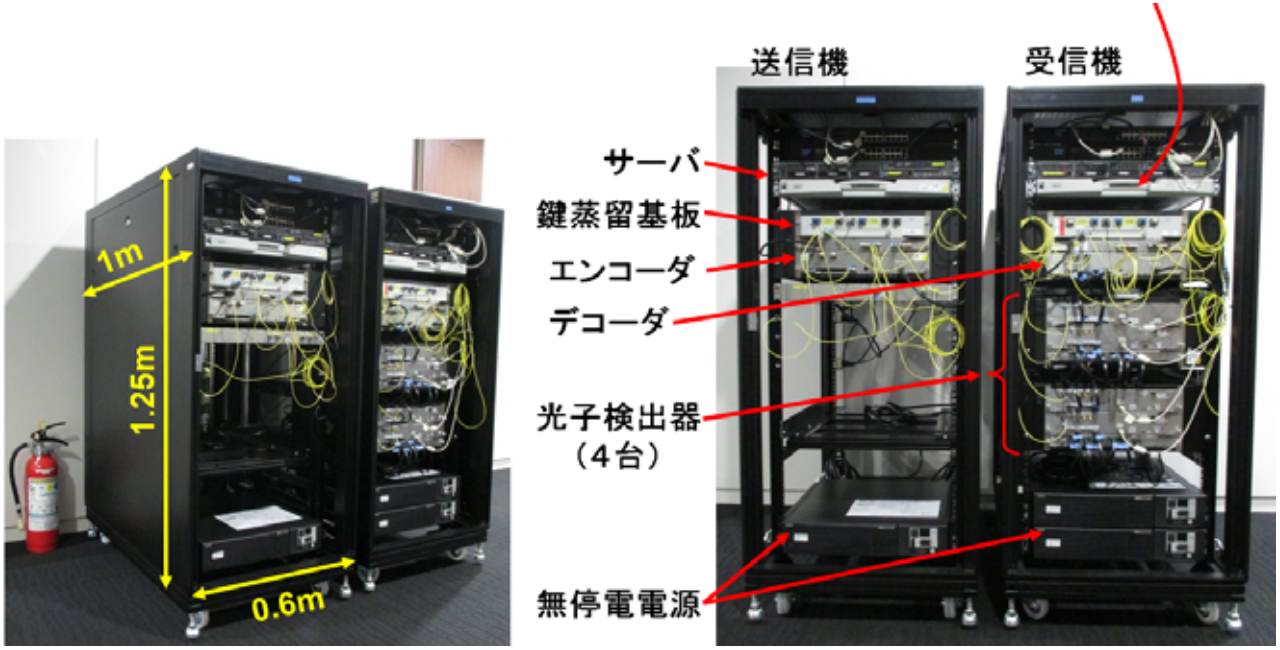
2003-2005年、理論研究のブレークスルー

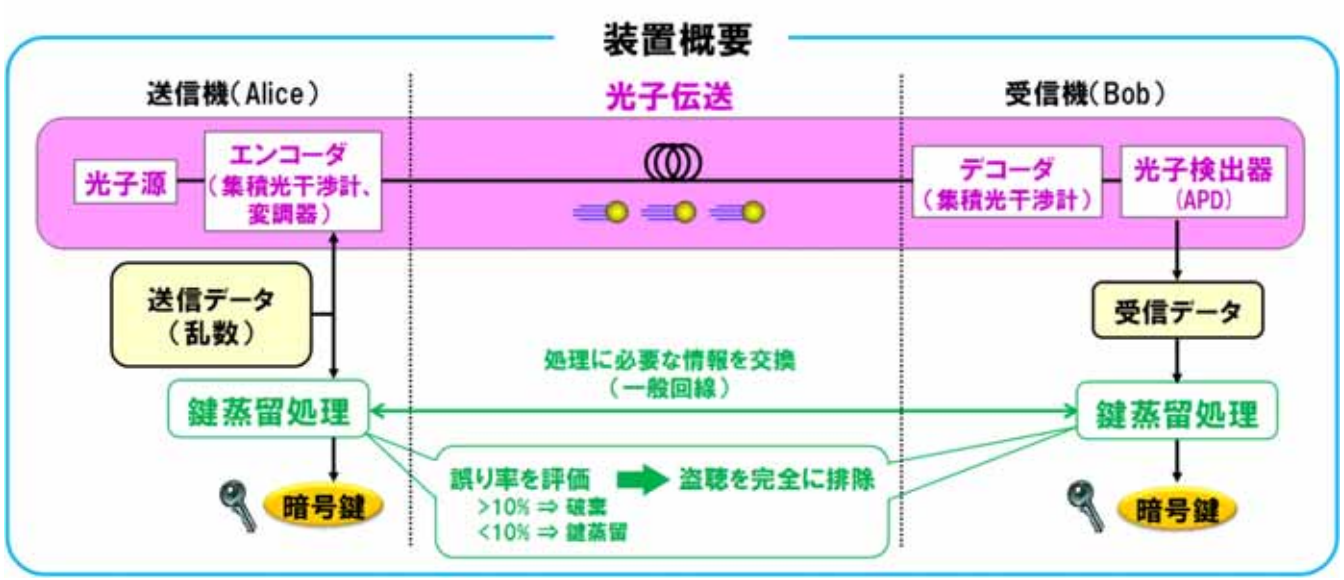
レーザー光源で単一光子並みの性能を実現する方式の提案
（デコイBB84方式）

平均光子数が1以下の超微弱なレーザー光を使用
→ 光通信技術を活用した実装が可能に。

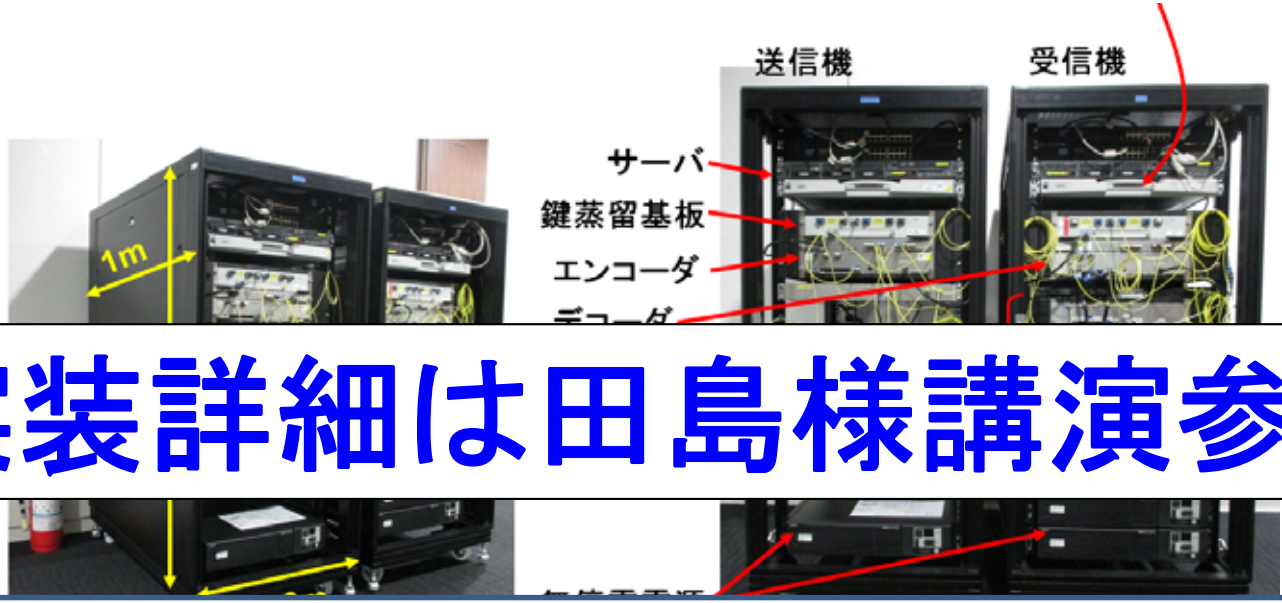
装置開発・実証実験のフェーズへ

QKDシステムの実装例（NEC社開発事例）



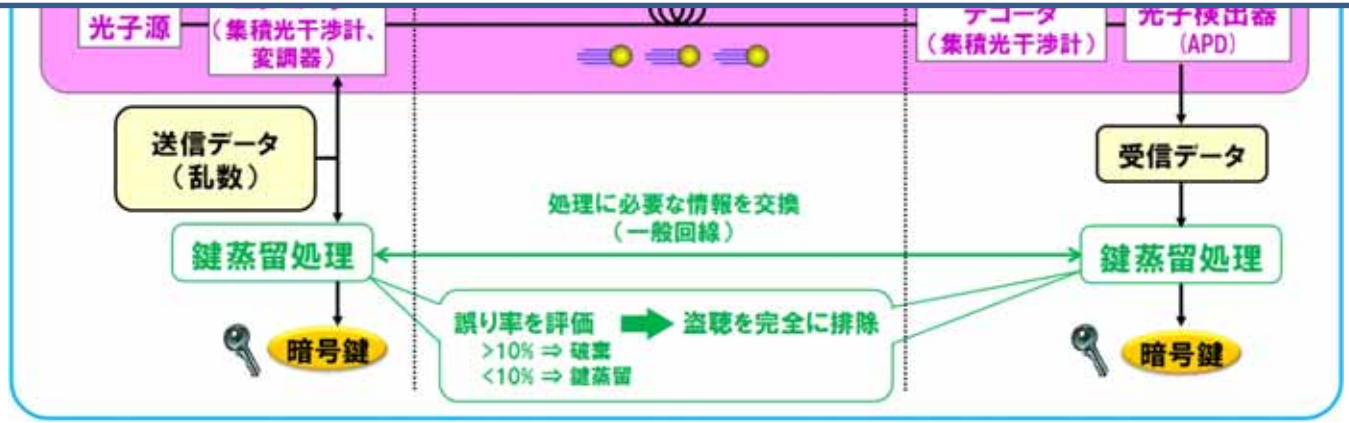


QKDシステムの実装例（NEC社開発事例）



実装詳細は田島様講演参照

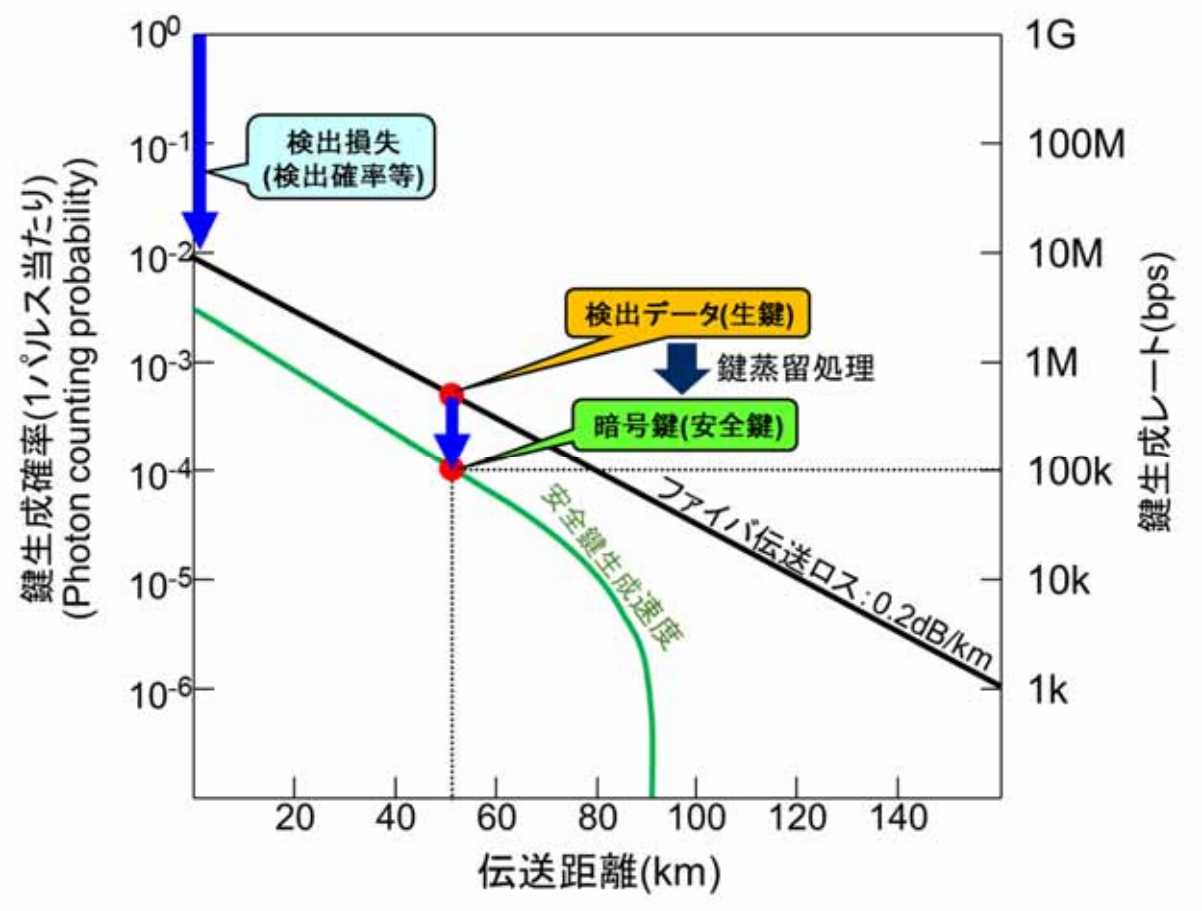
〇ハードウェア：最先端光通信技術＋光子検出器
〇ソフトウェア：QKD特有のデータ処理技術を実装



技術的な制限：鍵生成速度

・光子のほとんどはファイバーや検出器の損失で失われる
・中継増幅器は量子状態を破壊するため使えない

⇒ 鍵の伝送距離・速度が制限される



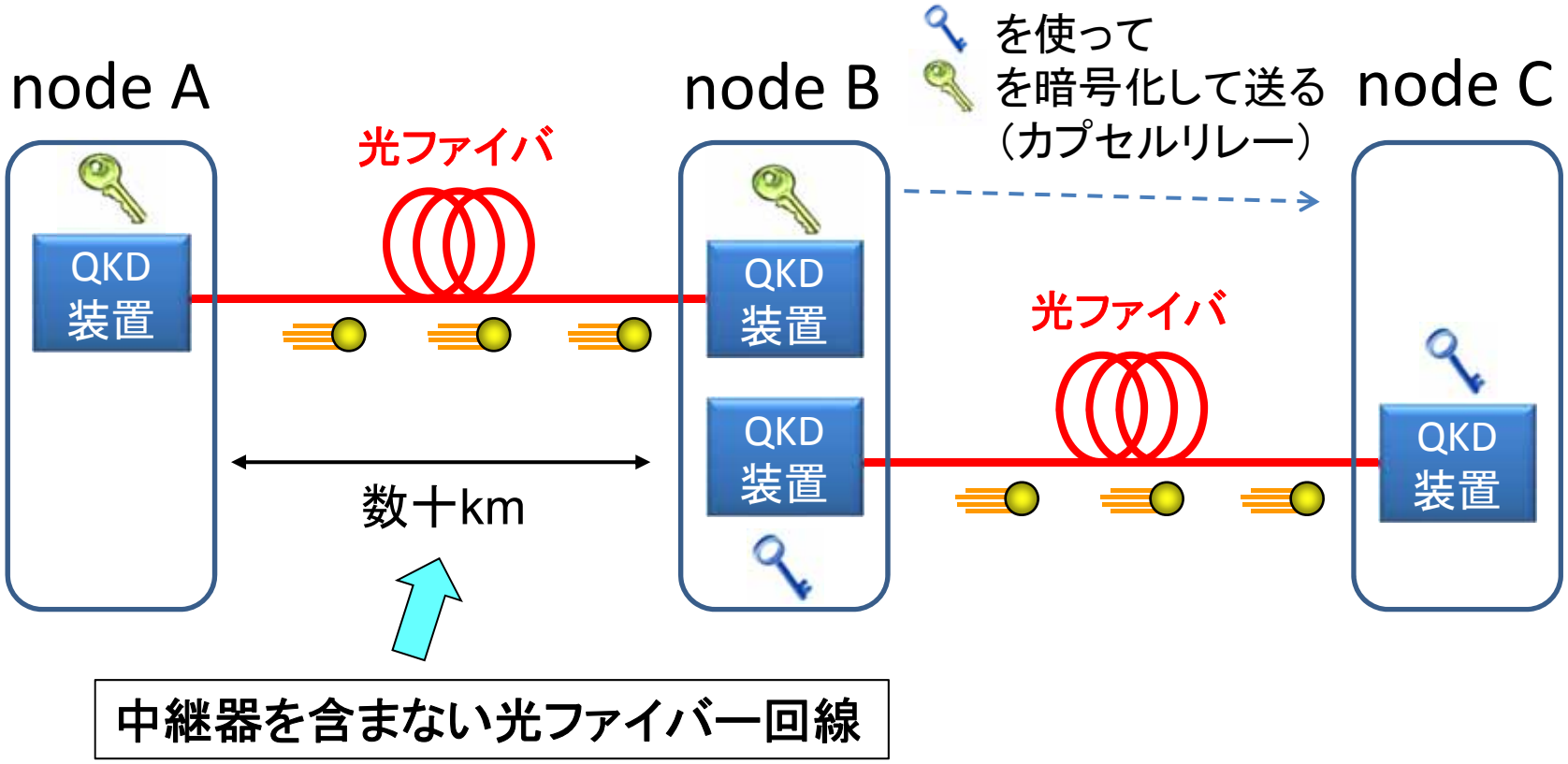
典型的な鍵生成速度

距離50km程度で
鍵生成速度は
1波長あたり
数十～数百kbps程度

＊但し通信条件、各機関の装置の性能などに依存して大きく変動することに注意

長距離化･ネットワーク化（現在の方法）

- Trusted node（信頼できる局舎）



安全が確保されたな局舎を介して鍵をリレーする

内容

1. 導入：暗号の役割と現代暗号の安全性

2. 量子暗号の仕組みと安全性

3. 国内外の研究開発動向

4. 量子暗号の応用
   → 現代セキュリティ技術との融合

5. まとめ：社会実装に向けて

QKD研究開発の動向

（1） 地上QKDネットワーク

（2） 衛星QKD

各国のQKDネットワーク実証

米国 2004 DARPA Quantum Network (Boston)

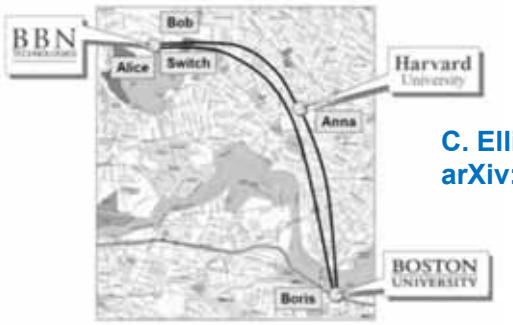


Figure 11: Logical Map of the Cambridge-Area Fiber Network.

C. Elliot et al., arXiv:quant-ph/0503058

欧州 2008 SECOQC Network (Vienna)

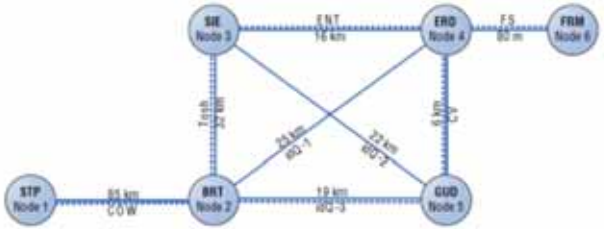
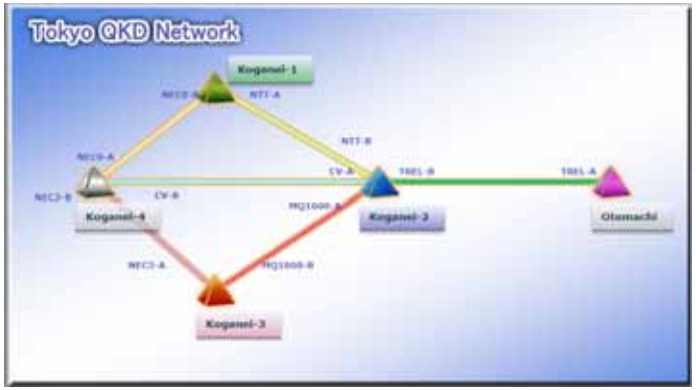


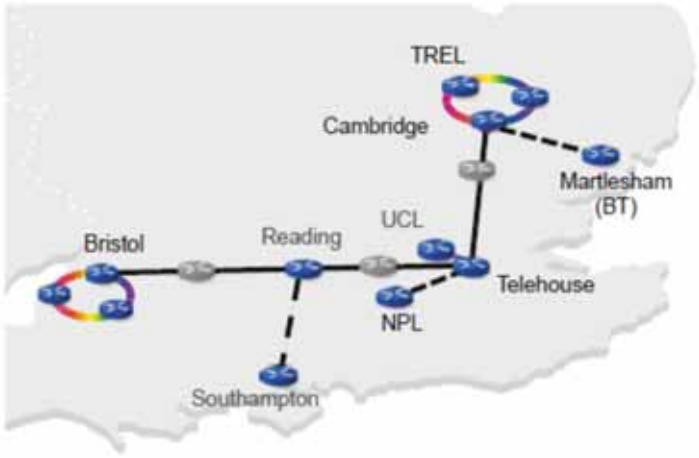
Figure 2. Network topology of the SECOQC QKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.

M. Peev et al., New J. Phys. 11, 075011 (2009)

日本 2010～現在 Tokyo QKD Network (Tokyo)



英国 UK quantum network（Cambridge-Bristol, 建設中）

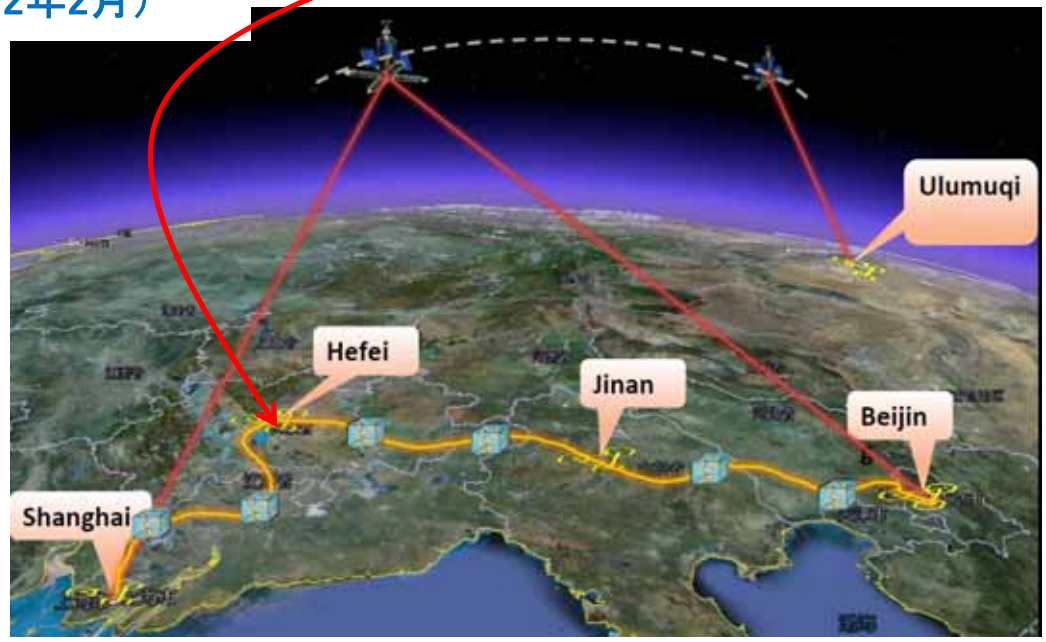


各国のQKDネットワーク実証

中国　世界最大のQKDネットワークを構築

（「量子バックボーンネットワーク」2017年運用開始）

新華社通信実利用計画の
プレスリリース（北京、2012年2月）

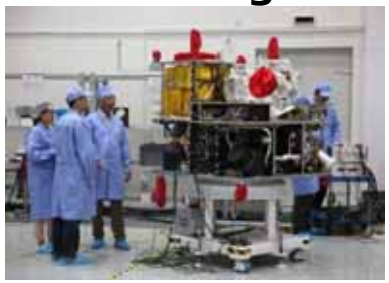


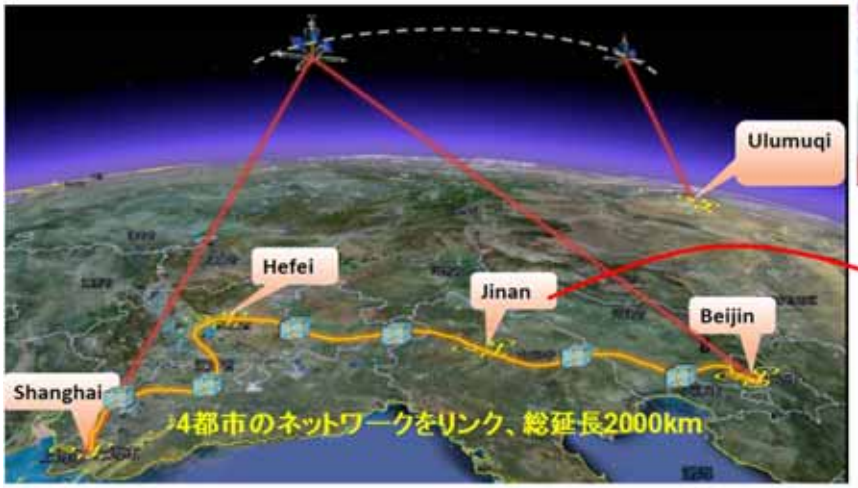
- 巨額国家予算（5年300億円）
- 北京ー上海間2000kmの
  バックボーン＋50ノード級の
  都市圏ネットワーク
- 企業による試験利用
  （新華社、中国工商銀行）
- ベンチャー企業の立ち上がり
  （Quatnum Ctek, QTEC,
  CAS Quantumnet, etc.）

韓国　SKテレコムがスイスの量子暗号ベンチャー企業（ID Quantique）に大型出資し、協業開始

中国の動向

量子科学技術衛星
600kg





http://news.xinhuanet.com/english/china/2012-02/21/c_131423541.htm

50ノード級の都市圏量子暗号ネットワーク

科学技術覇権の確立に向けた長期的国家戦略のもと巨額の国家予算を投入(5年で300億円)。

衛星通信網、電力網、金融網などの重要インフラを先進国の盗聴攻撃から防御。

⇒ ・2017年7月、衛星量子暗号を世界で初めて実証
・2018年1月、衛星量子暗号により中国と欧州の地上局間で鍵共有に成功
・2018年3月、世界最大規模の量子暗号ネットワークの運用を開始

⇒国営企業が試験利用（新華社通信、中国工商銀行、国家電網公司など）

⇒ベンチャー企業が製品化（Quantum Ctek, CAS Quantumnetなど）

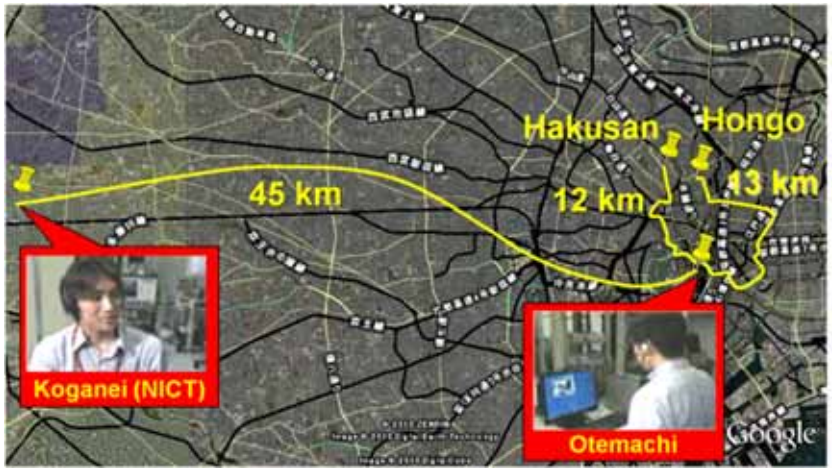
⇒中国独自に標準化戦略を推進

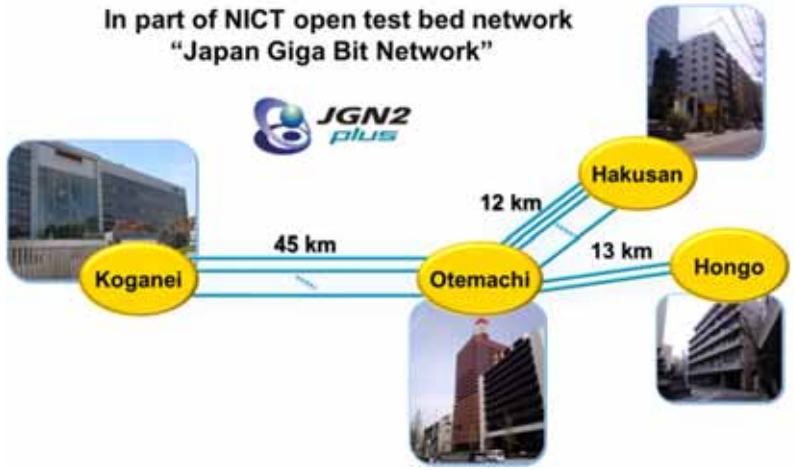
国内：China Communication Standard Association、国際：ISO/IEC

海外帰国組のリーダーのもと15年にわたる継続的な取り組み ⇒

東京QKDネットワーク

・2010年にテストベッド「東京QKDネットワーク」を構築。
NICT委託研究参画機関を中心に、フィールド実証を実施

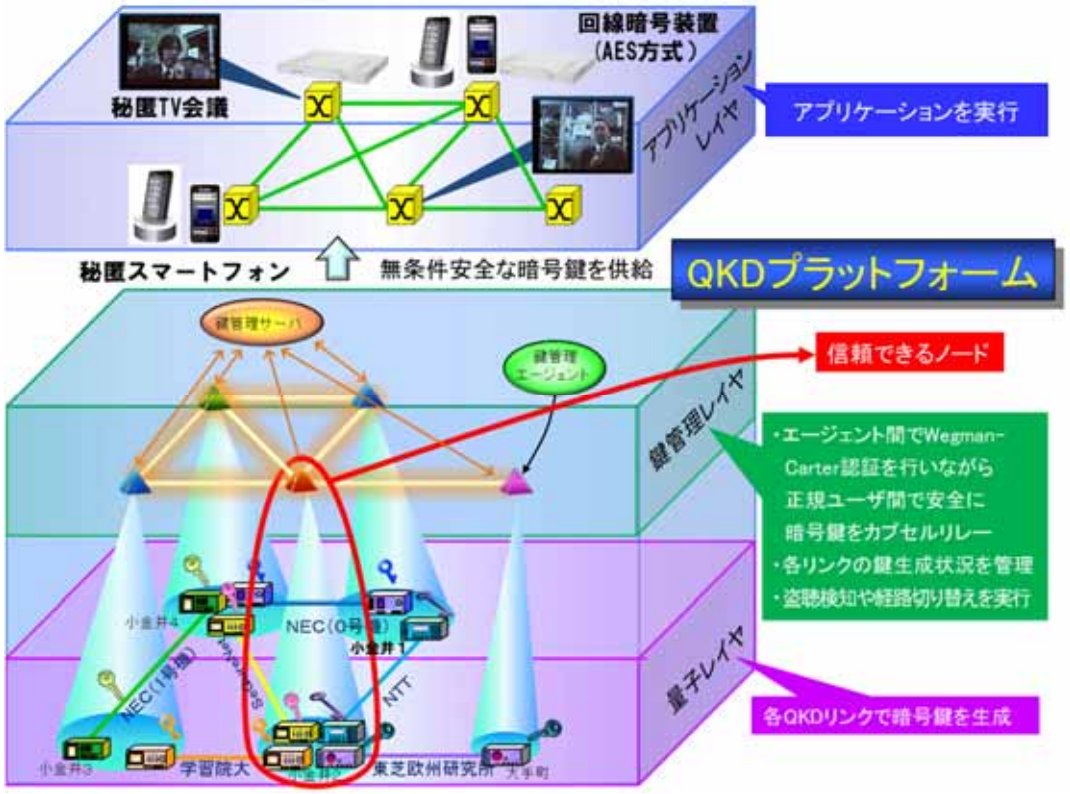




〇東京都心と郊外（小金井市）をつなぐテストベッド光回線"JGN"
を利用したQKDネットワークテストベッド
〇NEC、東芝、NTT、学習院大等の産学機関、及び一部海外機関が
それぞれのQKD装置を導入しネットワークを構成。
〇2010年、世界初となるQKDによる秘匿動画配信（TV会議）の実証に成功

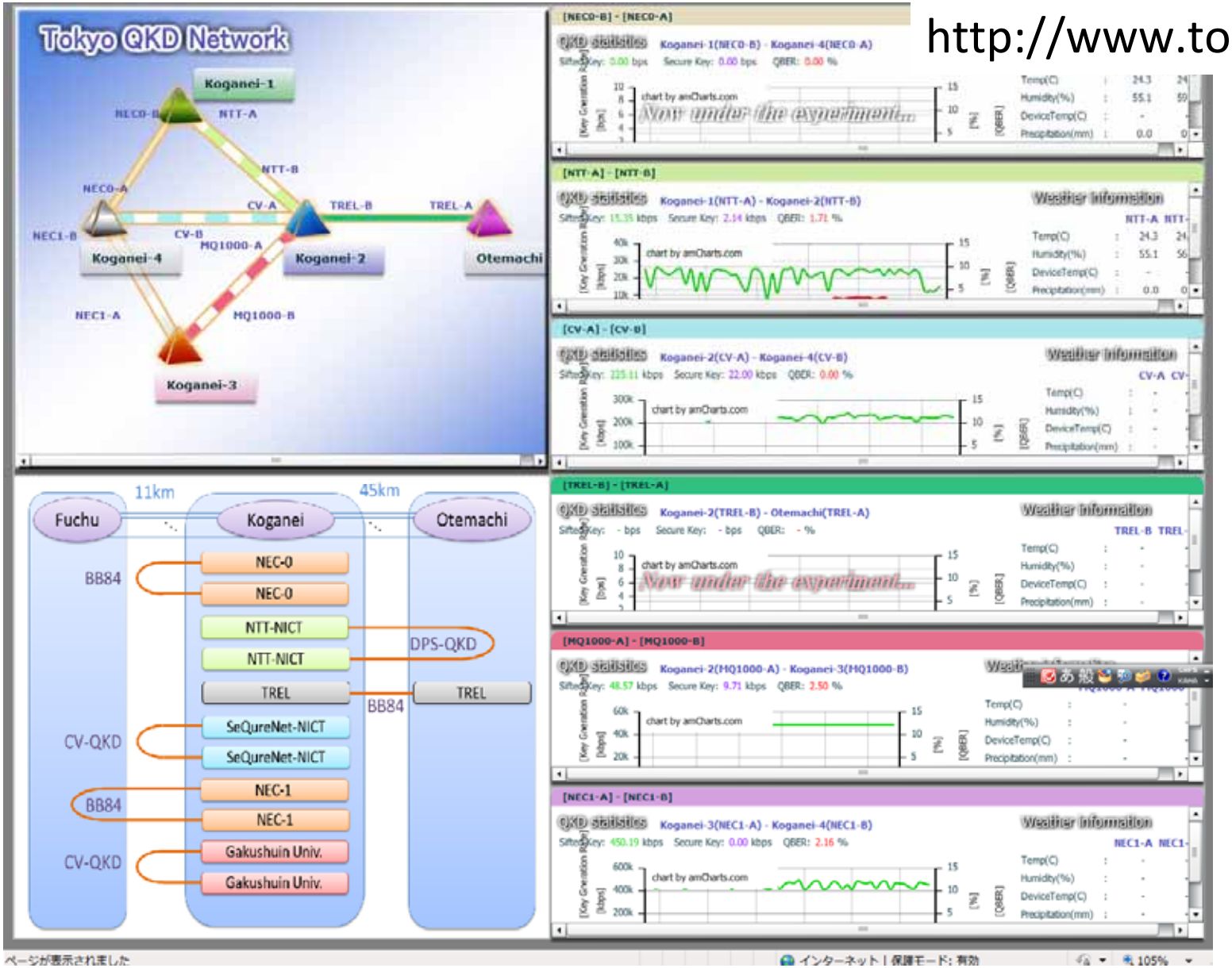
東京QKDネットワーク

QKDネットワーク全体の制御と鍵管理、アプリケーションへの提供を安全に行う「QKDプラットフォーム」技術を開発



QKD装置の改良も推進：フィールド実装されたQKD装置としては世界最速の鍵生成速度（300kbps/リンク）を実現

現在のネットワーク稼働状況



http://www.tokyoqkd.jp/

実運用試験

- NEC

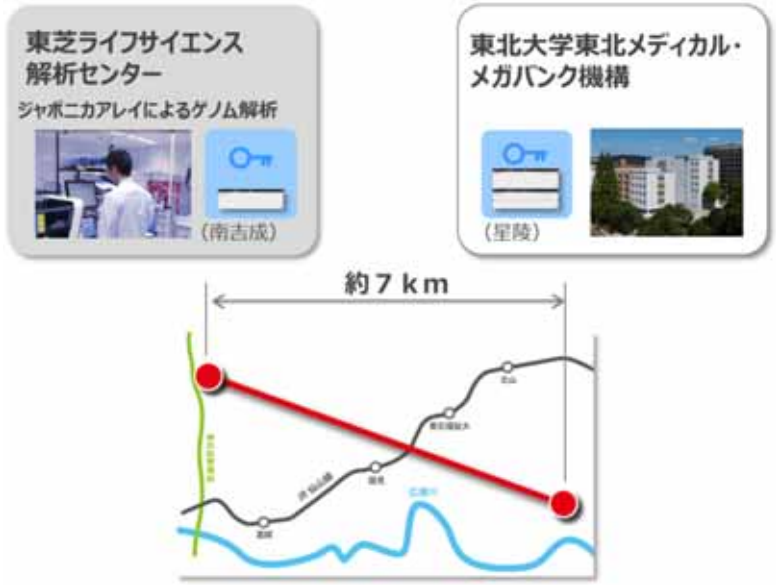
「サイバーセキュリティ・ファクトリー」内で実運用評価試験を開始（2015年7月～）

プレスリリース

http://jpn.nec.com/press/201509/20150928_03.html

- 東芝

仙台の自社ー東北大間を結ぶQKD回線を構築。ゲノム解析データの暗号通信を開始（2015年8月～）



プレスリリース

http://www.tqccs.com/cl/tech/qccs/

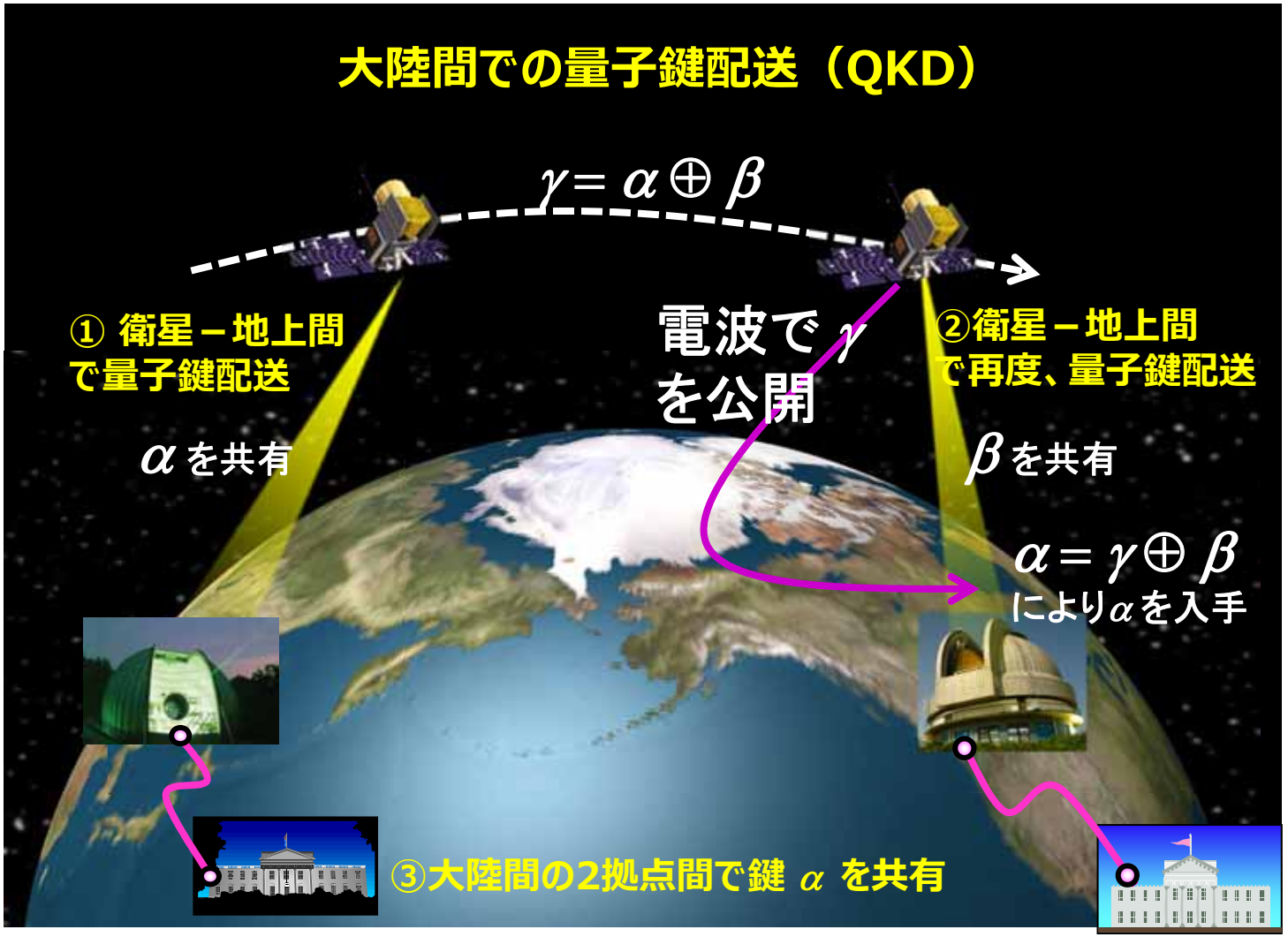
QKD研究開発の動向

（1） 地上QKDネットワーク

（2） 衛星QKD

衛星量子通信

- 現在の海底ケーブルは、量子暗号では使えない (中継増幅器が盗聴検知を阻害)
  ⇒大陸間スケールの量子鍵配送は地上インフラのみでは今のところ困難
- 衛星を経由すれば、大陸間で量子鍵配送が可能（宇宙空間では光の減衰はほぼゼロ)



衛星QKDの実現に向けた研究

- “Airborne demonstration of quantum key distribution receiver payload”, Quantum Sci. Technol. 2, 024009 (2017).
  (U. Waterloo, Canada)

- “Quantum-limited measurements of optical signals from a geostationary satellite”, Optica 4, 611 (2017).
  (Max Planck Institute, Tesat-Spacecom, DLR, Germany)

- “Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite”, Nature Photo. 11, 502 (2017).
  (NICT, Japan)

<最初の衛星QKD実証>
- “Satellite-to-ground quantum key distribution”, Nature 549, 43 (2017).
  (USTC, CAS, China)

<Intercontinental QKD demonstration>
- “Satellite-relayed intercontinental quantum network”, Phys. Rev. Lett. 120, 030501 (2018). (China-Austria)

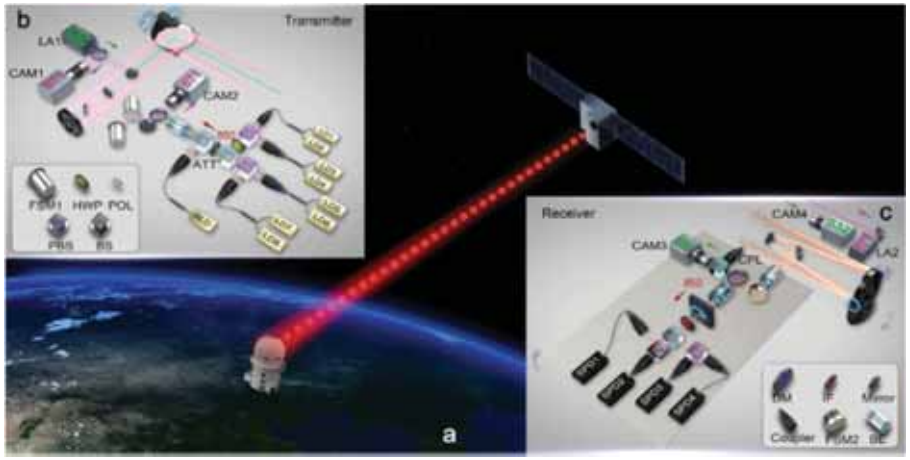
中国の衛星量子通信技術

量子科学技術衛星 Mozi（墨子）
を打ち上げ（2016年8月）

量子科学技術衛星 (600kg)

Courtesy by Qiang Zhang (USTC)

世界初の衛星ー地上間量子鍵配送に成功　Nature 549, 43 (2017)

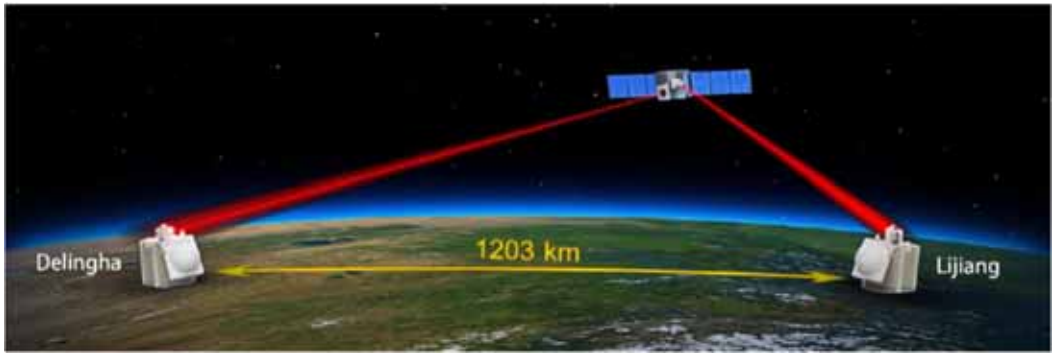


- Key rate 1.1 kbit/s
- security parameter $\mathbf{10^{-9}}$

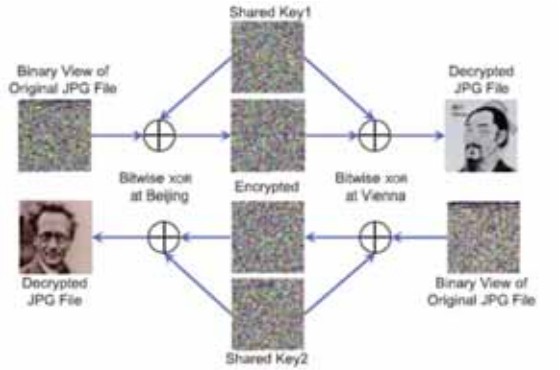
・Wavelength 848.6 nm
・Rep rate100 MHz
・Pulse width 0.2 ns
・Beam diameter on ground 10 m
（1200 km propagation）

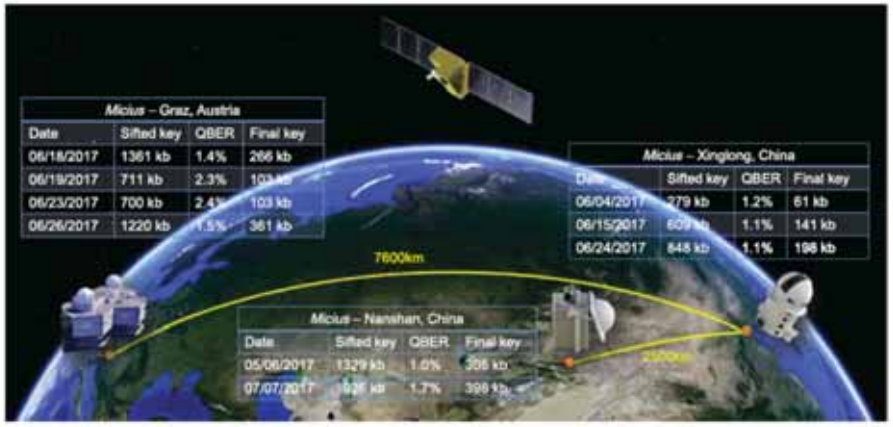
中国の衛星量子通信技術

1200km離れた2つの地上局に向けて衛星から量子もつれ配信に世界で初めて成功
Science 356, 1140 (2017)



世界初の大陸間QKDに成功（中国－オーストリア） Phys. Rev. Lett. 120 030501 (2018)
・衛星QKDを介して鍵を共有した後、通常回線で画像（5 kB）を暗号化・伝送





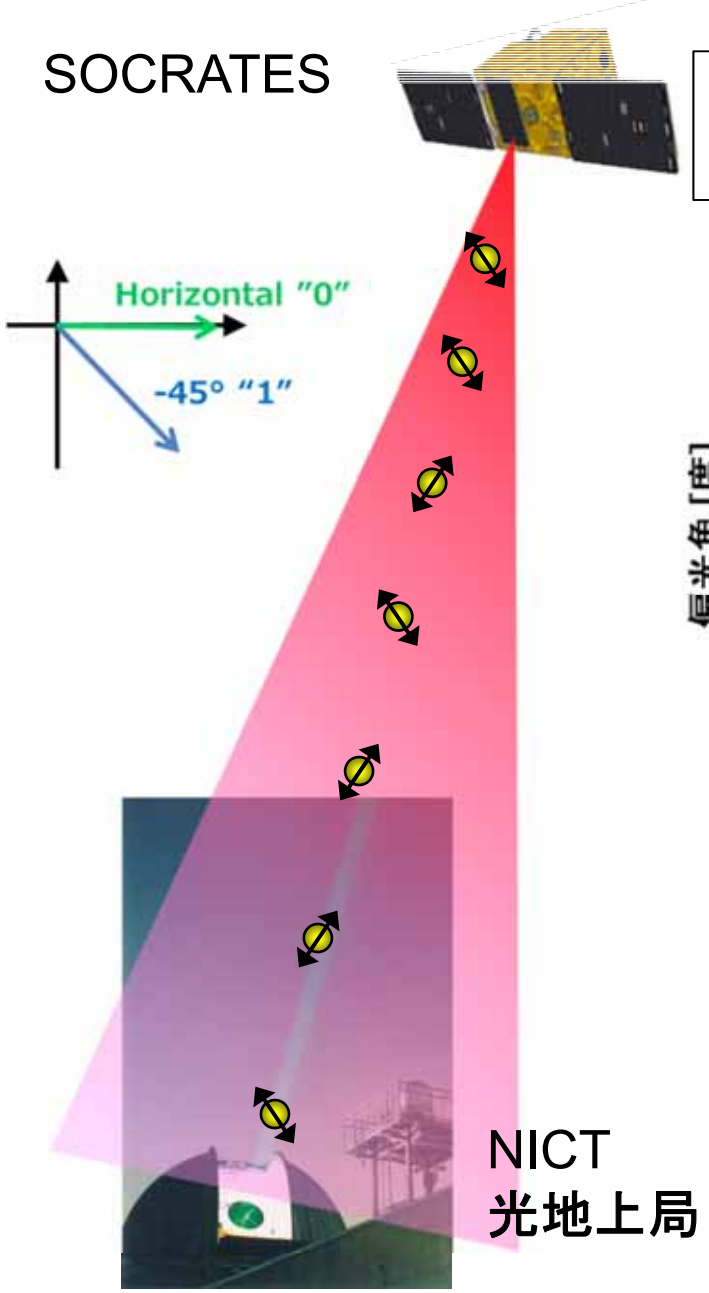
世界最高精度のレーザ捕捉追尾技術により実現

日本の衛星量子通信の取り組み

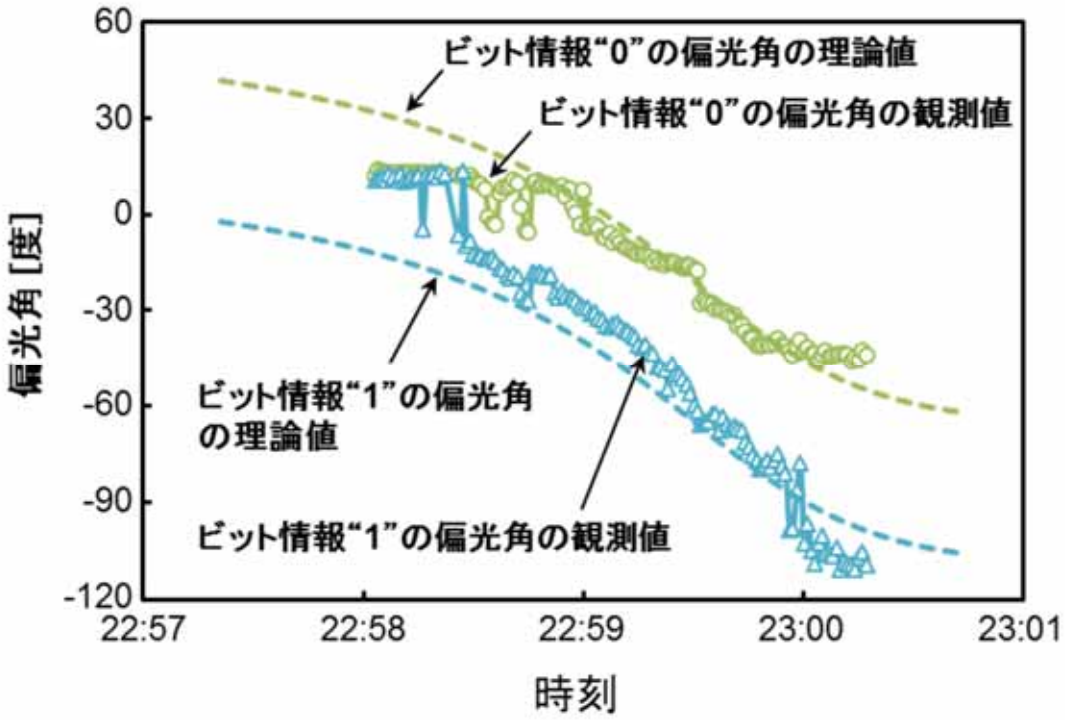
超小型衛星による衛星光・量子通信技術の開発（NICT）

・超小型衛星SOCRATES（NICT-AES共同開発、2014年打ち上げ）
・超小型光送受信機SOTA (Small Optical TrAnsponder)を搭載
⇒ 超小型衛星による衛星光通信実証、及び量子通信基礎実験に
それぞれ世界で初めて成功

日本の取り組み（衛星量子通信）



偏光に情報を載せた光子レベルの微弱光を送信
⇒ 地上局で光子の偏光状態を正確に識別



超小型衛星による量子通信基礎
実験に世界で初めて成功 (2017)

H. Takenaka, et al., Nature Photonics, 11, 502 (2017)

衛星量子通信分野の諸外国の動向

○米国
- ●米国企業が観測網・通信網のための**大規模衛星コンステレーション**を計画
- ●軍研究所等で衛星量子暗号技術に関する研究開発を推進

○中国
- ●2016年8月に打上げた量子科学技術衛星(600kgの大型)で低軌道と地上局間での量子暗号の実証実験に成功(2017年７月) 海外チームと共同実験継続中
- ●さらに静止軌道上から24時間リアルタイムで量子暗号を行う技術を開発中

→静止軌道、低軌道上で中国独自の量子暗号網を構築する試み

○ドイツ
- ●Max Plank研、Tesat-Spacecom、ドイツ航空宇宙局が静止衛星・地上局間で量子通信の実証実験に成功(2017年6月)
- ●2020年頃量子暗号用小型衛星を打上げ予定(低軌道)

→ドイツは衛星光通信で世界トップレベルの技術を所有

○スイス
- ●スイス宇宙局の小型衛星開発プロジェクトがスタート
  ID Quantique社の小型衛星量子暗号に関する提案“QuSat”が採択
  http://www.idquantique.com/quantum-space-race/

→当社は量子暗号の世界市場を拡大中 衛星分野でも今後勢いを増す予想

○カナダ
- ●ウォータールー大学が衛星量子暗号プロジェクト“QEYSSat” を開始（2017年4月）
  http://www.ept.ca/2017/04/canada-enters-quantum-space-race-u-waterloo-project/

→国立光学研究所, Xiphos Technologies, Neptec, Excelitas, COMDEVなどと連携し国際的リーダーシップの獲得を目指している

○日本
- ●総務省プロジェクト「衛星通信における量子暗号技術の研究開発」2018年～

内容

1. 導入：暗号の役割と現代暗号の安全性

2. 量子暗号の仕組みと安全性

3. 国内外の研究開発動向

4. 量子暗号の応用
→ 現代セキュリティ技術との融合

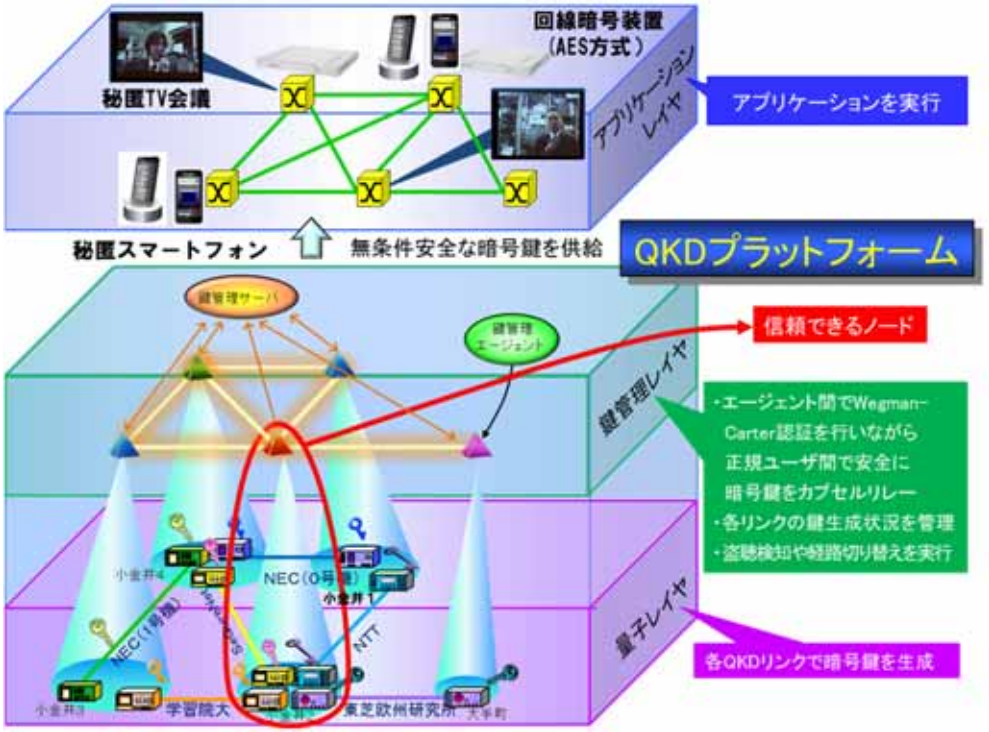
5. まとめ：社会実装に向けて

量子暗号の応用

QKDネットワーク上で実証されてきた応用例

1. 秘匿TV会議
2. 秘匿携帯電話
3. 電子カルテ秘匿通信
4. 共通鍵暗号（AES）の種鍵
   （既存暗号の種鍵の
   安全性を強化）
5. 選挙・金融ネットワーク

6. 分散ストレージ



QKDの特長

- 情報理論的安全性（計算機で解読不可能な安全性）

⇔現在の暗号：計算量的安全性
→ 将来の計算機の進展により解読の危険性
（現在暗号化されたデータが10年後に解読される恐れも）

「データの寿命」

データの寿命

秘匿期間	分野	情報	セキュリティレベル	理由
30	軍事	作戦計画等	**非常に高い**	防衛情報を扱っている為
		防衛装備品に関する技術情報	**非常に高い**	防衛情報かつ法律でも定められている為
30	行政	政策	**普通**	国の混乱を招く恐れがあるが一時的となる可能性が高い為
		外交情報	**非常に高い**	国の信用問題であり各国との関係に悪影響を及ぼす為
＞100	医療	遺伝子情報	**非常に高い**	遺伝情報から差別や，雇用における採否に影響する可能性がある為
		電子カルテ	**高い**	アレルギーなど人の生死に係る為
30	インフラ	SCADA	**高い**	ライフラインを不正操作された場合各地域に影響を及ぼす為
		新エネルギー開発	**高い**	国際的に重要な開発は資産である為
5	金融	金融政策	**高い―普通**	非公開期間が短期間である為
		株式	**非常に高い**	企業情報が主な秘密情報である為

秘密分散ストレージ

- 医療情報
  - 世紀単位の超長期安全性が必要（遺伝子等）
  - バックアップデータの必要性（災害時など）

秘密分散法＋量子鍵配送

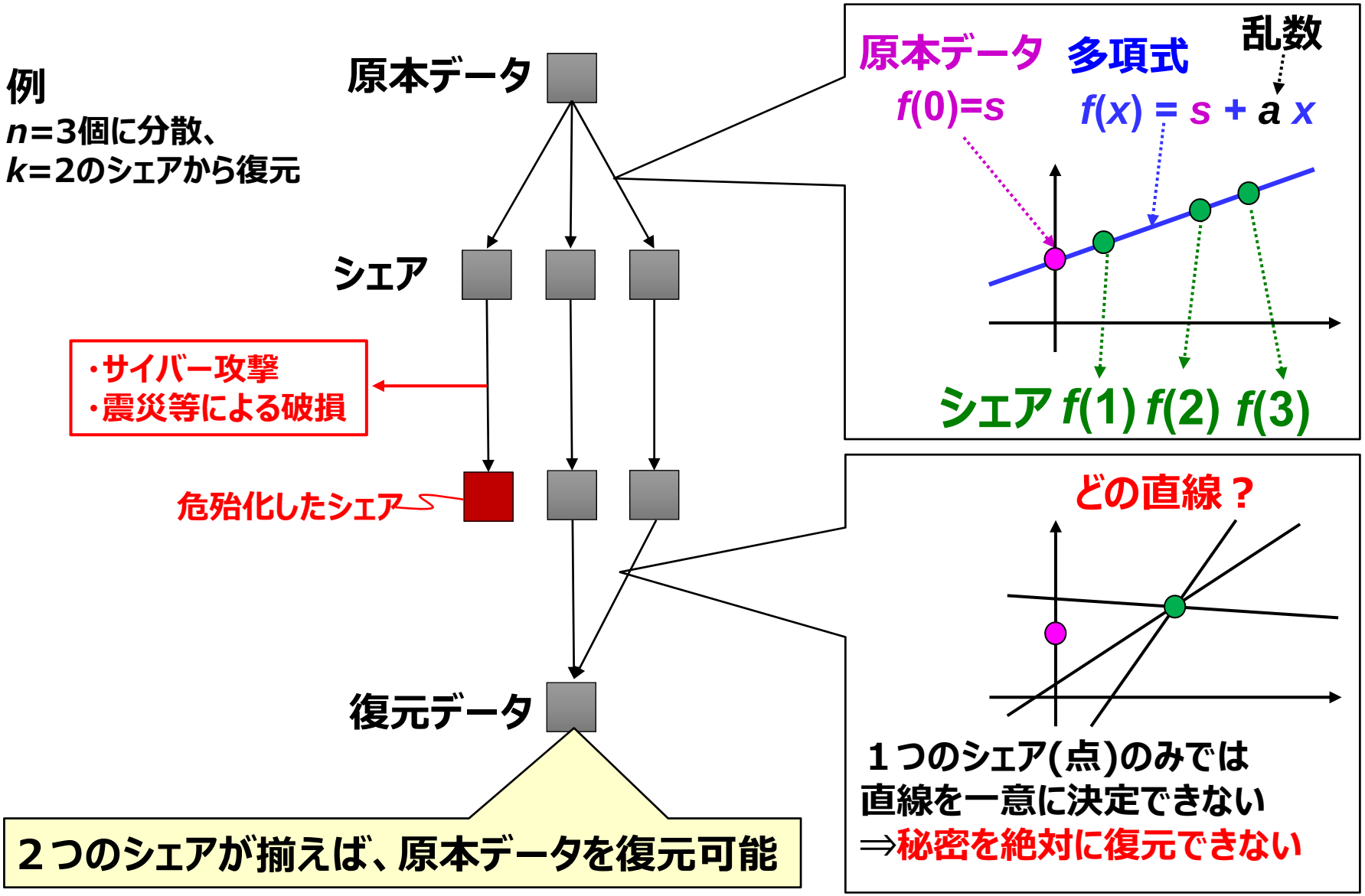
情報理論的に安全な
分散ストレージシステム

秘密分散

1979 Shamir

原本データを無意味化された複数のデータ（シェア）に分割

例
n=3個に分散、
k=2のシェアから復元



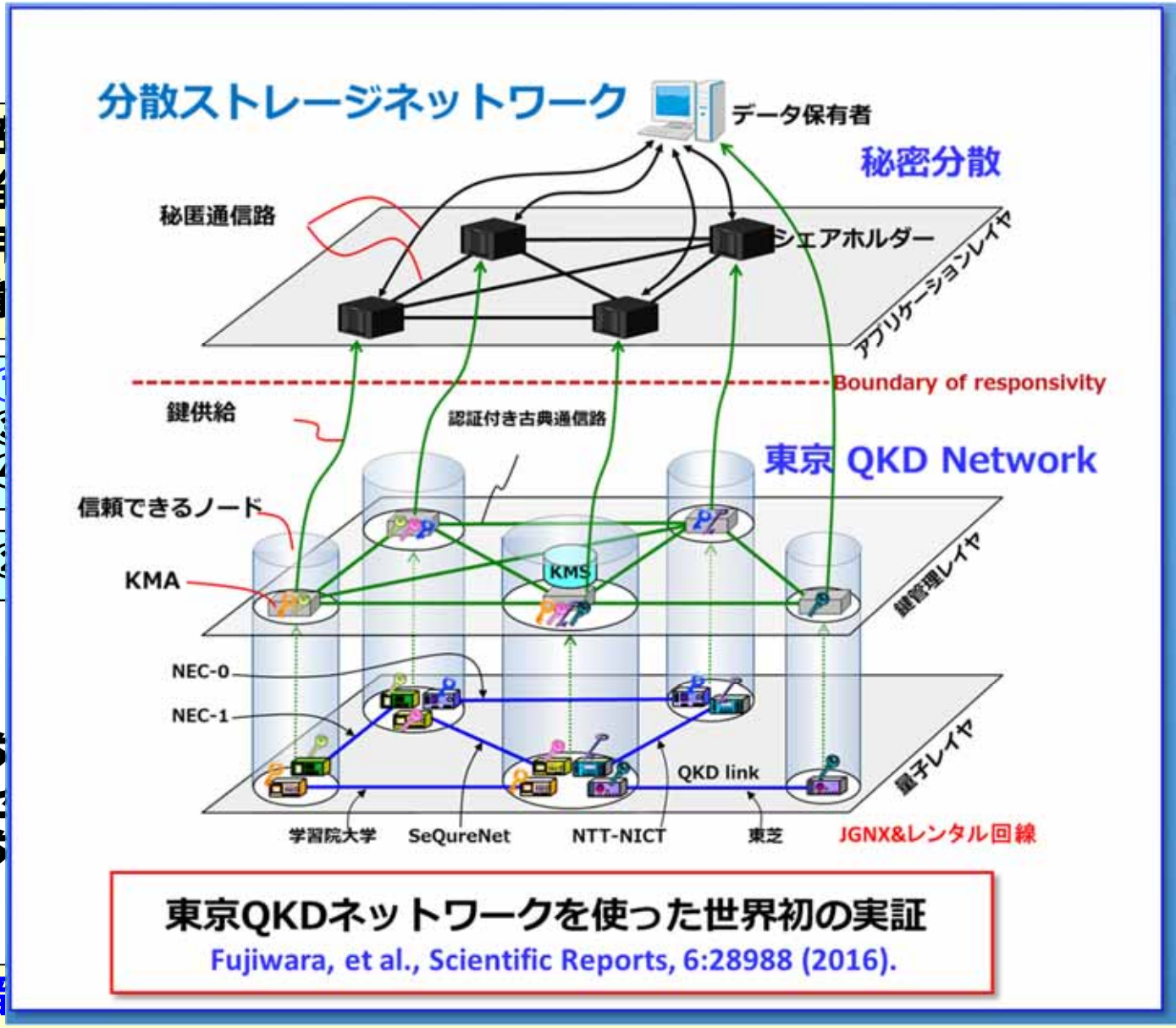
超長期安全性を実現するQKD秘密分散ストレージ

要件

1. 機密
2. 完全
3. 可用
4. 機能

暗号のみでは
不可能
バ間通信の
性を超長期間
できない

デジタ
メッセ
データ



東京QKDネットワークを使った世界初の実証
Fujiwara, et al., Scientific Reports, 6:28988 (2016).

現代暗 現可能

内容

1. 導入：暗号の役割と現代暗号の安全性

2. 量子暗号の仕組みと安全性

3. 国内外の研究開発動向

4. 量子暗号の応用
   → 現代セキュリティ技術との融合

5. まとめ：社会実装に向けて

まとめ：社会実装に向けて

- 量子暗号とは

○量子コンピュータを含むあらゆる計算機で解読不可能な
唯一の暗号技術

○量子鍵配送（QKD）は距離・速度に制限（中継増幅不可）
→ P-to-P回線は長くても50～100km程度
→ trusted nodeを介したネットワーク化
→ 鍵管理のアーキテクチャ

QKDネットワーク

まとめ：社会実装に向けて

- 既存の敷設ファイバーネットワーク

  ○原理的には適用可能（中継器の無い回線）
  △日本の事情 → 敷設が古い
  → 高損失ファイバー
  架空線の多様
  迂回路多数
  } **QKD、光通信、共通の課題**

- 新規ネットワークの戦略的敷設（5Gなど）

  ＜QKD、光通信の効率的運用に向けて＞

  ○直線的なネットワークの設計（線路・河川などの考慮）
  ○中継器の無いダークファイバの戦略的敷設
  ○ファイバー融着の少ない設計
  ○低損失ファイバーの導入（＜0.2 dB/km）
  ○運用に適した鍵管理アーキテクチャの開発