資料3－1
科学技術・学術審議会 先端研究基盤部会
量子科学技術委員会（第4回）
平成28年6月20日

量子通信、量子暗号の研究動向と今後の戦略

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

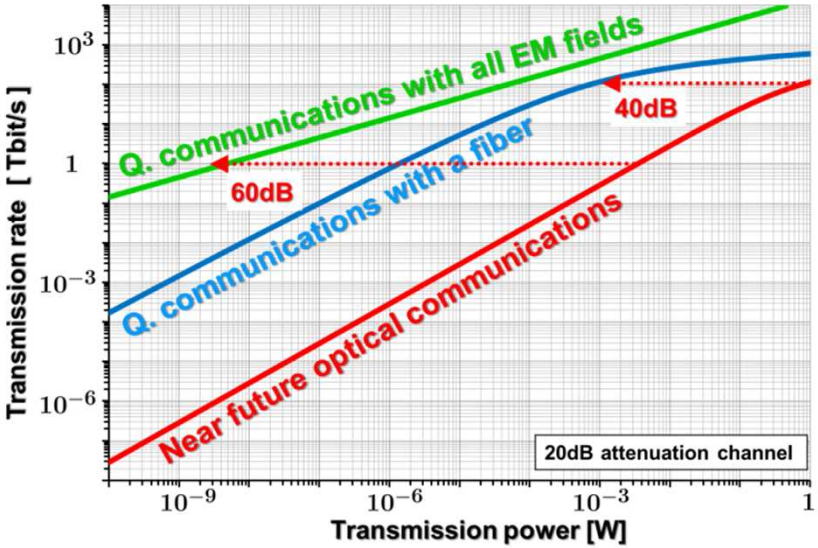
未来ICT研究所　佐々木雅英
Mail: psasaki@nict.go.jp, Tel: 042-327-6524

量子通信

受信過程で重ね合わせの原理を使い
信号識別性を向上

⇩

低電力・大容量通信



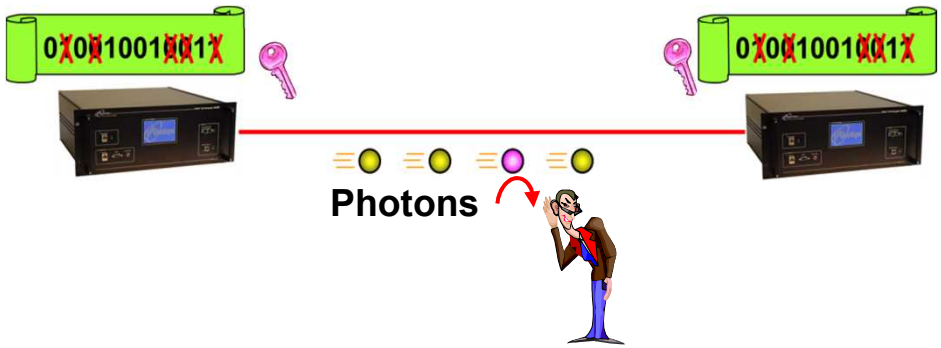
量子暗号

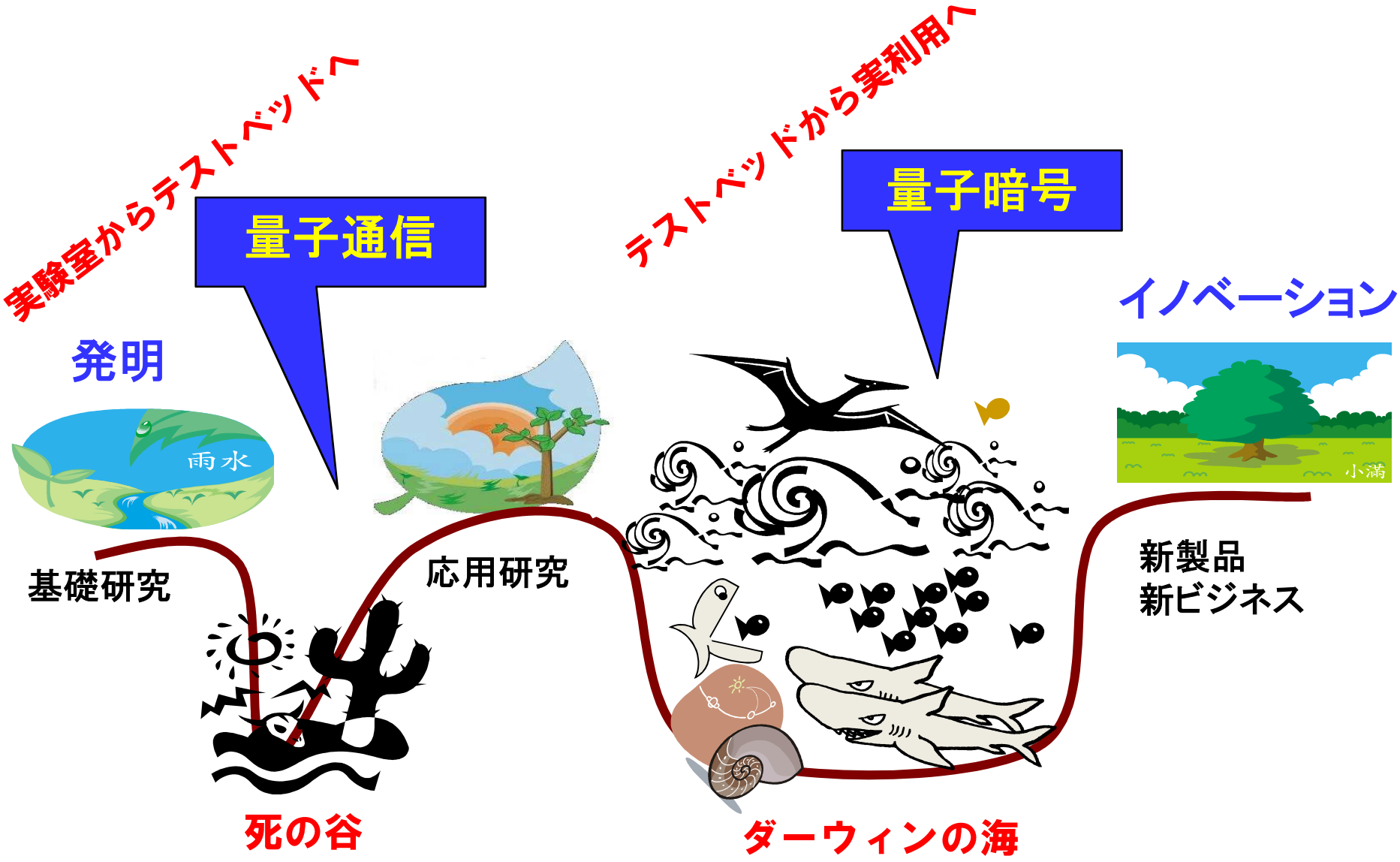
不確定性原理を使い盗聴を確実に
検知し、安全に暗号鍵を配送

⇩

どんな技術でも破れない暗号技術

量子鍵配送（QKD）





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

量子通信、量子暗号の現状と問題 （参考資料：資料1~4）

日本：NICTや企業が実用レベルのQKD技術、及び新しいネットワークアプリケーションを開発。しかし、市場開拓までには至っていない（ダーウィンの海で格闘中）。
量子通信と暗号を融合する新技術を開発中（ワイヤレス用途）。

欧米：ID Quantiqueなどベンチャー企業がQKD装置を販売（速度は日本製の約50分の一）。
大型国家プロジェクトは、日本より基礎研究寄り。
実用化への具体的戦略があまり読み取れない。

中国：世界で最も大規模のQKDネットワークを構築中。
標準化に打って出られれば他国は太刀打ちできない。
しかし、大規模ネットワークでの安全性保証をどうやるのか不透明（ここをクリアしないと暗号分野に受け入れられない）。

どの国も、単に量子技術を深めるだけでは、
イノベーションを起こせない！

量子技術への研究投資動向

欧米中日の主な研究開発プロジェクト

（科研費（S以外）、NSF等の探索的PJは除く）

量子人工脳(ImPACT)、
量子アニーリング(D-wave)

量子通信　　量子計算

		量子暗号	量子ノード	量子計測標準	専用量子計算	万能量子計算
英	“Quantum Technology Hub” 2013～　5年間、約270億円＊1	○	○	○	○	○
蘭	“QuTech” Project 2015～　10年間、約200億円		○	○	○	○
米	DARPA、IARPAで複数PJを推進 予算額未公表	○	○	○	○	○
中	“Quantum Backbone” Project＊2 2013～　3年間、約100億円	○	左記とは別に超伝導、ナノ技術等にも巨額予算を投資			
EU	Quantum technologies flagship a €1-billion project from 2018	○	○	○	○	○
日	ImPACT: 2014～　5年間、約30億円 ERATO、科研費S、NICT関連予算	ImPACT		ERATO 科研費S	ImPACT	

＊1　関連する量子デバイス技術等を含め合計で約480億円を投資。
＊2　3年間で北京－上海間にQKDテストベッド構築。
　　2016年以降は別途予算で運用予定。

NICT自主・委託研究

「香取創造時空間PJ」
5年間、15億円程度

「ダイヤモンド量子センシング」
（慶大 他）5年間、2.5億円程度

量子通信、量子暗号は本当にイノベーションを起こせるのか？

現在の量子通信、量子暗号の機能と限界

・量子通信も、量子暗号も、量子中継も、まだ、1対1の通信プロトコルでしかない。(公開鍵暗号は1対百万、1対千万規模での電子署名を実行)

・量子暗号の直接リンクの距離と速度に『原理的』な限界がある。
(参考資料:資料5，6)
⇒プロトコルをいじっても抜本的解決にはならない。

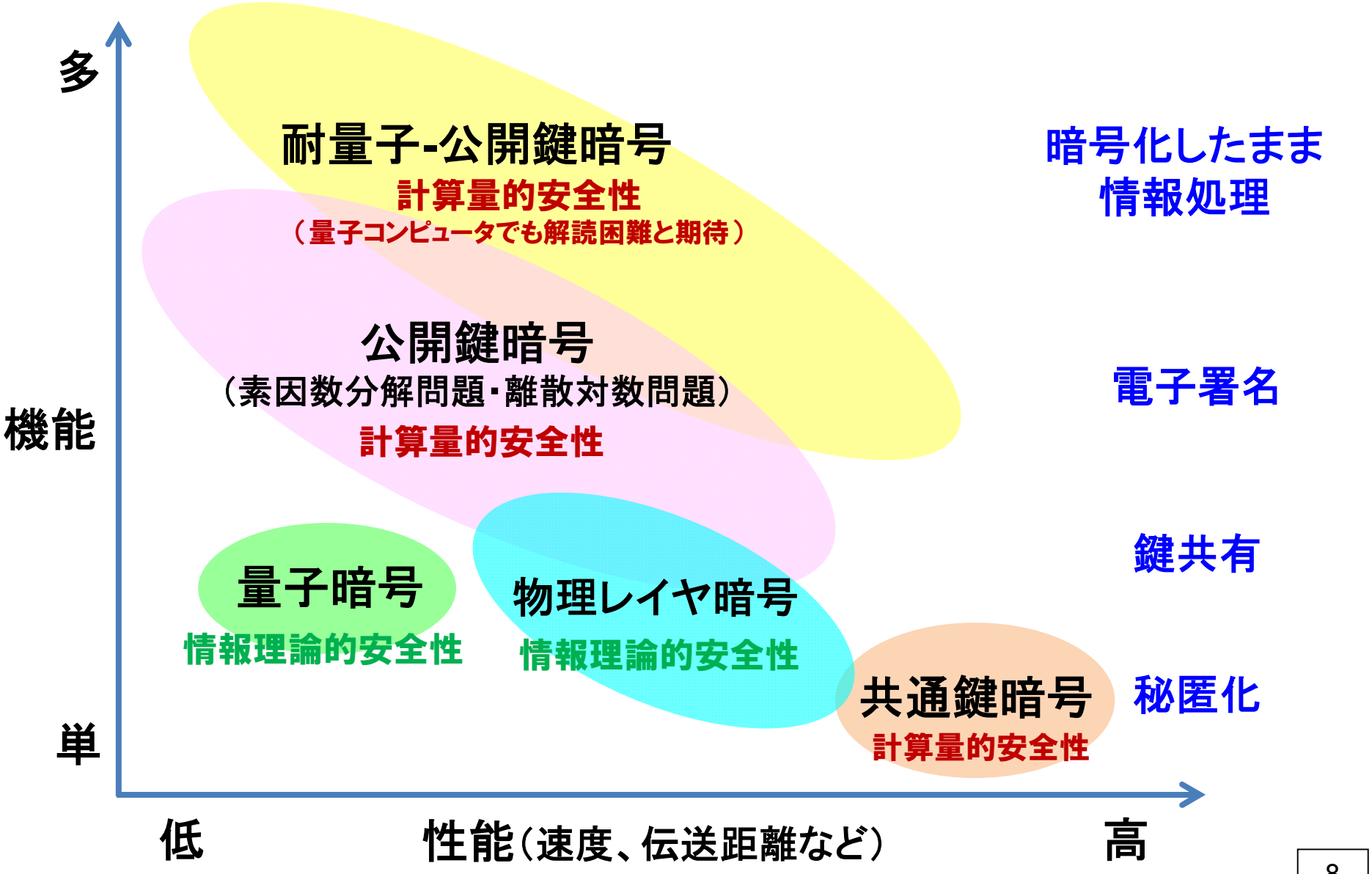
・ネットワーク化には古典的trusted nodesが必要。

・量子中継のスケーラビリティは誰も実証できていない
⇒まずは、量子情報処理システムを構成するための
回路ユニットと見なして取り組む方がよいのでは？

・量子通信・量子暗号は、現在のネットワーク技術、暗号技術の持つ多様な機能のうち、まだ、ほんの一部の機能しか実現できていない。
⇒まだ多くの可能性が掘り起こせる余地がある
⇒どのようにアプローチすればよいか？

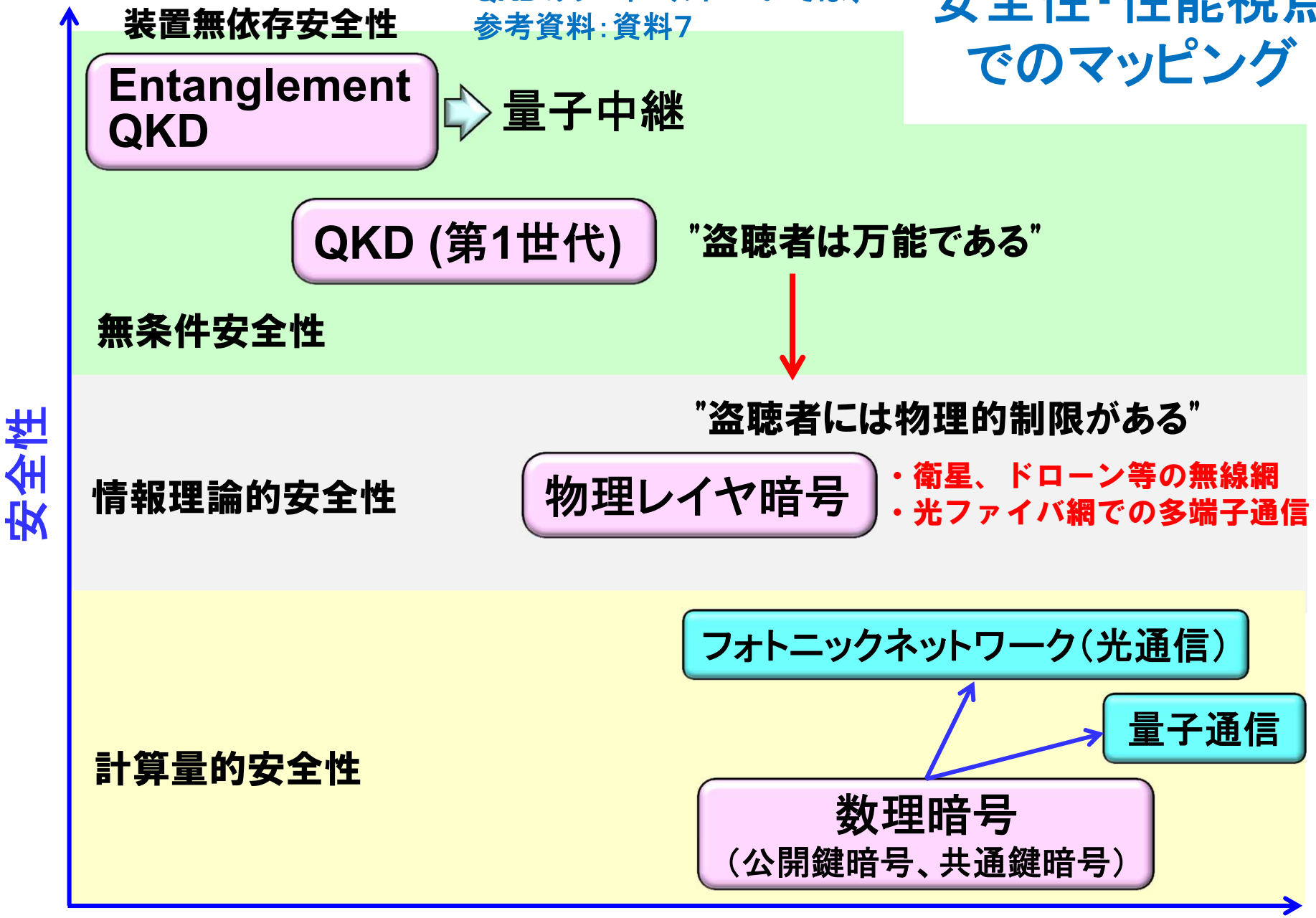
暗号技術全体の中での量子暗号の立ち位置

機能・性能視点でのマッピング



安全性・性能視点でのマッピング

QKDのプロトコルについては、
参考資料：資料7



・今見えている量子通信、量子暗号の技術体系を単に深めるだけでは先は無い。

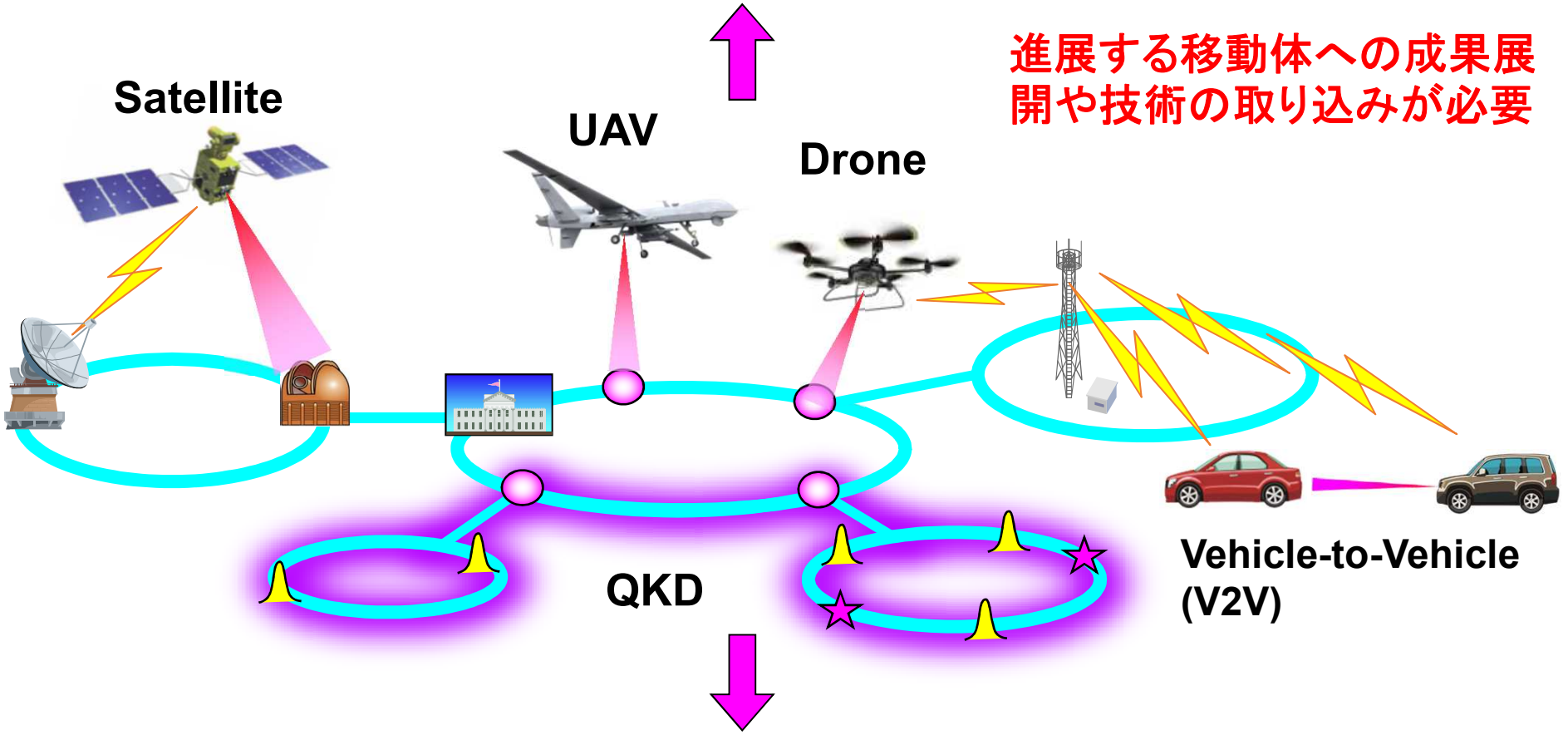
・情報理論や暗号技術、フォトニックネットワーク技術、ワイヤレスネットワーク技術と融合させ、新しい技術体系に移行できないと広い普及は難しい。

・しかも、これらの周辺分野を（量子の専門家である）我々自身で、必要な形に進化させないと、量子技術との意味ある融合は難しい。

ケーススタディ

（2）空の産業革命を支えるセキュア通信技術

進展する移動体への成果展開や技術の取り込みが必要



（1）超長期安全性を持つデジタルアーカイブシステム

ニーズが高く、現代暗号のみでは解決できない課題がある。そこを量子技術と従来技術の融合により解決！

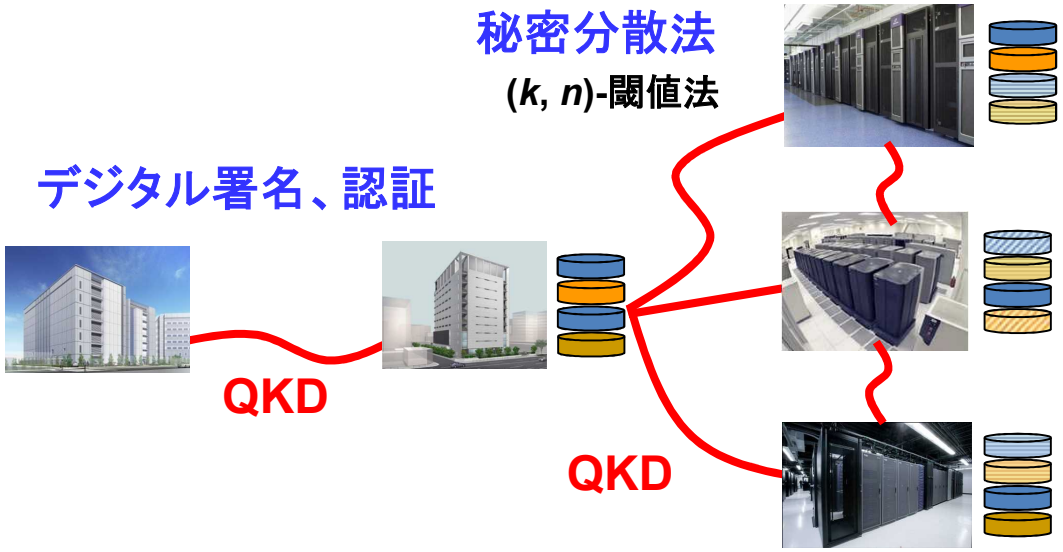
（1）超長期安全性を持つデジタルアーカイブシステム

目的　『世紀単位の時間』でセキュリティ確保が必要な重要情報（ゲノム情報など）を扱うストレージネットワークシステムの実現

要件
- 機密性：正規ユーザ以外に平文が漏れないこと ⇒ 暗号化
- 完全性：平文が改竄されていないこと ⇒ 署名、認証
- 可用性：必要な時に平文を得られること ⇒バックアップ、障害対策
- 機能性：暗号文のまま情報処理ができること ⇒ 完全準同型暗号化

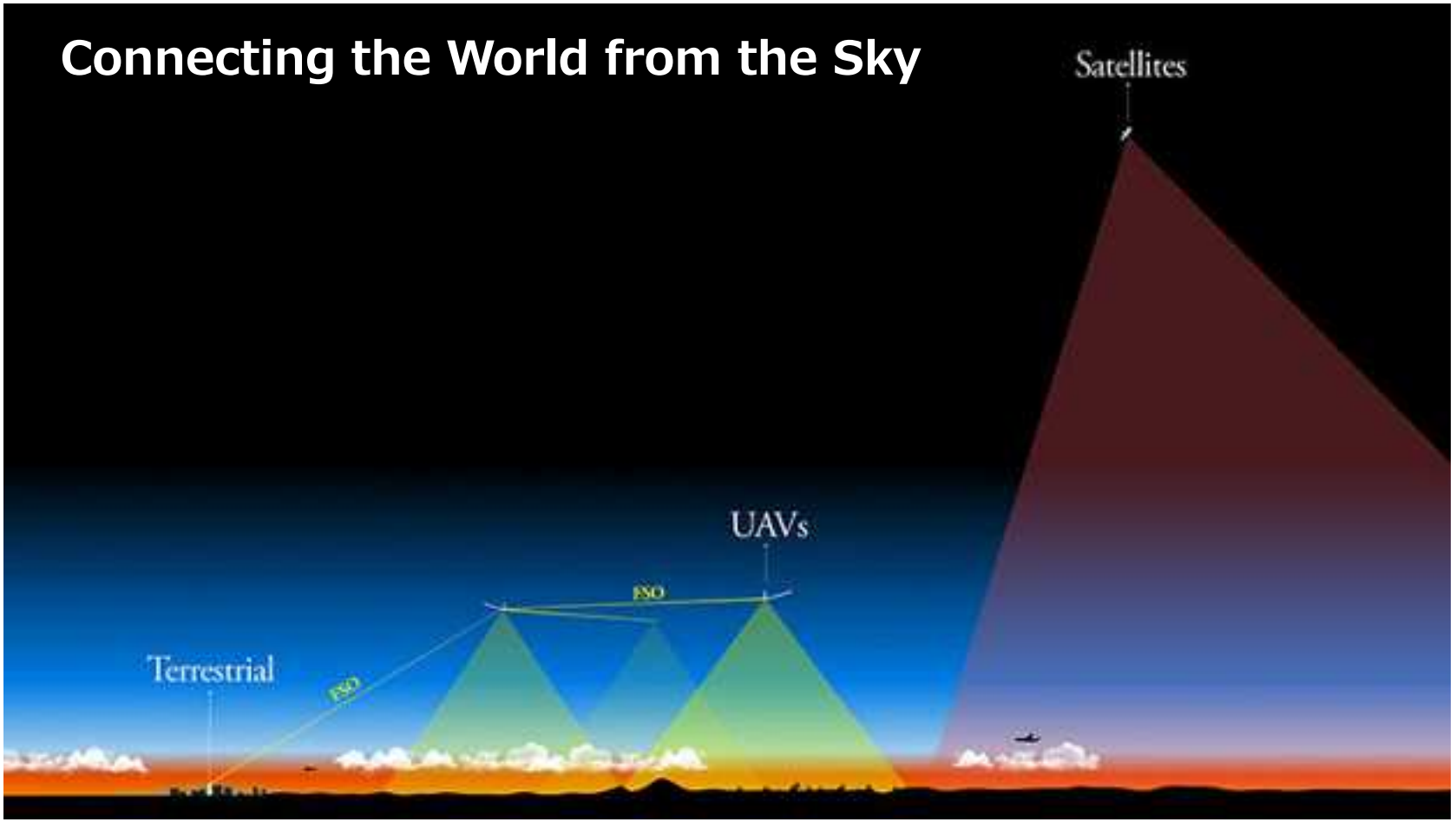
計算量的安全性に基づく現代暗号のみでは解決不可能。

量子暗号、現代暗号、ネットワーク技術の分野間連携が極めて有効



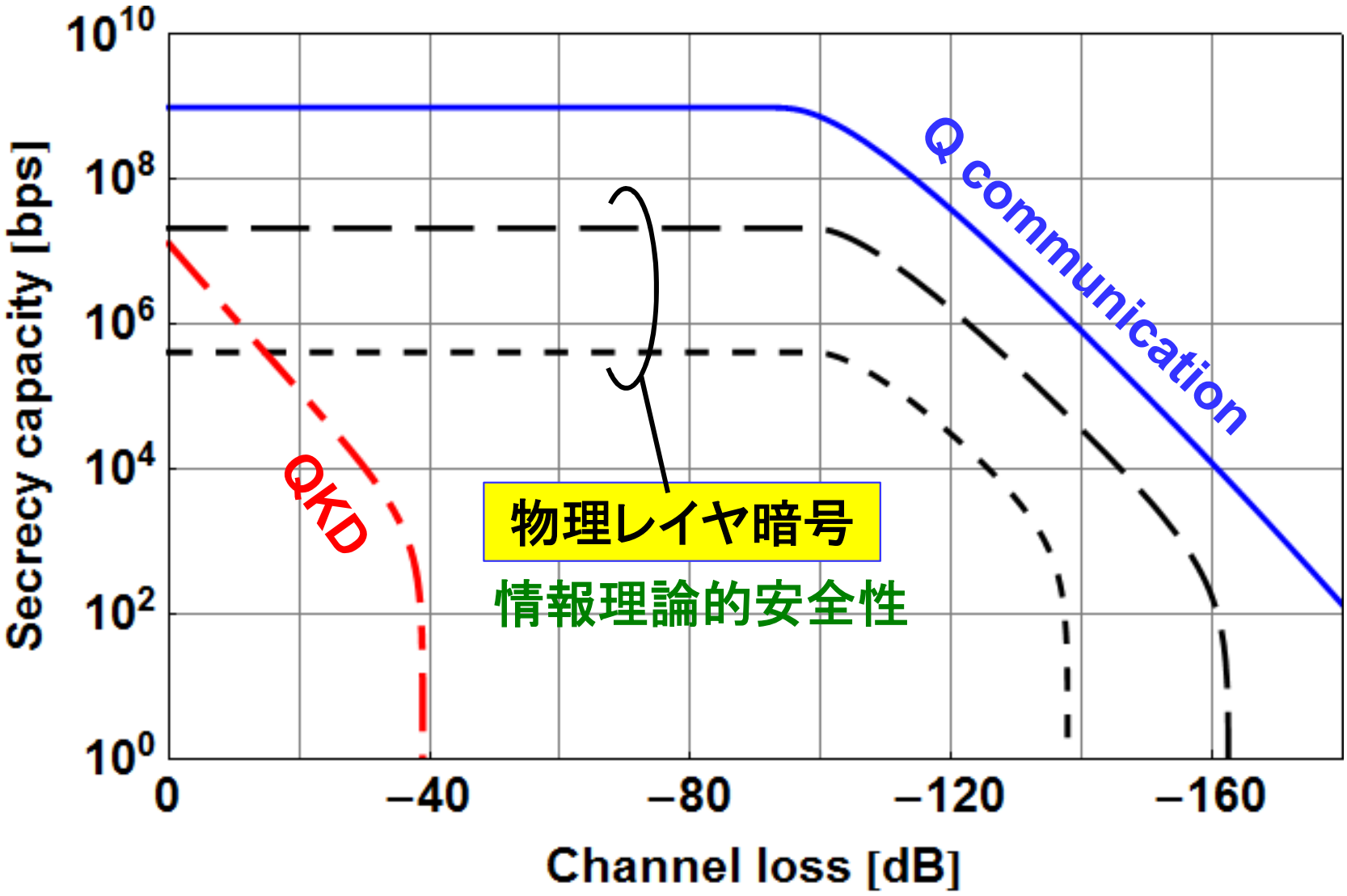
（2）空の産業革命を支えるセキュア通信技術

Facebook’s Connectivity Lab



http://www.geek.com/science/facebook-to-launch-internet-dropping-drone-1629926/

新しい境界領域（情報理論、暗号、量子）



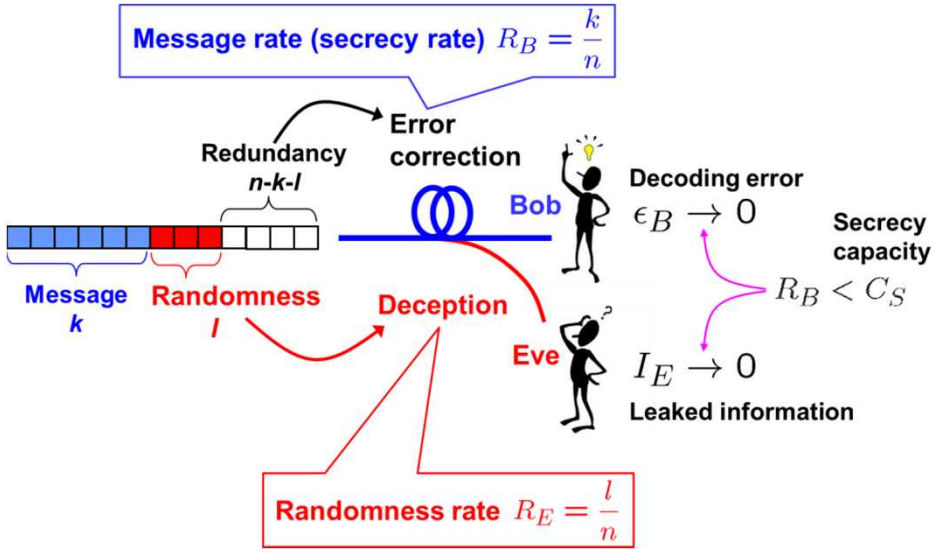
物理レイヤ暗号

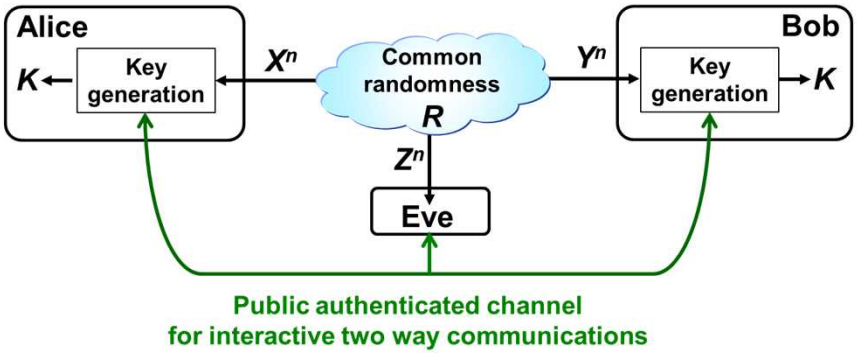
・正規通信路と盗聴通信路の性質が推定できる場合に、適切な符号化を行うことで**安全かつ高効率**にメッセージの伝送や鍵交換を行う暗号通信技術。
・通常、電波や光のワイヤレス通信（特に視野通信）を想定。
・どんな計算機でも解読できないことが証明できる（情報理論的安全性）。

①秘匿メッセージ伝送
一つの通信路で一方向にメッセージを伝送。正規受信者のSN比が、盗聴者のSN比より勝っている場合に機能。

②鍵交換
乱数を共有する通信路と鍵蒸留のための公開通信路。盗聴者のSN比が、正規受信者のSN比より優れていても機能。

QKDはこの一例





まとめ

- 単に量子技術を深めるだけでは、イノベーションは起こせない。

- ネットワーク、移動体、暗号分野の新潮流を捉え、これらの分野で新しい枠組みを自ら構築し、そこに量子技術を適材適所で導入して、分野融合に成功した者がイノベーションを起こす。

Thank you for your attention

参考資料

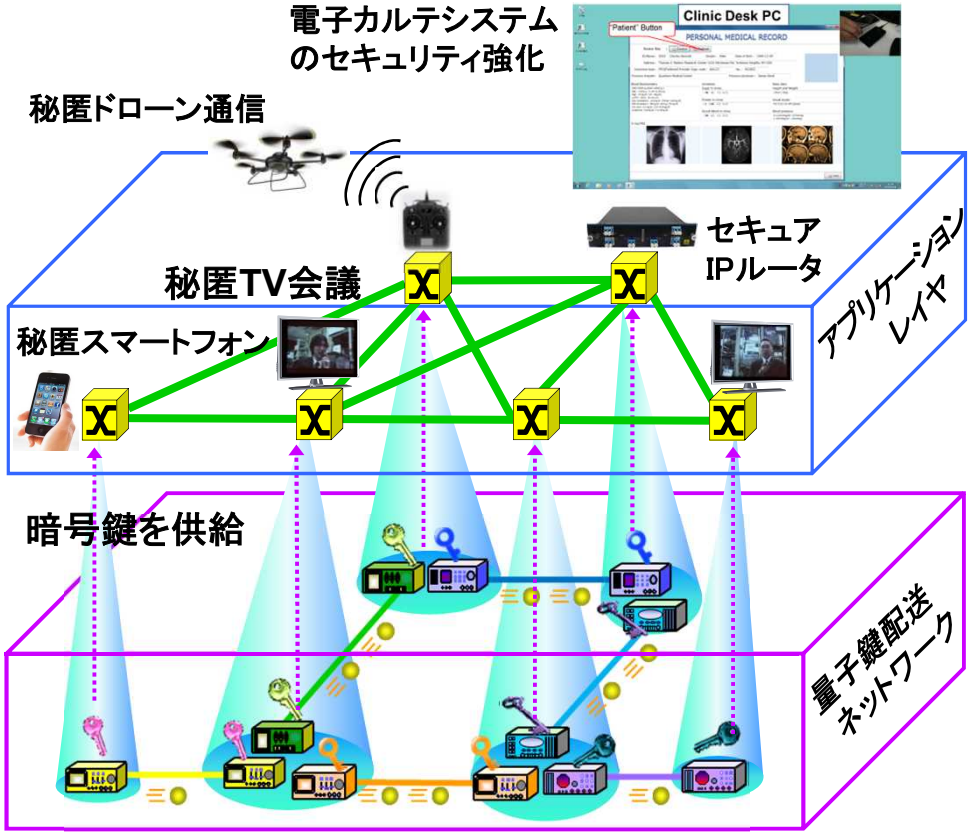
量子暗号技術の現状（日本）　資料１

NICT産学官連携プロジェクト（2001年～2015年）、ImPACTプログラム（2014年～2019年）

Tokyo QKD Network（2010年～）

- 安全性保証技術の開発
- 次世代技術の開発
- 様々な新しいアプリケーションの開発

NICT、NEC、東芝、三菱電機、NTT、
学習院大、東大、北大、東工大、名古屋大



2015年夏からユーザ環境での試験運用

NECサイバーセキュリティ・ファクトリーでの信頼性試験
http://jpn.nec.com/press/201509/20150928_03.html

東芝ライフサイエンス解析センター

東北大学東北メディカル・メガバンク機構

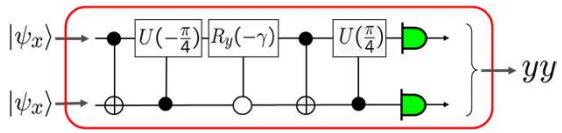
東芝：仙台市でのゲノム解析データの暗号化通信実験
http://www.toshiba.co.jp/about/press/2015_06/pr_j1801.htm

量子通信技術の現状（日本）

資料２

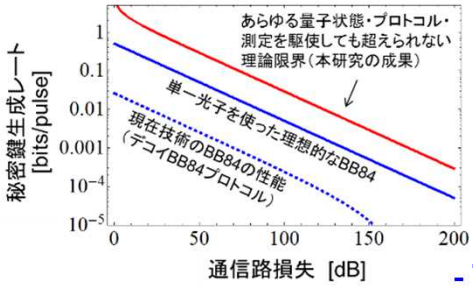
基礎研究（理論、実験）で世界をリード

量子受信機



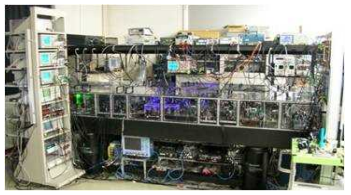
- Fujiwara, et al, PRL 90, 167906 (2003).
- Tsujino et al., PRL106, 250503 (2011).

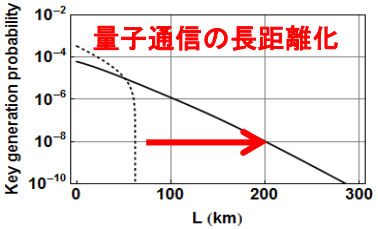
鍵配送容量の理論



Takeoka, et al.,
Nat. Commun. (2014)

量子リレー、量子もつれ交換



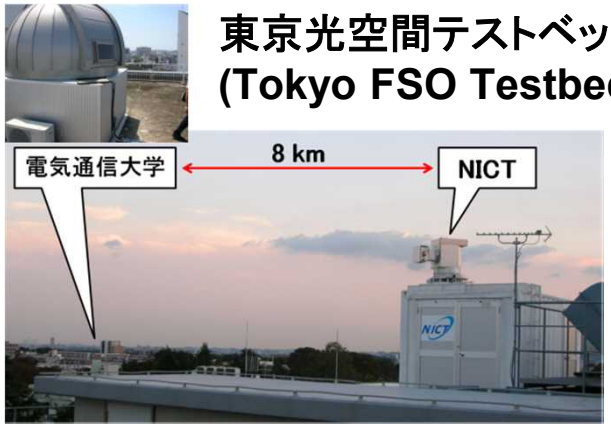


- Takahashi, et al. Nat. Photon. 4, 178 (2010).
- Neergaard-Nielsen, et al., Nat. Photon. 7, 439 (2013).
- Jin, et al., Scientific Reports 5, 9333 (2015).

テストベッドでの技術実証で世界を牽引

量子通信と暗号技術を融合した新技術を開発中（情報理論的に安全かつ大容量に伝送）

- Han, et al., IEEE-IT 60, 6819 (2014).
- Endo, et al., IEEE Photonics, J. 7, 7903418 (2015).
- Endo, et al., Opt. Exp. 24, 8940 (2016).



東京光空間テストベッド
(Tokyo FSO Testbed)

秘匿ドローン通信

衛星光通信
2015年から小型衛星ソクラテスで
実験中、NICT宇宙通信研と連携

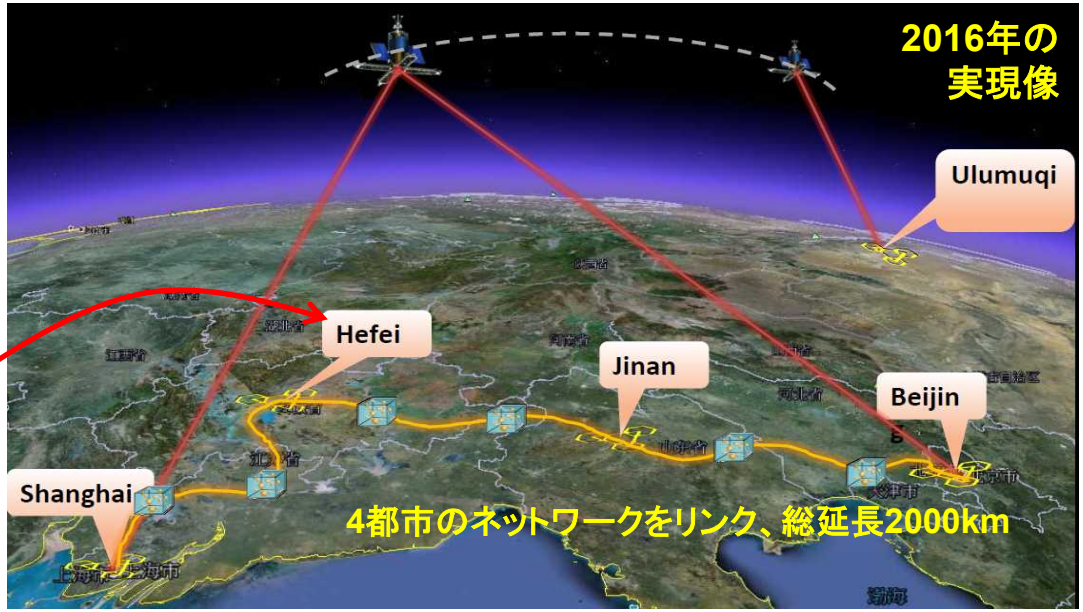
量子通信・暗号技術の現状（海外）1/2　　資料３

中国

新華社
金融通信に量子暗号を実利用
（2012年2月）

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

50ノード級の大規模量子暗号ネットワーク



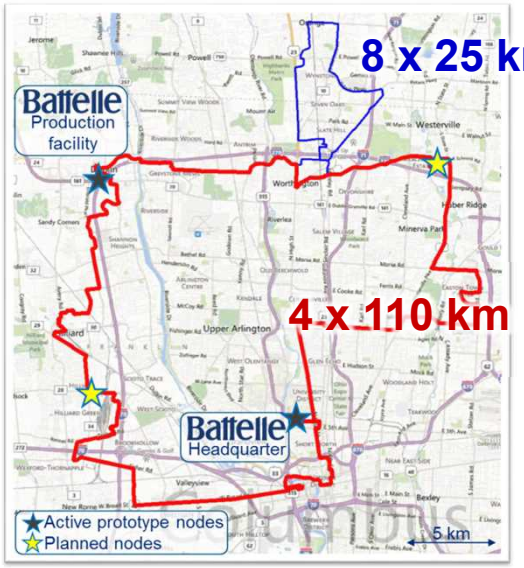
Qiang Zhang氏 (USTC) のご好意による

欧州

G. Ribordy氏のご好意による

ID Quantique社 (CEO:G. Ribordy)
・ジュネーブに本拠地
・金融セキュリティ市場へ参入

米国



Battelle社
ワシントンーオハイオ州都間700kmの量子暗号回線を構築（2015年）、非営利団体の研究者にオープンテストベッドとして開放

Nino Walenta氏(Battelle社) のご好意による

量子通信・暗号技術の現状（海外）2/2　資料 4

英国

Quantum Technology Hubs （2015年から5年間270億円の予定）
量子計算、量子通信、量子計測標準、量子イメージングの4つのHubs

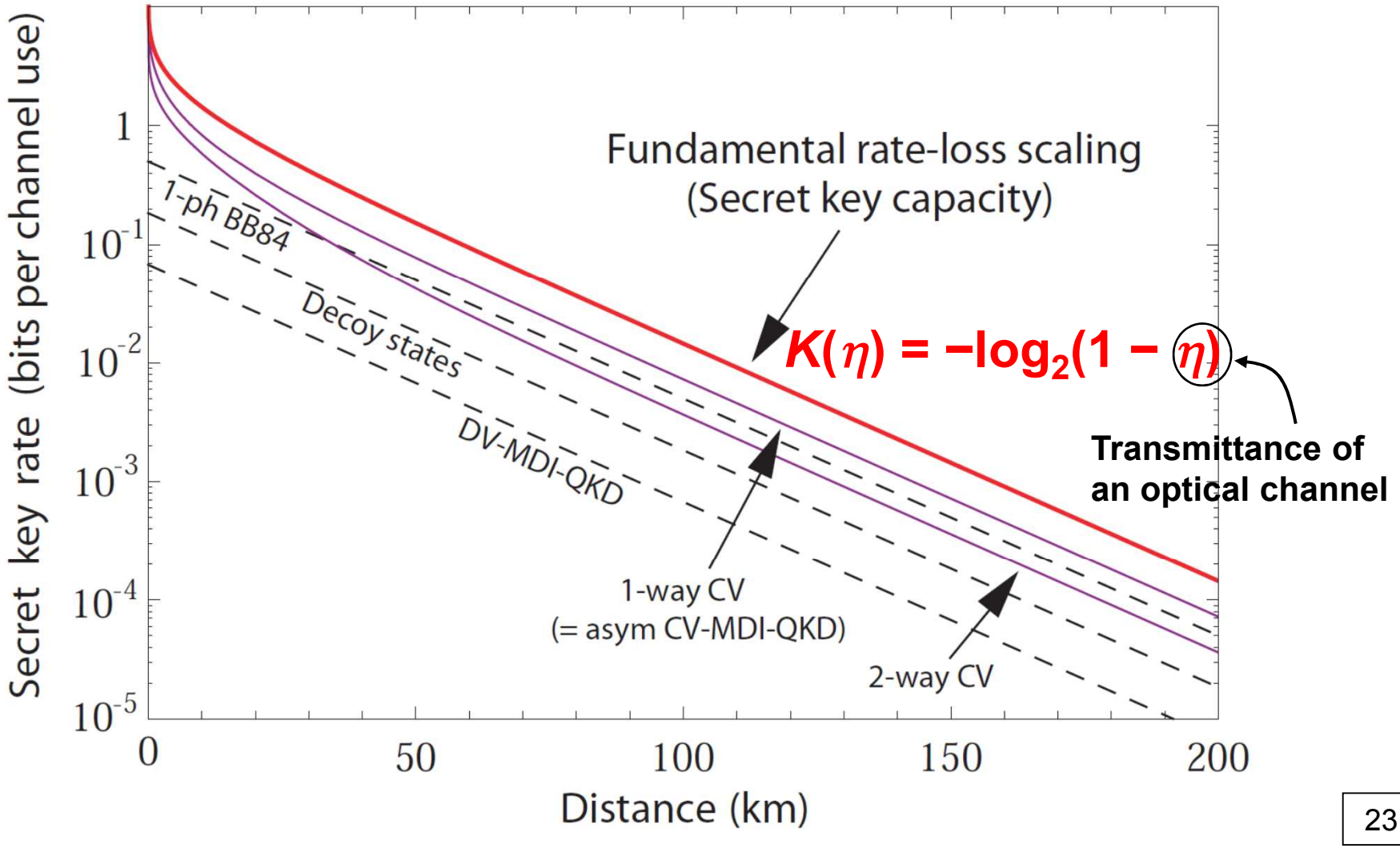
量子通信

・York大、東芝Cambridge、British Telecom、Bristol大、Heriot-Watt大
・ブリストル、ケンブリッジ地区にそれぞれQKDメトロネットワークを形成、
　2都市間をBritish Telecomのダークファイバ280kmで結ぶ構想。
・集積回路技術や小型QKD装置の開発にも積極的に取り組んでいる。

2015年から日本との連携を開始
“UK-Japan Quantum Technology Initiatives”
・定期会合（これまで2回：英国大使館、第3回目は2016年11月ロンドンの予定）
・優れた共同研究の成果が出始めている

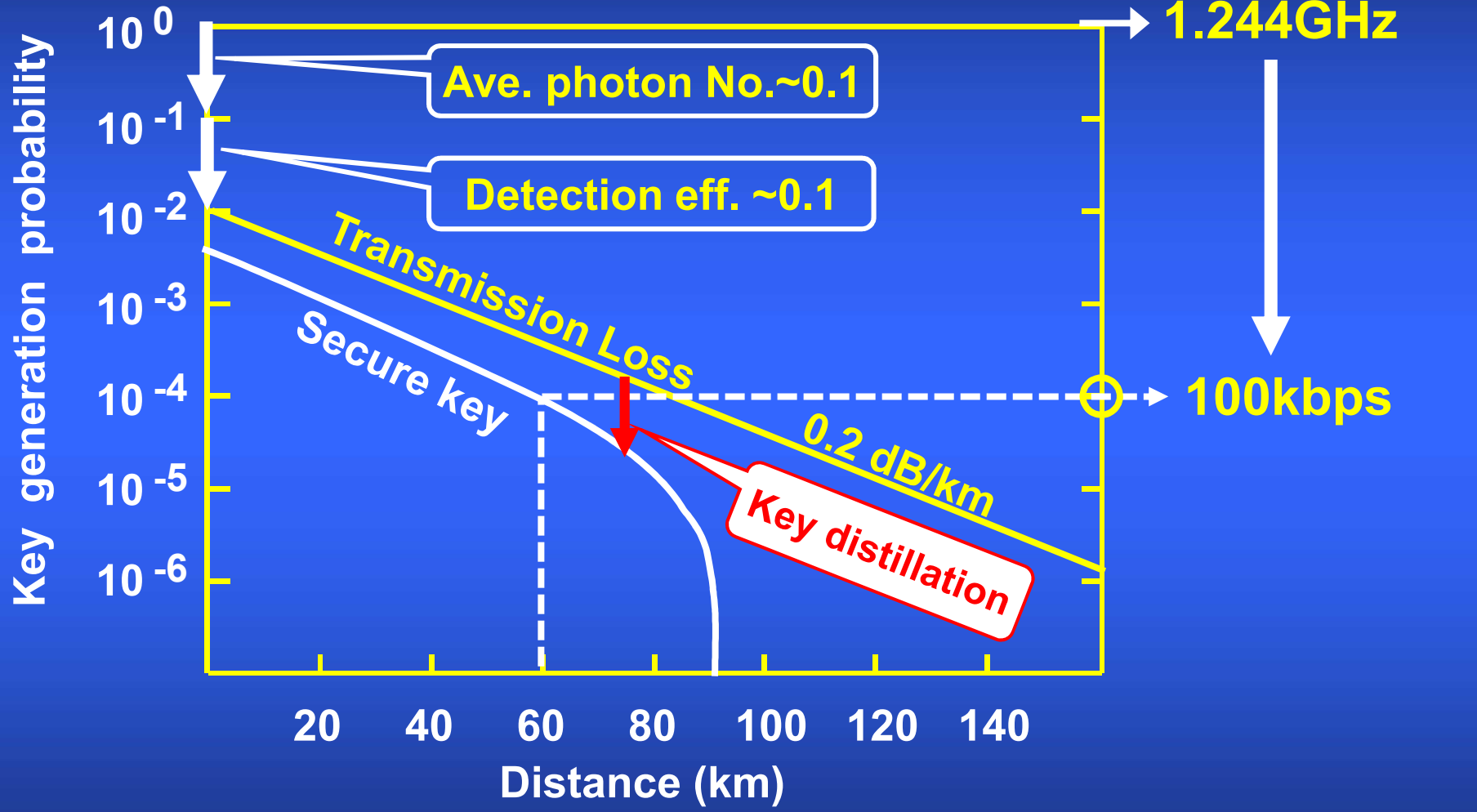
量子暗号の直接リンクの距離と速度に『原理的』な限界がある。
⇒プロトコルをいじっても抜本的解決にはならない。

S. Pirandola, et al., arXiv:1510.08863 [quant-ph]



資料 6

Current QKD performance (Decoyed BB84)



To increase the key rate further apply wavelength division multiplexing to QKD.

量子暗号(QKD)の方式の大まかな分類　資料 7

	量子もつれ型		光子型	光波型
安全証明	装置モデルに対する仮定を緩和、あらゆる攻撃に対して安全	装置モデルに対する一定の仮定のもと、あらゆる攻撃に対して安全	装置モデルに対する一定の仮定のもと、あらゆる攻撃に対して安全	量子一括攻撃まで安全
安全性レベル	極めて高	高	高	中
プロトコル	Device-independent QKD, Measurement-device independent QKD	E91, BBM92	BB84, DPS, Coherent-one way, RR-DPS	Continuous variable
実装形態	量もつれ光子源 ＋ 高感度単一光子検出	量もつれ光子源 ＋ 単一光子検出	コヒーレント光 / 単一光子源 ＋ 単一光子検出	コヒーレント光 ＋ ホモダイン検波
コスト	極めて高	高	中	低
現状	実験室段階	50 bps @20km fiber	300kbps @50m fiber 1 kbps @100km fiber	10kbps @25km fiber