資料３

量子暗号及び関連技術による秘匿空間通信

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

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

2018年5月14日 宇宙政策委員会安全保障部会

内容

- 量子暗号の現状

  安全性、研究開発状況

  利点と問題点

- 量子暗号の要素技術を用いた
  暗号通信の各種シナリオ

  乱数搭載、光リンク、物理レイヤ暗号

- まとめ

量子暗号の安全性

現在の暗号の安全性

計算量的安全性

→ 原理的には計算機で解読できるが、膨大な時間がかかる

計算機能力・アルゴリズムの進歩による危殆化のおそれ

量子暗号で達成できる安全性

情報理論的安全性

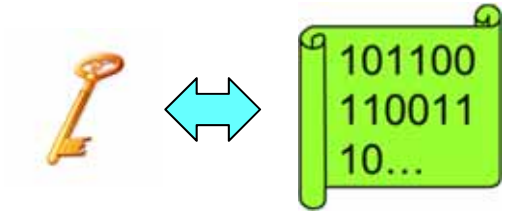
→ **あらゆる計算機を使っても**解読不可
（例え量子計算機を使ったとしても）

（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・排除

暗号

1. 秘密鍵の共有

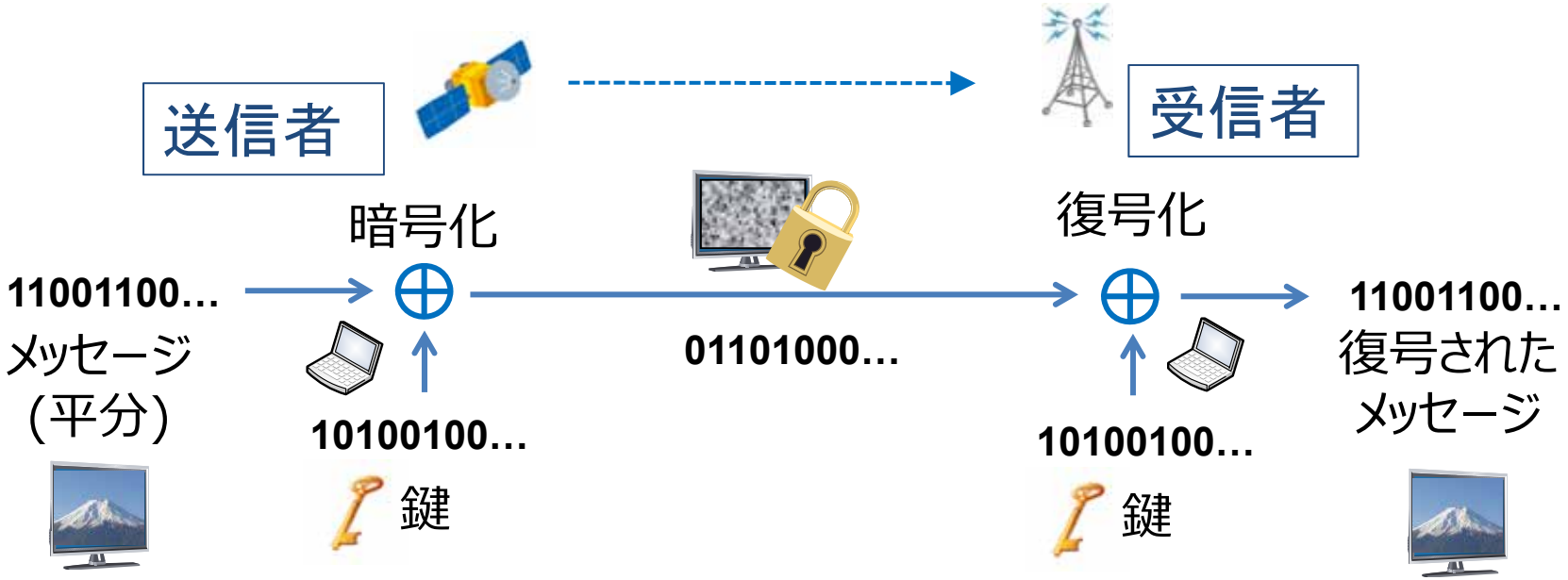


秘密鍵 ＝ 秘密の乱数列

送信者・受信者は、第三者に知られないように秘密の乱数列（鍵）を共有する。

暗号: 離れた場所で秘密鍵を共有する技術

2. データの暗号化



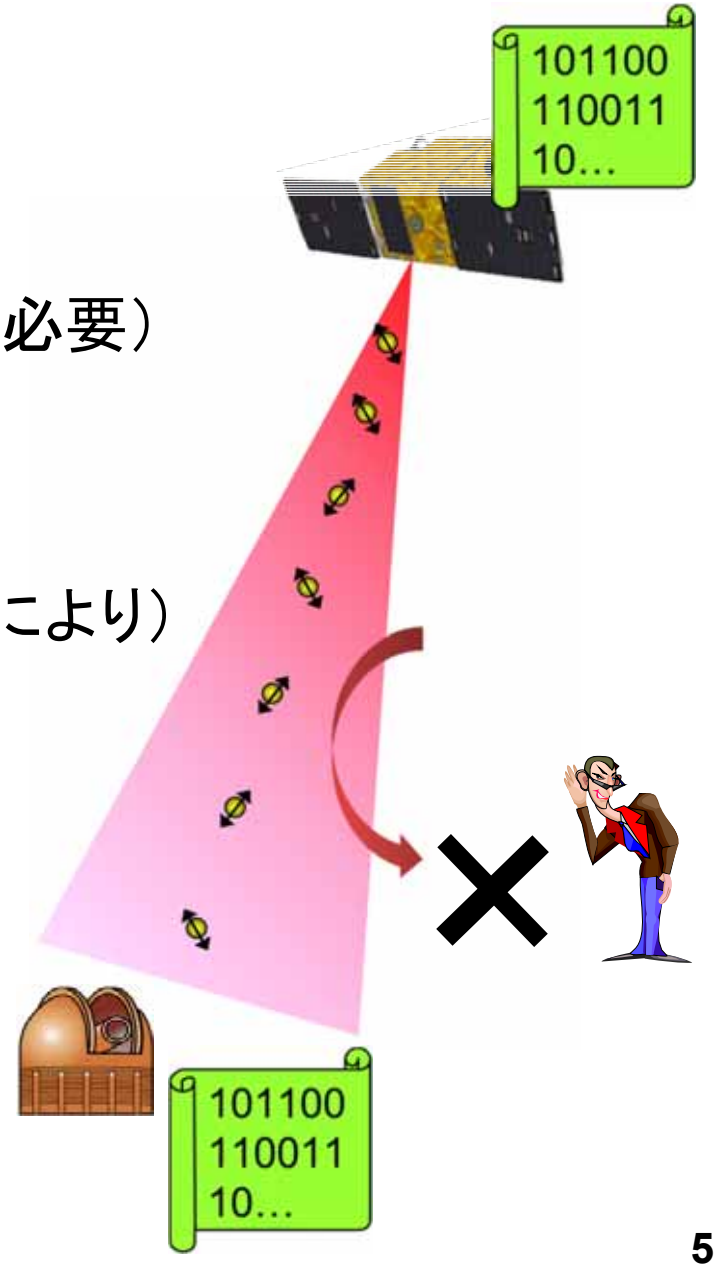
量子暗号（量子鍵配送：QKD）

- 量子鍵配送技術は光通信に立脚

- 違い：乱数列（鍵）は光子で送られる
  （超微弱光の制御技術、光子検出技術が必要）

- あらゆる盗聴攻撃は検知される
  （光子の量子性（分割不可・不確定性等）により）

- QKDによる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
  （量子力学の真のランダム性により）



QKD: Quantum Key Distribution

QKDファイバーネットワーク実証

USA 2004 DARPA Quantum Network (Boston)

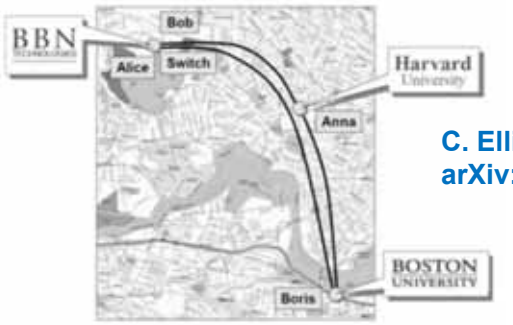


Figure 11: Logical Map of the Cambridge-Area Fiber Network.

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

Europe 2008 SECOQC Network (Vienna)

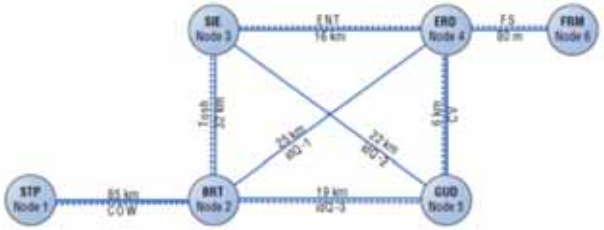
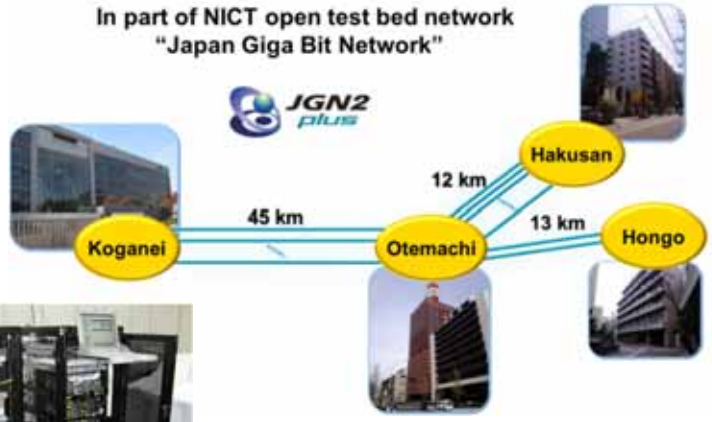


Figure 2. Network topology of the SECOQC QKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.

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

Japan 2010～ Tokyo QKD Network (Tokyo)



QKD sender and receiver (NEC, 2017)

China 2017～ Quantum Backbone Network (Beijing-Shanghai)

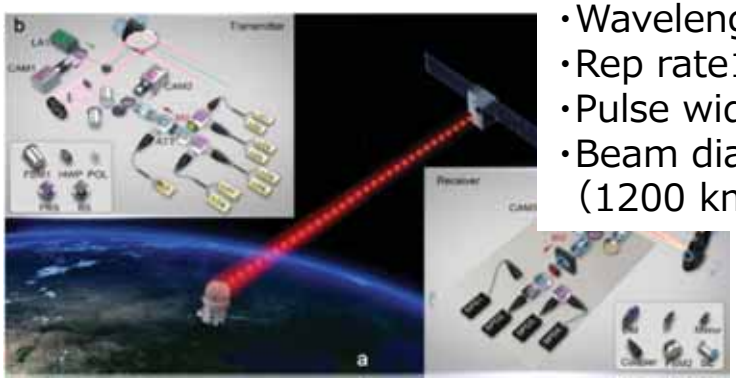
Courtesy by Qiang Zhang (USTC)

衛星量子暗号：中国

Quantum Science Satellite “Mozi” (launched in Aug 2016)

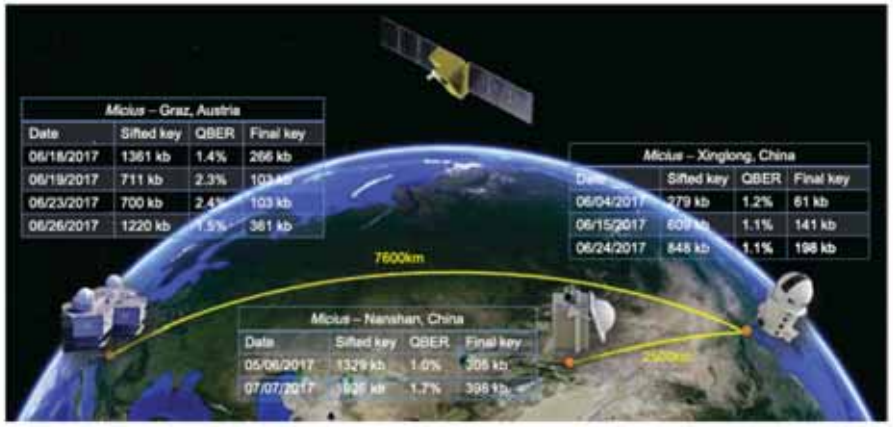
Mozi
（墨子）
600kg

世界初の衛星ー地上QKD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）

世界初の大陸間QKDに成功
Phys. Rev. Lett. 120 030501・
7600 km distance
（China-Austria）
・60-400 kb key generation
・Secure file transfer (5 kB)



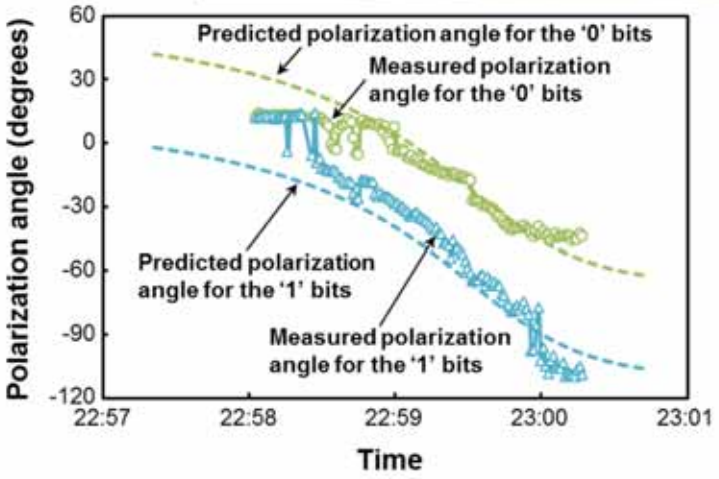
日本の研究開発（NICT）

Low Earth Orbit
650km

超小型衛星SOCRATES (50kg)
developed by AES Corp. and NICT
Launched in May 2014

Small Optical
Transponder (SOTA)
・Mass 5.9kg
・Laser wavelength
0.8mm, 1.5mm
・Repetition rate
10Mbps

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, pp. 502-508 (2017)

実用上の利点と問題点

利点：現状技術で最高の安全性

- あらゆる計算機で解読不可
- あらゆる物理的盗聴が不可

最重要機密の保護

問題点：可用性、コスト

- 距離・速度に原理的な限界（可用性）

  信号光が超微弱（光子レベル）：～10^{-19} J

  ⇨ 現状、低軌道ー地上 数kbpsレベルが限界

- コストの問題

計算機解読不可能性（情報理論的安全性）
を維持しつつ、可用性を高めることはできないか？

実用上の利点と問題点

計算機解読不可能性（情報理論的安全性）
を維持しつつ、セキュリティレベル、運用条件、
コストに見合った暗号通信はできないか？

量子暗号システムの
様々な要素技術を活用

量子鍵配送システムを構成する要素技術

物理乱数生成器

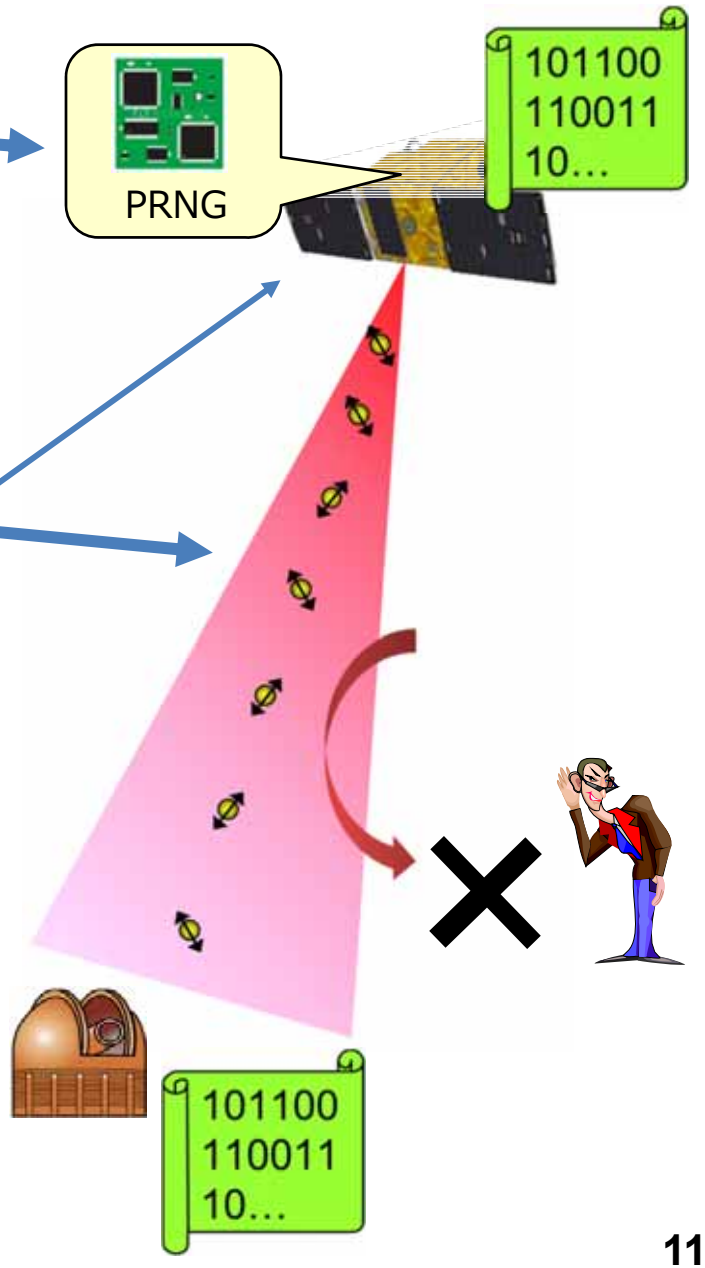
物理現象（電気回路の熱雑音、光の量子雑音等）
から真性乱数を抽出するデバイス

光通信（リンク）技術
光子制御・検出技術

光の量子性を使って盗聴行為
の有無（度合い）を検出

鍵蒸留技術

共有した乱数データの誤り訂正と、
盗聴可能性のあるデータの排除
を行う情報処理プロセス

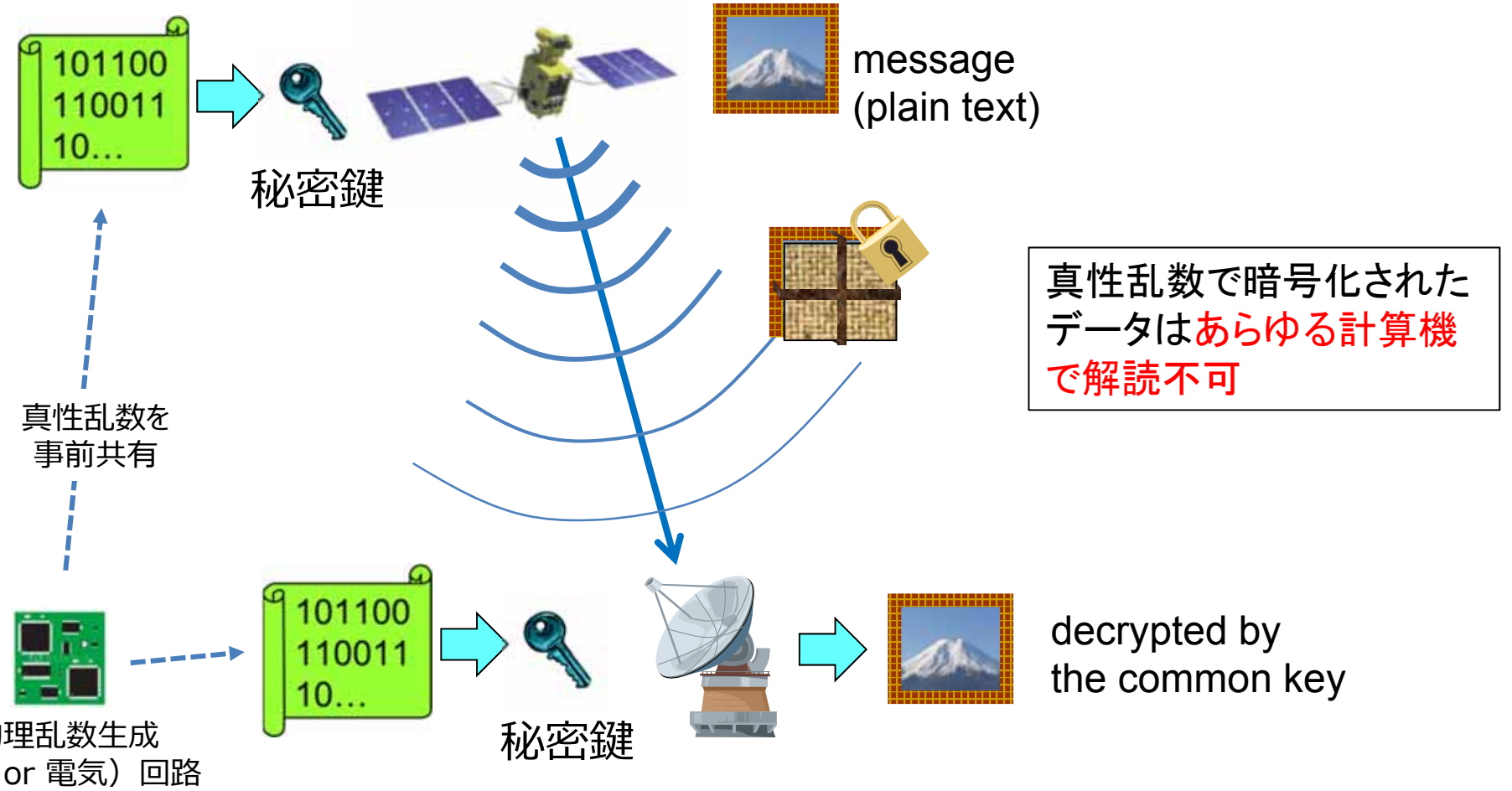


PRNG: Physical Random Number Generator

要素技術を使った秘匿通信 1

物理乱数生成器

送受信者が、事前に（衛星打ち上げ前に）物理乱数生成器で作った秘密鍵（真性乱数）を共有する。

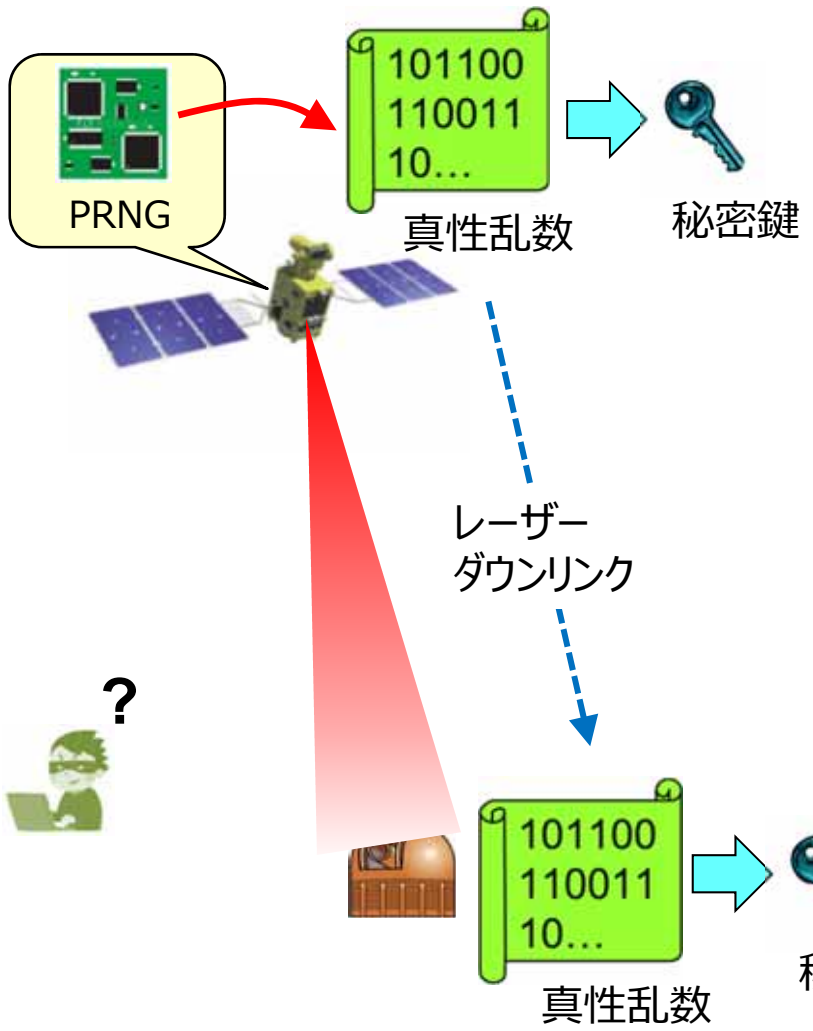


問題点：衛星のメモリサイズは有限 ➡ 短時間空間通信で有効な可能性（ドローン等）

要素技術を使った秘匿通信２

光リンク技術

光空間通信は比較的安全



衛星で真性乱数を生成し、地上へダウンリンク

- 光リンク：フットプリントが小さい
  → 物理的盗聴が難しい
- 高速化が可能
- ライセンスフリー
- 真性乱数をダウンリンクすれば、
  暗号化されたデータは
  あらゆる計算機で解読不可

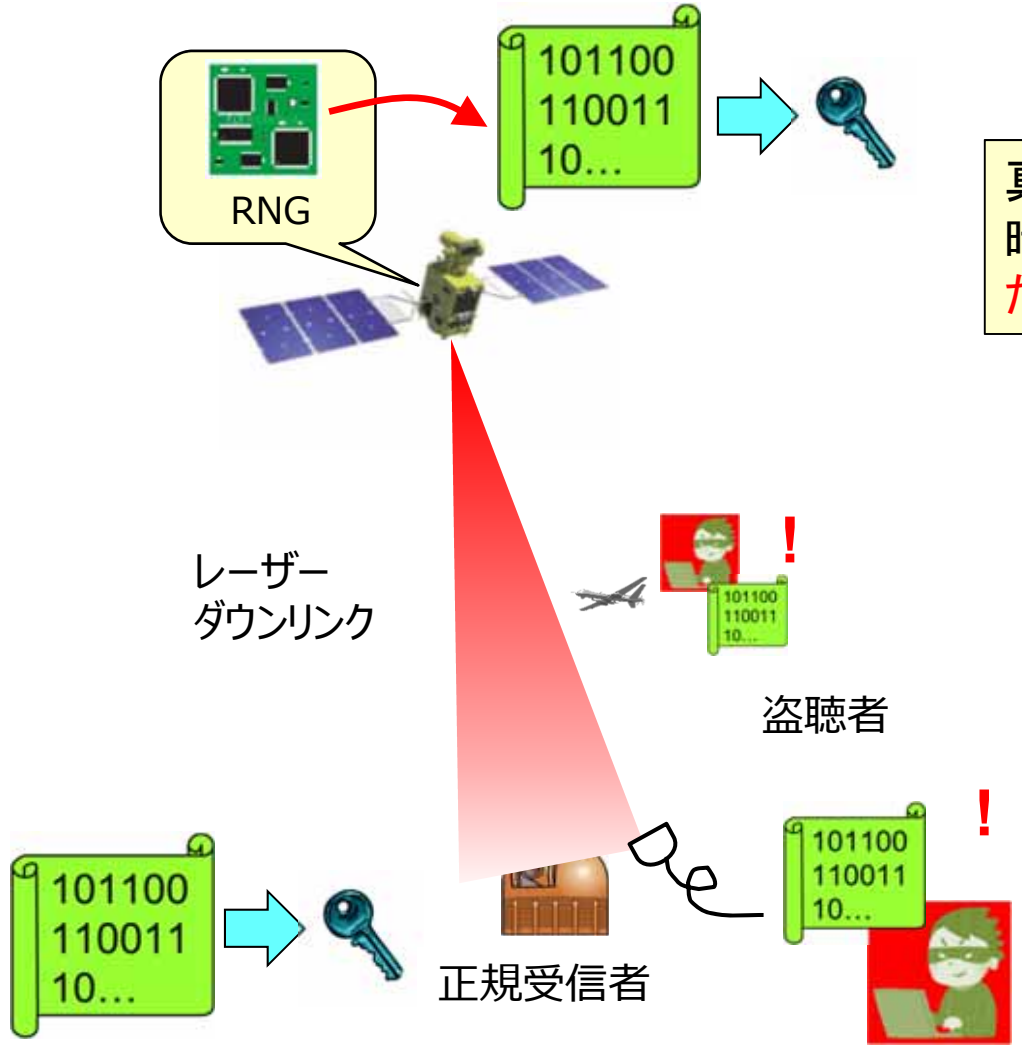
鍵が共有できたら、電波・光等
で暗号化通信を実行

PRNG: Physical Random Number Generator

光リンクの危険性

光リンク技術

光空間通信は比較的安全？



真性乱数を使っていれば、
暗号データは計算機で解読不可
ただし鍵が盗聴されていなければ・・・

光信号の盗聴が不可能とは言い切れない

- ステルス機？
- 正規受信者付近に
  超高感度検出器を設置？

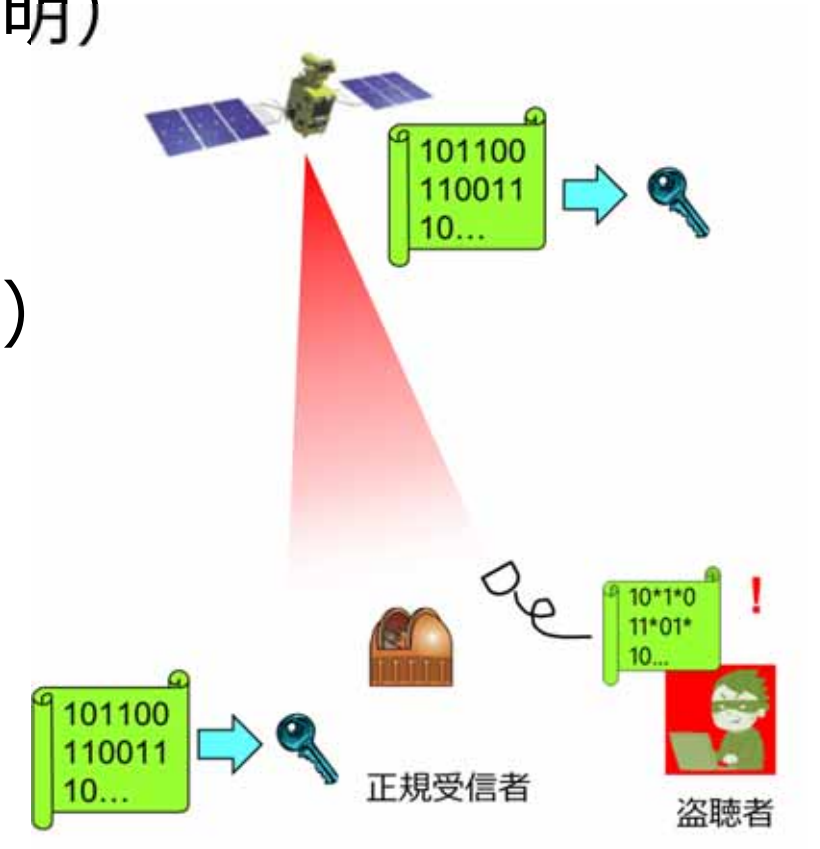
RNG: (Physical) Random Number Generator

鍵蒸留

鍵の情報が部分的に漏れている場合・・・
（どのビットが盗聴されているかは不明）

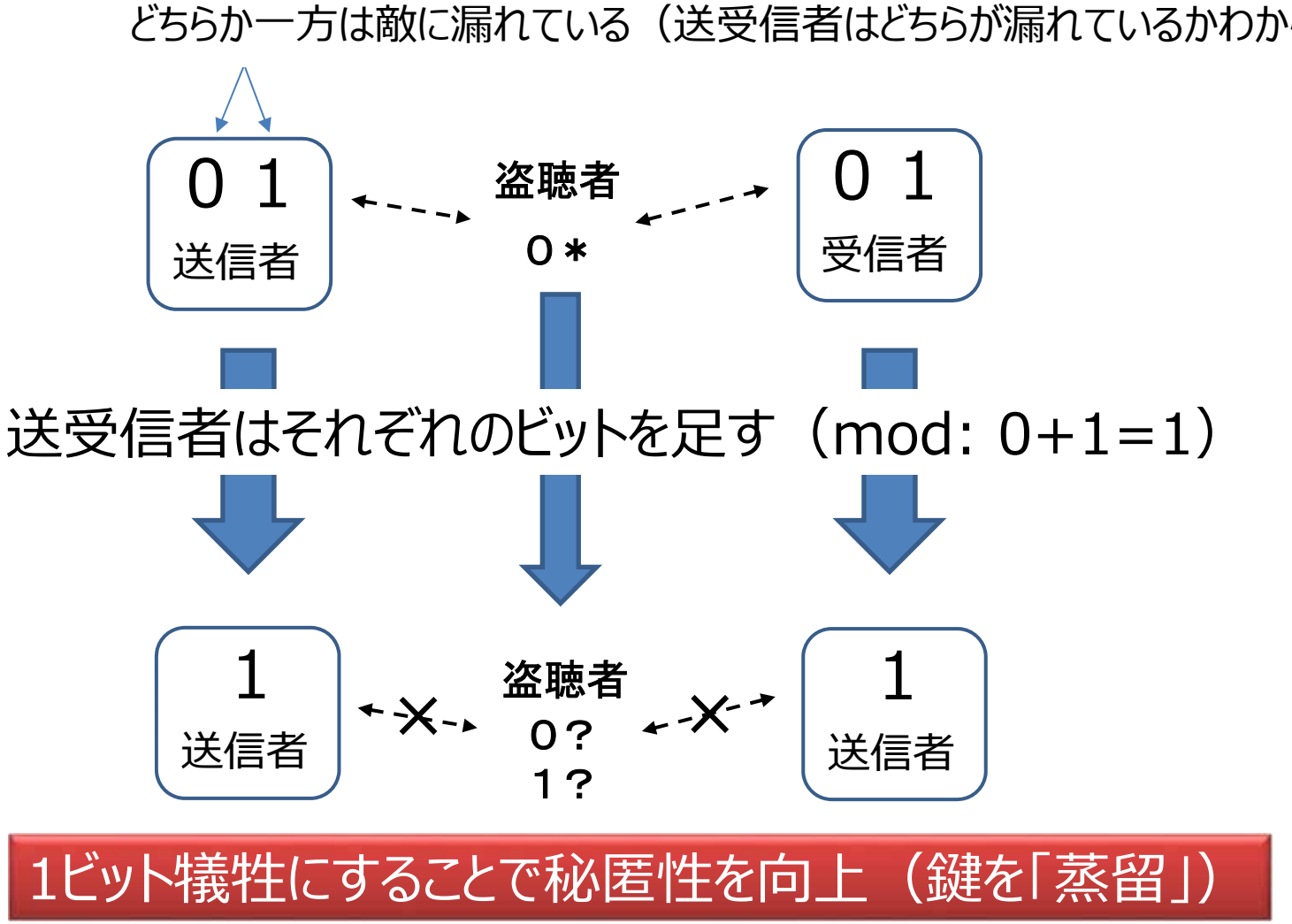
盗聴の恐れがある鍵（乱数ビット）
を取り除くことはできるか？

鍵蒸留により可能



鍵蒸留（秘匿性増強）の例

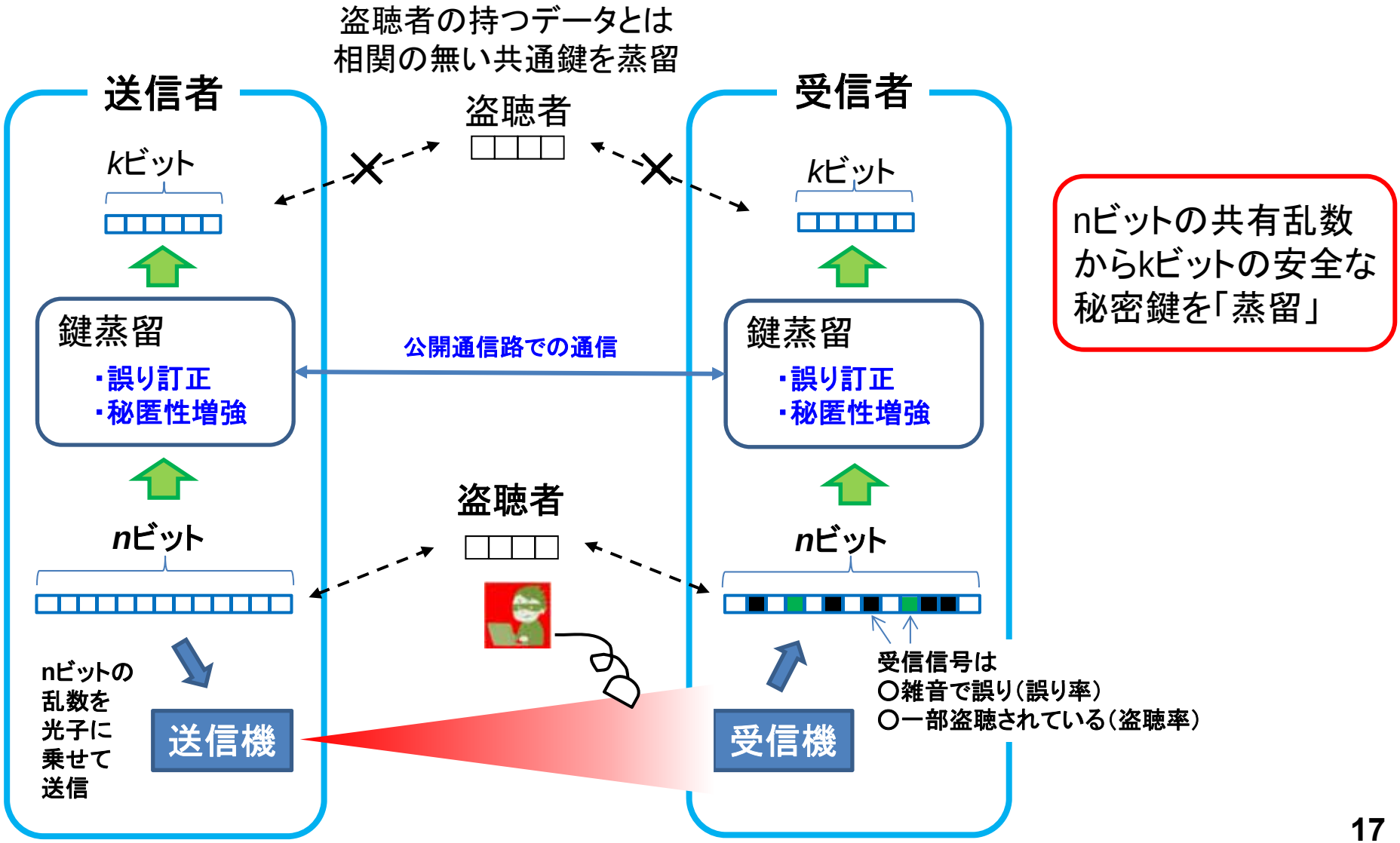
- 送受信者は2ビットの鍵を共有
- そのうちどちらか1ビットは敵に情報が漏れているとする。



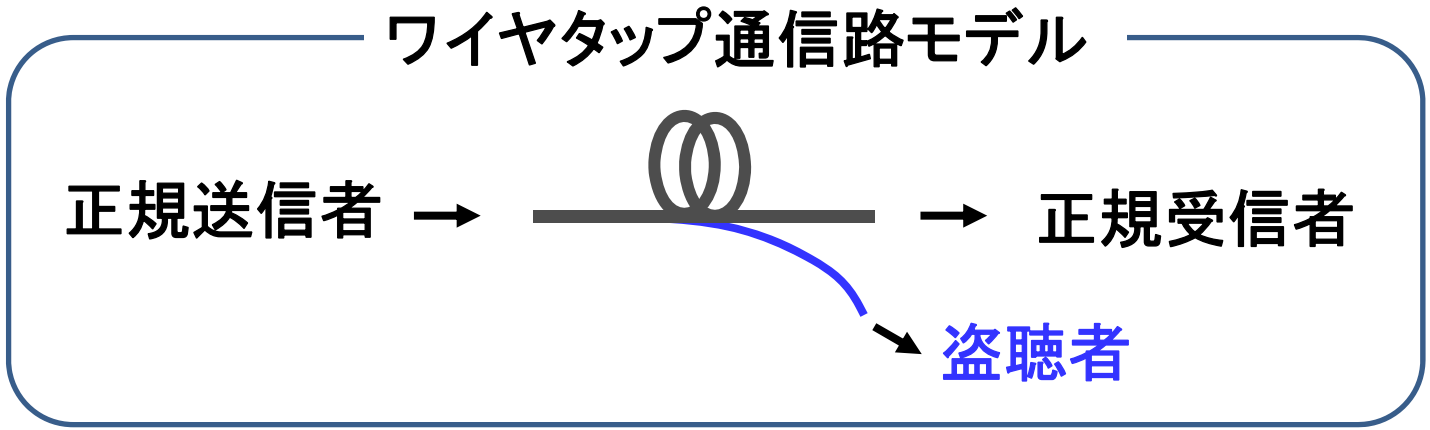
1ビット犠牲にすることで秘匿性を向上（鍵を「蒸留」）

鍵蒸留

- 実際には、ビット列のうちの何%かに盗聴の可能性



物理レイヤ暗号



盗聴者通信路のSN比が見積もれる（仮定できる）場合

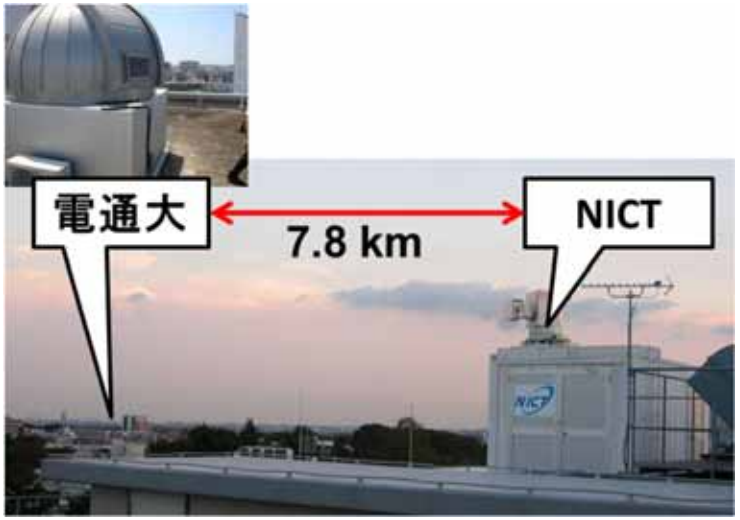
通信路雑音＋鍵蒸留＝ 計算機解読不可な鍵生成が可能

物理レイヤ暗号

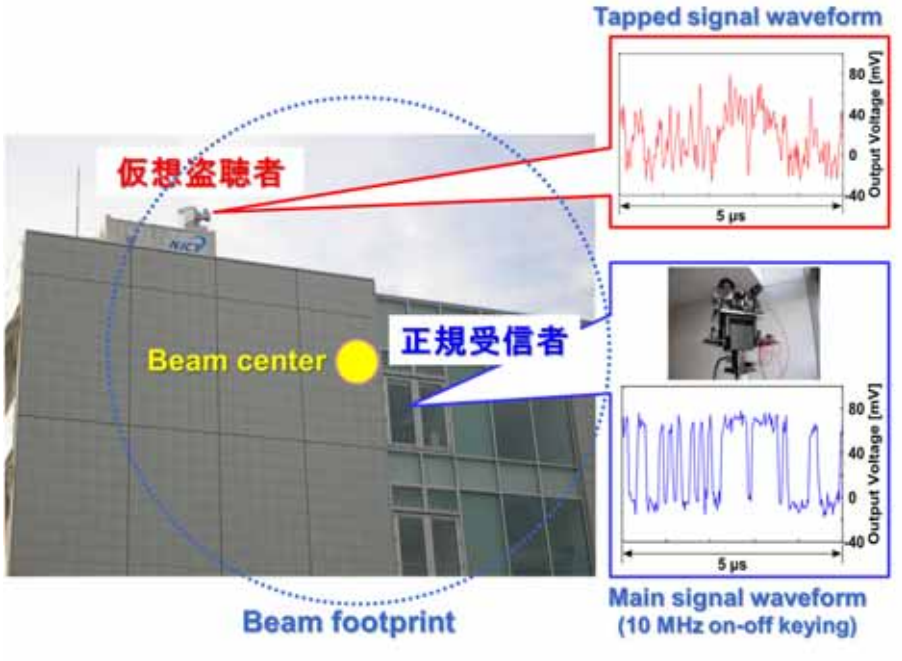
物理レイヤ暗号実装に向けて

- NICT-電通大（7.8km）に空間リンクを構築
- 光リンク物理レイヤ暗号に向けた基礎実験を開始

H. Endo, et al., Optics Express 24, 8940 (2016)



NICT-電通大
光空間通信テストベッド



正規受信者・仮想盗聴者の信号データ

課題：盗聴者の攻撃能力の妥当な仮定とは？

⇨ 具体的なユースケースに大きく依存

まとめ

- 量子暗号（量子鍵配送：QKD）
  - 究極の安全性（計算機で解読不可・物理的攻撃を必ず検知）
  - 距離・速度に限界（用途が限定）

- 物理レイヤ暗号（QKDの要素技術を活用）

光リンク＋鍵蒸留（＋物理乱数生成） ⇒ 計算機で解読不可

  - 高速化可能（光通信に準ずる。～Gbps）
  - 計算機による解読不可
  - 物理的攻撃能力に仮定が必要
  - 基本的には電波にも応用可（EHF？）

⇒ ユースケース（要求条件）に応じた設計・研究開発が必要

Future outlook