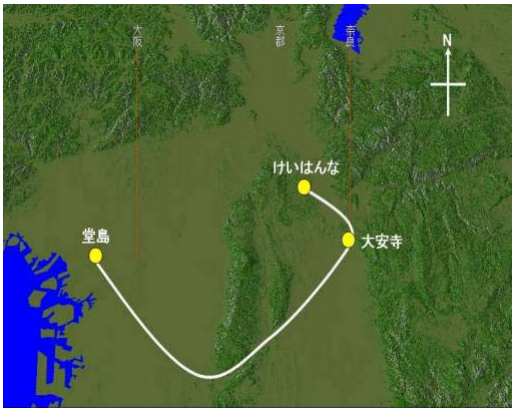
MITSUBISHI 三菱電機

Changes for the Better

JGN2光テストベッドを用いた 量子暗号システム試験



三菱電機株式会社
情報技術総合研究所　清水克宏

MITSUBISHI 三菱電機

アウトライン

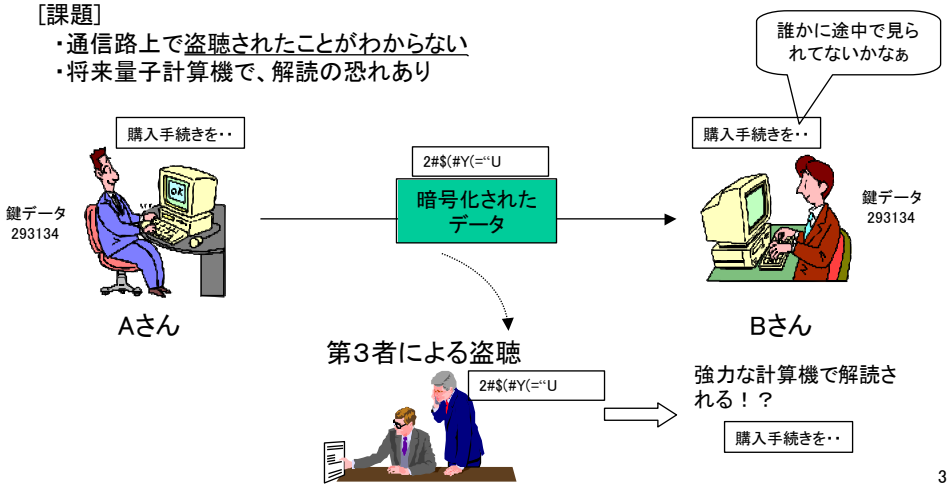
Changes for the Better

1. **量子暗号システムとは？**
   - 現代暗号技術と量子暗号技術
   - 量子暗号と光通信
2. **量子暗号システムの動作原理**
   - 量子暗号鍵配布システムの動作原理
   - 伝送距離と鍵配布速度のトレードオフ
   - 長距離化と高速化への技術課題
3. **フィールド試験の意義**
   - 当社のこれまでの取り組み
   - フィールド試験の意義
4. **試験結果**
   - 試験系と適用装置
   - 試験結果
5. **今後の展開**

現代暗号技術と量子暗号技術

現代暗号の仕組みと課題

[現代暗号のしくみ]
・秘密の鍵データで暗号化/復号化処理を行う
・鍵データは秘密に保つ
[課題]
・通信路上で盗聴されたことがわからない
・将来量子計算機で、解読の恐れあり



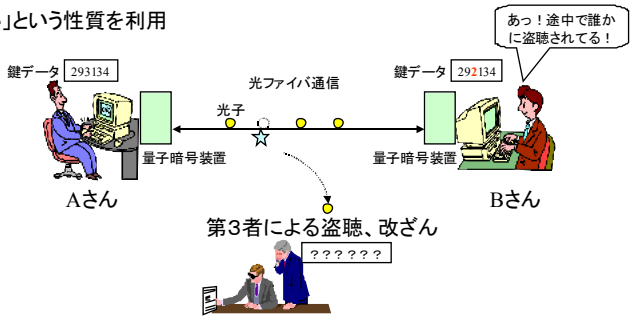
現代暗号技術と量子暗号技術

量子暗号

量子力学の基本的性質を利用した、解読が不可能な究極の暗号技術。
[特徴]
通信路上での盗聴を検知可能。
量子力学の不確定性原理により、安全な鍵共有と暗号通信が実現。

量子暗号の本質の物理法則

「系は観測により必ず影響を受けて変化する」、「未知の量子状態を複製(cloning)することはできない」という性質を利用

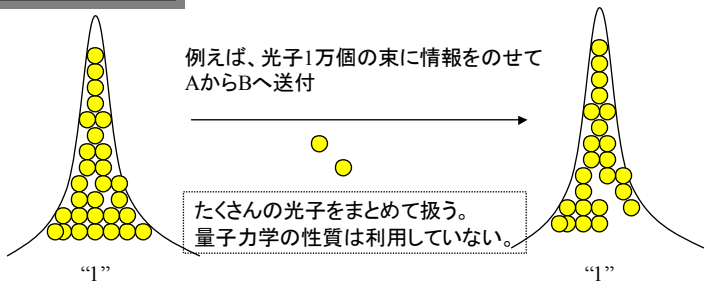


MITSUBISHI 三菱電機

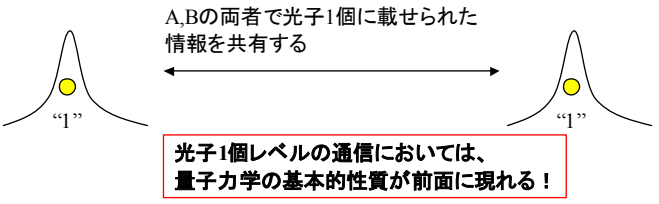
量子暗号と光通信

Changes for the Better

通常の光通信（強い光）



量子暗号（微弱光）



光子1個レベルの通信においては、
量子力学の基本的性質が前面に現れる！

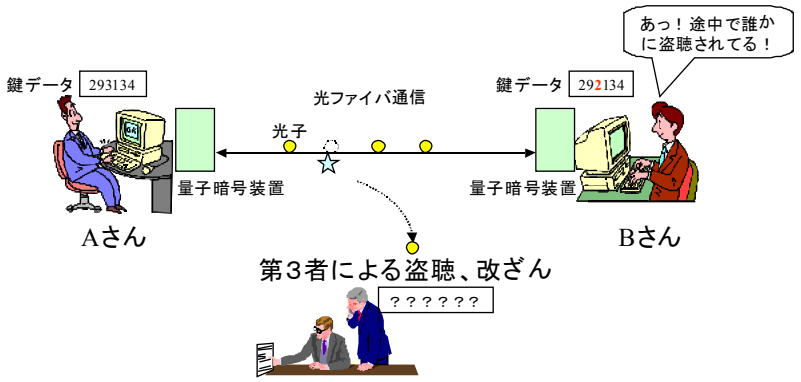
MITSUBISHI 三菱電機

量子暗号システムの仕組み

Changes for the Better

量子暗号鍵配布システム

「系は観測により必ず影響を受けて変化する」、「未知の量子状態を複製(cloning)することはできない」という性質を利用した暗号鍵共有手段



AさんからBさんへ暗号鍵を送付する仕組みではない。
AさんからBさんへ微弱光パルス列を送付することで、結果として、AさんとBさんがある長さのビット列を共有できる。

MITSUBISHI 三菱電機

光量子暗号鍵配布システム

Changes for the Better

量子暗号鍵配布システム＝1フォトン干渉実験

送信者の変調ϕ_A

“π”測定系

ビット	0	1
位相	0	π

“π/2”測定系

ビット	0	1
位相	π/2	3π/2

$\Delta\phi=\phi_A-\phi_B$の値によって
MZIの出力が変化

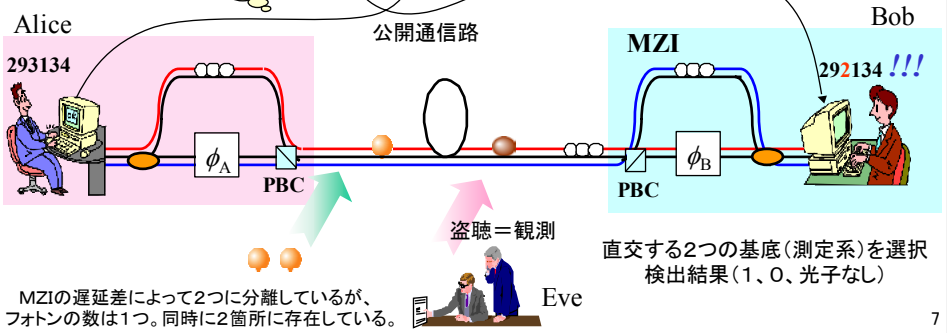
受信者の変調ϕ_B
（測定系を選択）

測定系	“π”	“π/2”
位相	0	π/2

測定系が一致したときには暗号鍵を共有できる

測定系が一致しないときはデータを破棄

使用測定系を情報交換



直交する2つの基底（測定系）を選択
検出結果（1、0、光子なし）

MZIの遅延差によって2つに分離しているが、
フォトンの数は1つ。同時に2箇所に存在している。

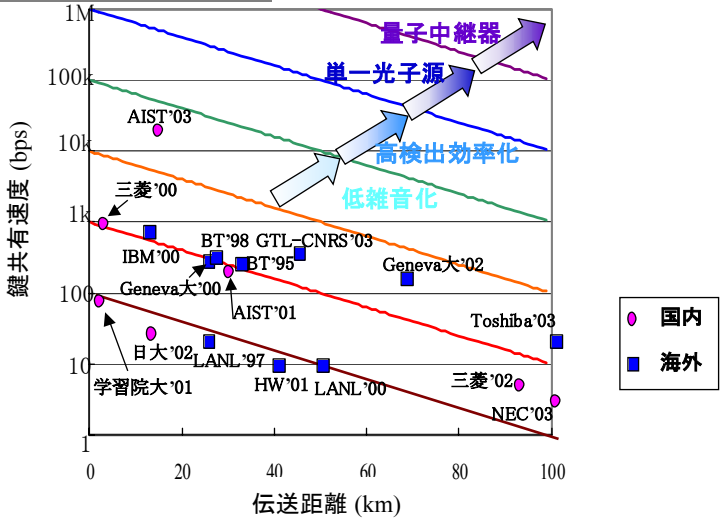
MITSUBISHI 三菱電機

伝送距離と鍵共有速度のトレードオフ

Changes for the Better

128ビットの暗号鍵を10秒毎に交換していけば限りなく安全　＝10bpsでもOK
暗号鍵の長さと情報量が一致しているときが究極の安全　＝　早ければ早いほどよい

主な量子暗号実験（実験室）



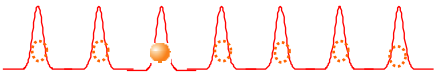
MITSUBISHI 三菱電機

伝送距離・速度の制限要因

Changes for the Better

損失 ⇐ 検出器に届く光子の数が減少

- 伝送路・光学系の損失 η_t
- 光子検出器の検出効率 η_d
- 1パルス当たりの平均光子数 $\mu < 1$ (/pulse)



ex. η_a=10dB(～50km), η_d=10%, μ=0.1/pulse, 光源繰返し=1GHzの場合

⇒ R_{raw} ～$10^{-10/10} \times 0.1 \times 0.1 \times 10^9$

～ **1 Mbps**

QBER ⇐ 誤り訂正、秘匿性増強に必要なオーバーヘッドが増大

- APD光子検出器の暗計数(dark-count)
  - 光子がないのにも関わらず信号パルスが発生する（背景雑音）
    信号1パルス当たりに暗計数が発生する確率→暗計数率 p_{dark}
- アフターパルス(after-pulse)
  - 光子検出された後ゲートパルス印加すると、光子がないのにも関わらず信号パルスが発生する（光源繰り返し時間に依存）
    →アフターパルス計数率 p_{after}
- 干渉計、Rayleigh散乱、迷光など、その他光学系による誤り

MITSUBISHI 三菱電機

高速化・長距離化への技術課題

Changes for the Better

光子検出技術

- 長距離伝送に適する**長波長帯**で高効率な小型光子検出器
  （電子冷却による小型化/温度制御パラメータの最適化）
- 長距離伝送と高速伝送を実現する光子検出技術
  （**暗計数** と **アフターパルス**の低減）

単一光子発生技術

- 現在はレーザーを光源として微弱光にして使用
  （1パルス当たりの平均光子数は0.1個以下）
- 単一光子源はまだ研究段階
  ー量子ドットデバイス
  ーパラメトリック下方変換による双子の光子（もつれ合い状態）
  →単一光子源の使用により通信速度は10倍になる

量子中継技術

- 中継なしでは通信距離100km程度が限界
  →量子テレポーテーションなどにより光子の量子状態を中継することが可能に

MITSUBISHI 三菱電機

当社のこれまでの取り組み

Changes for the Better

1. 国内初、量子暗号通信システム実験に成功（2000年9月）
2. 世界最長距離87kmでの量子暗号通信システム実験に成功（2002年11月）
3. 国際展示会 ITU TELECOM WORLD 2003に量子暗号装置を出展（2003年10月）
4. JGN2光テストベッドを用いた量子暗号システムのフィールド試験に成功（2004年11月）

87km量子暗号通信システム

国際展示会TELECOM2003@Geneva

MITSUBISHI 三菱電機

フィールド試験の意義

Changes for the Better

フィールド試験と実験室試験の差異

	フィールド試験	実験室内
1. 温度変化の影響	×大きく影響受ける	○影響受けず
2. 光学反射・偏波変動の影響	×大きく影響受ける	○影響小
3. 既設ファイバー結合損失の影響	×損失大	○損失小
3. 遠距離2点間での通信確認	×必要（困難）	○容易
4. 耐久性	×安定性検証要	○安定環境

⇨ システムの成熟度・実用化検証にはフィールド試験が不可欠

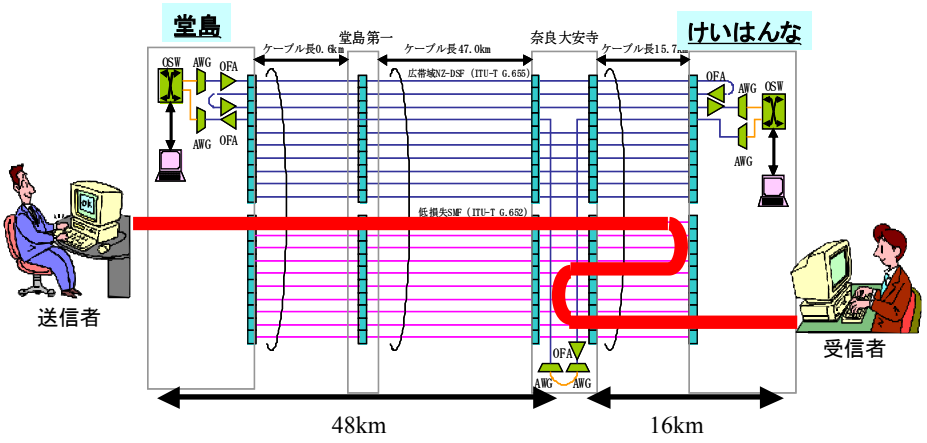
フィールド試験に適用できる装置の条件

(1)持ち運び可能なまで小型・軽量であること
(2)物理的に遠距離2地点で安定動作可能なこと
(3)温度変化/種々の揺らぎ擾乱を吸収できること
(4)種々の装置パラメータを柔軟に調整可能なこと
(5)耐久試験用にログを容易に保存できること

フィールド試験

概要

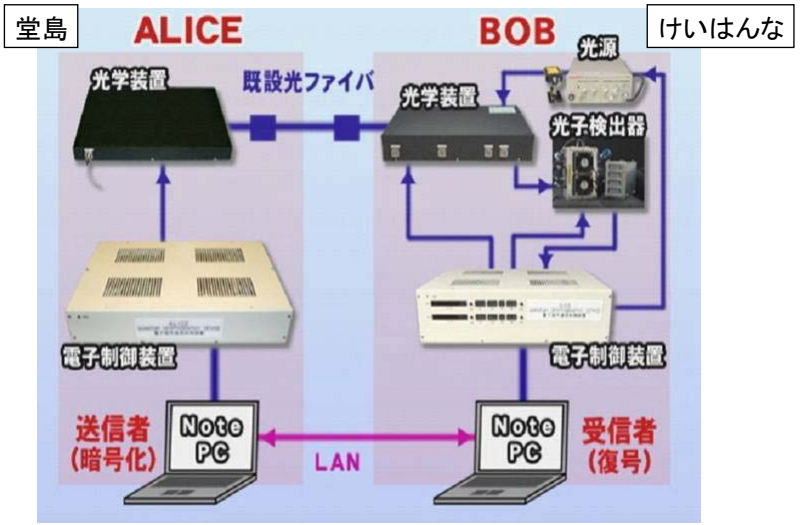
JGNII 光テストベッドを利用し
堂島(大阪) - けいはんな(京都) 間で64km、
（堂島– けいはんな）＋（けいはんな－大安寺）往復で96kmのフィールド試験を実施



（NICT殿ご提供資料を一部修正） 13

フィールド試験

システム構成



フィールド試験

試験パラメータ

	堂島– けいはんな)	堂島– 大安寺– けいはんな
通信距離 L(km)	64	96
光の波長 λ(nm)	1550 nm	
平均光子数 μ(c/pulse)	0.1 photon/pulse	
レーザーの繰返し周波数 ν(MHz)	1 MHz	
検出器の動作温度 T(K)	203 K	
検出器デッドタイム値 T_{dead} (μsec)	10 μsec	

適用した量子暗号装置

高性能な電子制御装置

・遠方2地点で動作可能な光同期通信機能(環境による時間揺らぎを補償)
・駆動周波数を柔軟に調整可能(1MHz～10MHz)
・MISTYなどの現代暗号と組み合わせた統合システムを実現
・BBBSS方式に加え、LDPC符号を用いた誤り訂正方式を実装

受信者側の高性能電子制御装置

MITSUBISHI 三菱電機

小型化した光学系・検出器

Changes for the Better

(1) 小型光学モジュール

・量子暗号の構成光部品を集積化
  - 位相変調器
  - 偏光ビームスプリッタ など

例）受信者側の小型光学装置

(2) 可搬な小型検出器

・ペルチェ冷却による装置の小型化
・-80℃までの高性能な低温冷却

例）小型ペルチェ冷却での高性能検出器

MITSUBISHI 三菱電機

試験結果

Changes for the Better

実験成果

1. 世界最長96kmでの量子暗号フィールド試験に成功
   ・大阪-奈良-京都を通る既設光ファイバ96kmで実現し、従来記録67kmを更新
   ・鍵共有速度は8.2bps ＠平均光子数 ＝ 0.1、誤り率＝9.9%

2. 64kmでの量子暗号フィールド試験では高速動作を検証
   ・既設光ファイバ64kmで高速な動作を検証
   ・鍵共有速度は21.5kbps ＠平均光子数 ＝ 0.1、誤り率＝4.7%

3. 安全性と実用性を備えた通信システムを実証
   ・遠距離通信向けに光同期機能を開発し、高い安定性を実現
   ・量子暗号を鍵配布に用い、その鍵を用いて当社MISTY暗号で高速暗号化

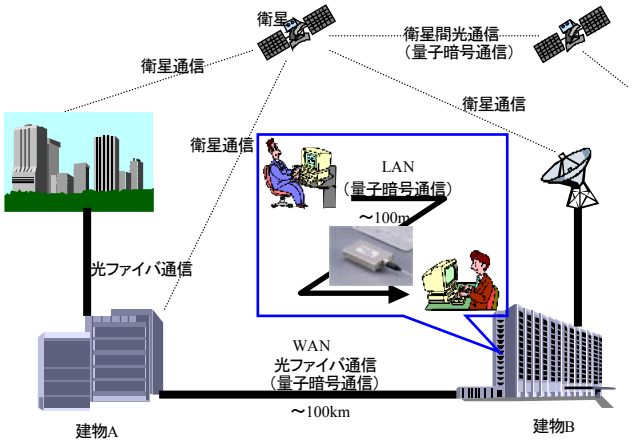
4. 実用化に向け光学系や検出器等を持ち運び可能な大きさまで小型化
   ・光学系を小型モジュール化，ペルチェ冷却による検出器の小型化

MITSUBISHI 三菱電機

今後の展開

Changes for the Better

1. システムのさらなる高速化・長距離化を推進
2. システムの信頼性・長期安定性を引き続き検証
3. 軍事・官公庁・金融システムから実用化検討を開始



MITSUBISHI 三菱電機

まとめ

Changes for the Better

1. 世界最長距離での量子暗号フィールド試験に成功

・JGN2光テストベッドを用いて、従来記録67kmを大幅に更新

[システム性能]

通信距離： 96 km（世界最長距離）

ビットレート： 8.2 bps ＠平均光子数： 0.1

2. 安全性と実用性を備えた通信システムを実証

・既存の光通信技術を融合し安定性を向上し，
安全かつ実用的な2段階方式の通信システムを実証

3. 実用化に向け光学系や検出器等を持ち運び可能な大きさまで小型化

・光学系を小型モジュール化，ペルチェ冷却による検出器の小型

本研究は、総務省「量子情報通信技術の研究開発」の一環である情報通信研究機構の
委託研究「量子暗号技術の研究開発」として実施されたものである。