代表的な直接伝送型QKDと長距離QKD

NTT未来ねっと研究所　川上駿

2024/7/17

自己紹介

所属：NTT未来ねっと研究所　フロンティアコミュニケーション研究部
役職：研究主任
学歴：工学博士
略歴：

学歴・職歴	業務内容
2012-2017 東京大学大学院　物理工学専攻（修士・博士課程）	量子暗号の安全性に関する理論研究
2017-2019 某研究開発法人	総括業務（企画・調整等）
2019-2023 某人材系企業	機械学習エンジニアリング
2024- NTT未来ねっと研究所	量子通信の理論とシステム化

Copyright 2024 NTT CORPORATION

NTT R&D組織構成

- IOWN総合イノベーションセンタ(IIC)【S】
  - IOWNプロダクトデザインセンタ(IDC)【S】
  - ネットワークイノベーションセンタ(NIC)【M T Y】
  - ソフトウェアイノベーションセンタ(SIC)【M S】
  - デバイスイノベーションセンタ(DIC)【A Y】
- サービスイノベーション総合研究所(SV総研)【Y】
  - 人間情報研究所(人間研)【Y TM】
  - 社会情報研究所(社会研)【M Y】
  - コンピュータ＆データサイエンス研究所(CD研)【Y M TM】
- 情報ネットワーク総合研究所(NW総研)【M】
  - ネットワークサービスシステム研究所(NS研)【M】
  - アクセスサービスシステム研究所(AS研)【T Y M】
  - 宇宙環境エネルギー究所(SE研)【M】
- 先端技術総合研究所(先端総研)【A】
  - 未来ねっと研究所(未来研)【Y】 ← 量子通信
  - 先端集積デバイス研究所(先デ研)【A】
  - コミュニケーション科学基礎研究所(CS研)【K A】
  - 物性科学基礎研究所(物性研)【A】
- 知的財産センタ(知財C)【M】
- NTT Research, inc.【U】
  - 量子計算科学研究所(PHI)【U】
  - 暗号情報理論研究所(CIS)【U】
  - 生体情報処理研究所(MEI)【U】


武蔵野研究開発センタ【M】


筑波研究開発センタ【T】

NTTResearch


北米R&D
NTT Research, inc.【U】


NTT京阪奈ビル【K】


品川シーズンテラス【S】


厚木研究開発センタ【A】

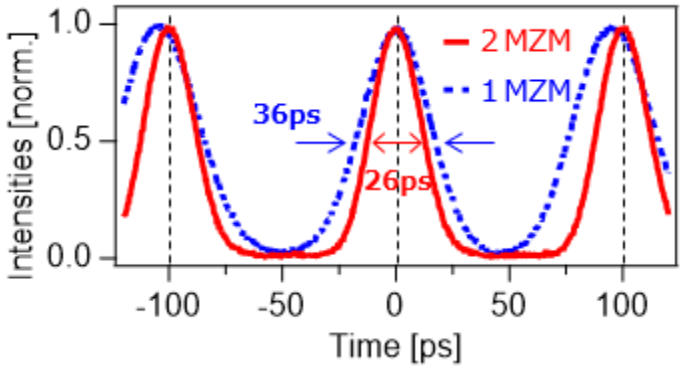

横須賀研究開発センタ【Y】


田町グランパーク【TM】

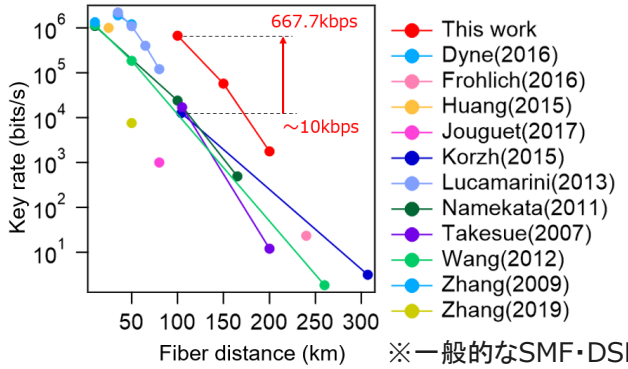
Copyright 2024 NTT CORPORATION

NTT未来研の量子通信に関する取り組み例

送信側のパルス生成方法を改良



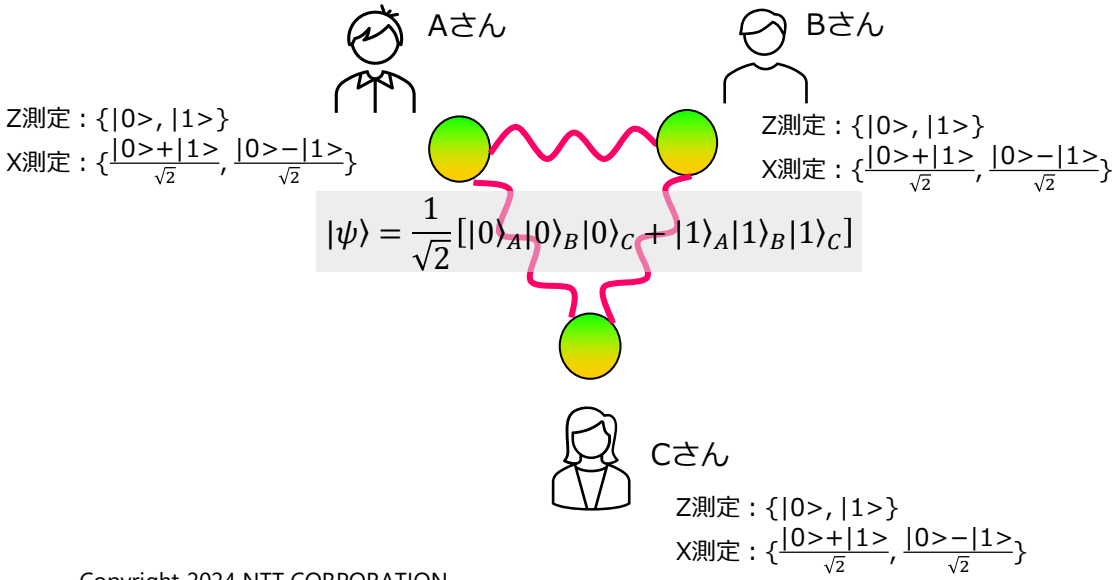
QKDの先行研究※と比較し高い鍵レートを実現

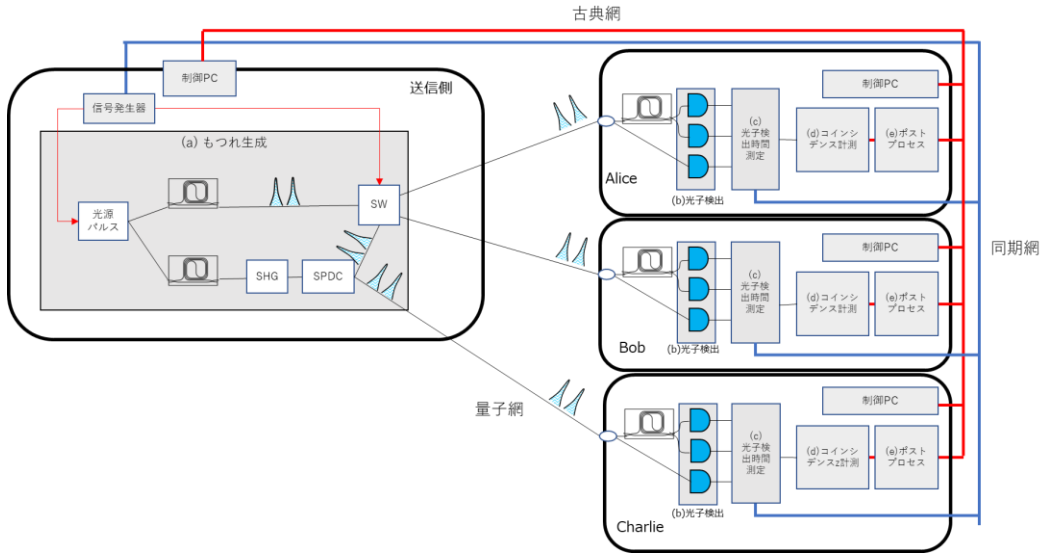


※一般的なSMF・DSF伝送の先行研究のみを比較

[佐成らによってQIT49(2024)で発表]

多者間量子もつれを用いた鍵共有プロトコルのシステム化（総務省委託研究 2023~進行中）





Copyright 2024 NTT CORPORATION

第一部：代表的な直接伝送型QKD

量子暗号の位置づけ

現代暗号の課題

計算量的安全性に準拠
・計算能力の進歩による脅威
・新アルゴリズム（特に量子）の登場による脅威

解決策１

耐量子暗号（計算量的安全性）：
現在知られている計算能力、量子アルゴリズムでは解けないと思われる問題を使った暗号

解決策２

量子暗号（**情報論的安全性**）：
量子力学の原理を正しいとすれば将来に渡って情報論的安全性が証明できる暗号

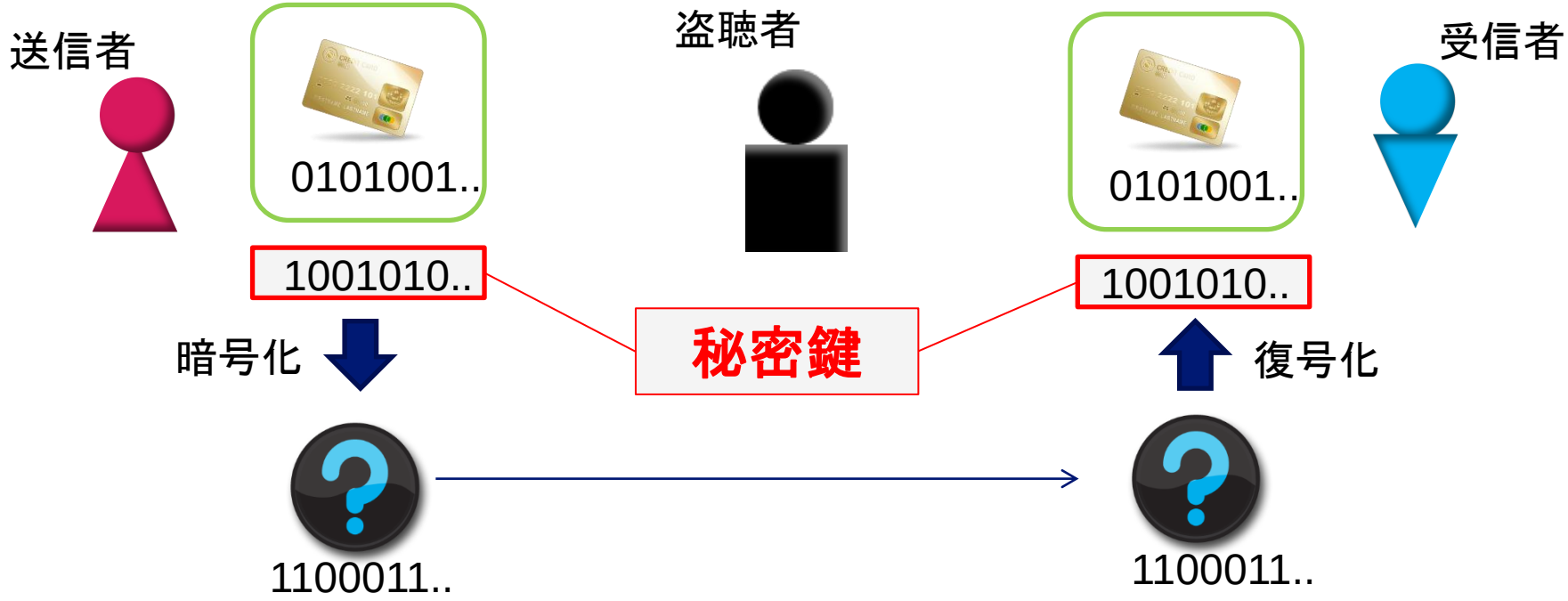
現代暗号が抱える課題の根本的な解決を目指すうえで量子暗号は価値がある

Copyright 2024 NTT CORPORATION

量子鍵配送（QKD）の位置づけ

One time pad＋QKD　→　情報論的に安全な暗号

One time pad：暗号化したいメッセージと同じ長さの秘密鍵を一度だけ使う方式

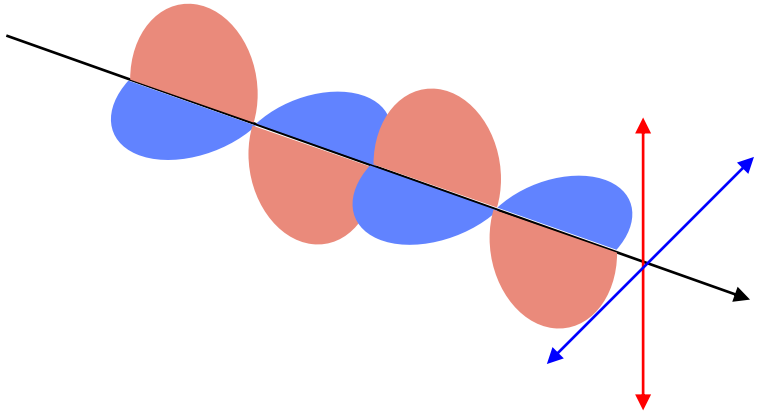


どうやって秘密鍵を共有するか？　→　方法の一つが量子鍵配送（QKD）

Copyright 2024 NTT CORPORATION

QKDにおける情報伝達媒体

- 基本的には光を使う
  - 光の偏光で0/1を表現する場合



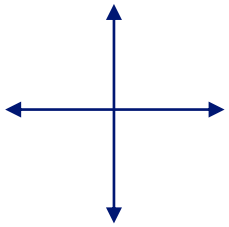
青（横偏光）:0
赤（縦偏光）:1

  - 光子の位置で0/1を表現する場合

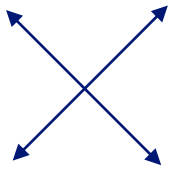
Copyright 2024 NTT CORPORATION

QKDの安全性の源：量子力学の不確定性原理

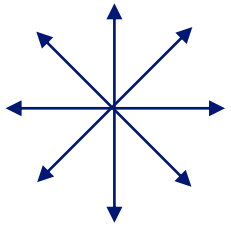
- ある物理量を確定（測定）させると、それと相補的な物理量が不確定になってしまう原理
- 光子の偏光の場合
  - 偏光の縦/横成分（ここではZ基底と呼ぶ）を測定して知ろうとすると、右斜め/左斜め成分（X基底と呼ぶ）を知ることができなくなる。逆も同様。



できること:
偏光の縦/横を確実に見分ける
（Z基底の測定）

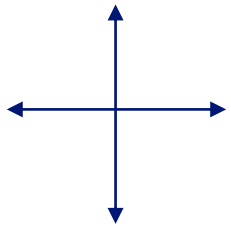


できること:
偏光の右斜/左斜を確実に見分ける
（X基底の測定）



できないこと:
どの偏光か確実に見分ける

に対してZ基底の測定を行うと



の結果が半々で得られる

Copyright 2024 NTT CORPORATION

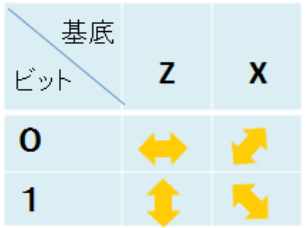
QKDの誕生：BB84プロトコル

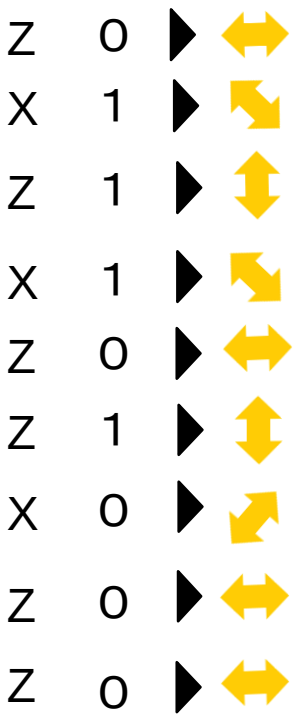
- 1984年にBennettとBrassardが提案した最初のQKDプロトコル
- 直接伝送型（二者間で状態準備&測定が行われる）であり、実装の複雑さが少ない
- 理論的にも扱いやすく、安全性が証明されている

Copyright 2024 NTT CORPORATION

BB84プロトコルの流れ（状態送信と測定）

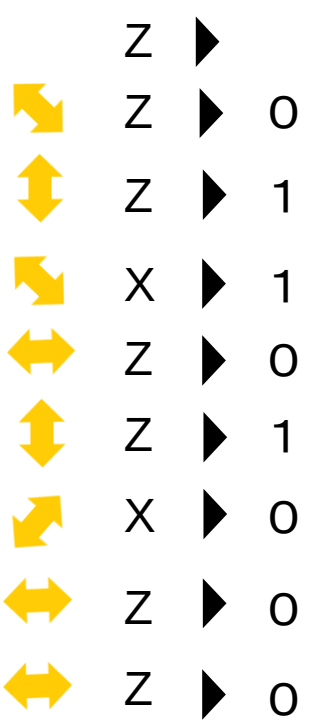
送信者は以下を繰り返す
1. 基底Z/Xを選択する
2. ビット0/1をランダムに選択する
3. 表の関係を使って、対応する偏光を送る

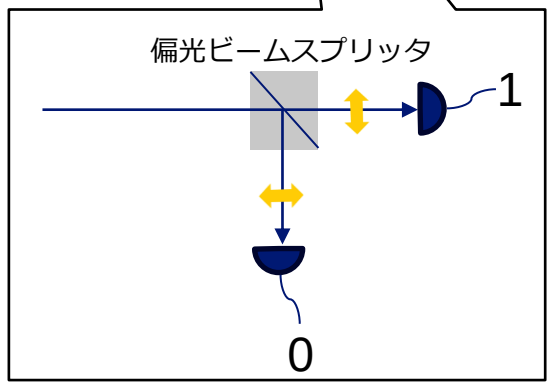




量子通信路
（光ファイバなど）

受信者は以下を繰り返す
1.基底Z/Xを選択する
2.やってきた光に対して、Zなら横/縦を識別する測定を行い、Xなら右斜め/左斜めを識別する測定を行う
3.測定結果から0または1を得る

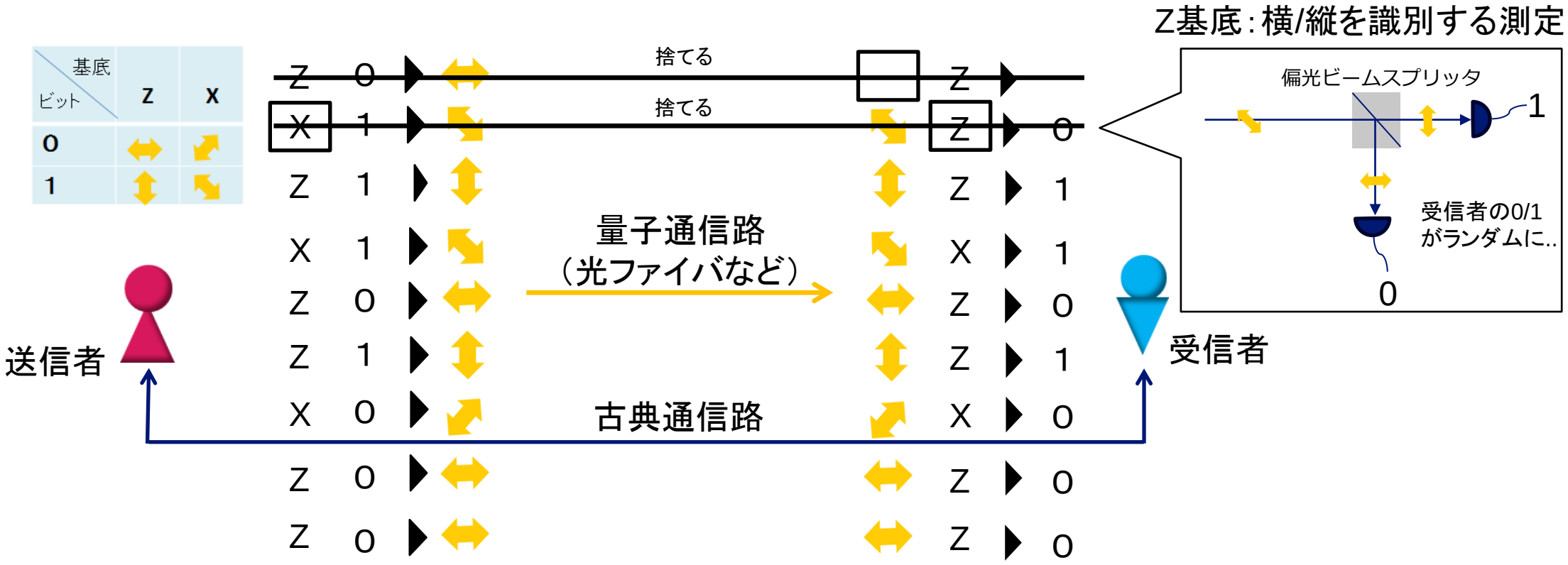




Copyright 2024 NTT CORPORATION

BB84プロトコルの流れ（損失と基底確認）

送信者と受信者は古典通信路（秘匿化されていなくて良い）を使って以下を行う
1. 受信者に光子が届かなかった場合はイベントを捨てる
2. 送信-受信者間で基底が一致していない場合はイベントを捨てる（siftingと呼ぶ）

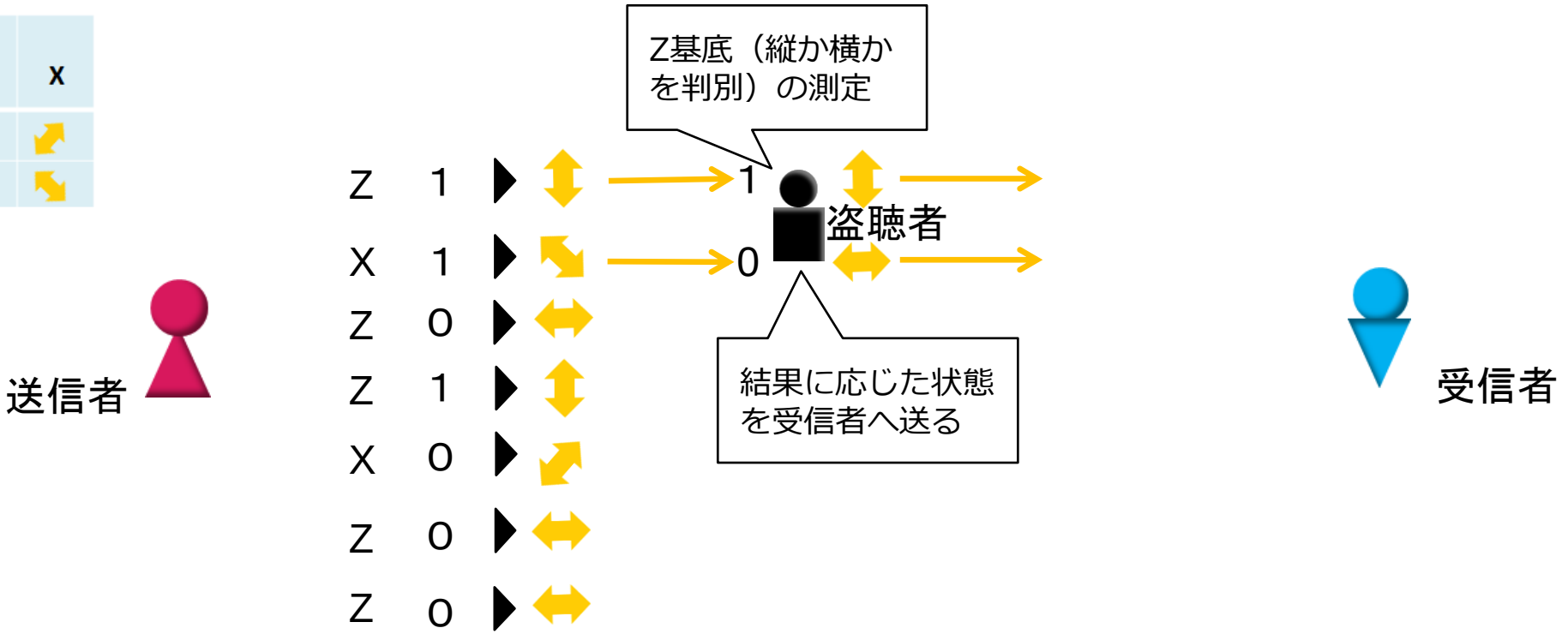


Copyright 2024 NTT CORPORATION

BB84プロトコル（攻撃例とその影響）

良く知られた遮断-再送信攻撃の例を考える
1. 盗聴者は送信者から送られてきた光子をZ基底で測定して0/1を得る
2. 使った基底と得られた0/1に応じて、表の関係から偏光状態を受信者に送る

ビット＼基底	Z	X
0	↔	⤢
1	↕	⤡

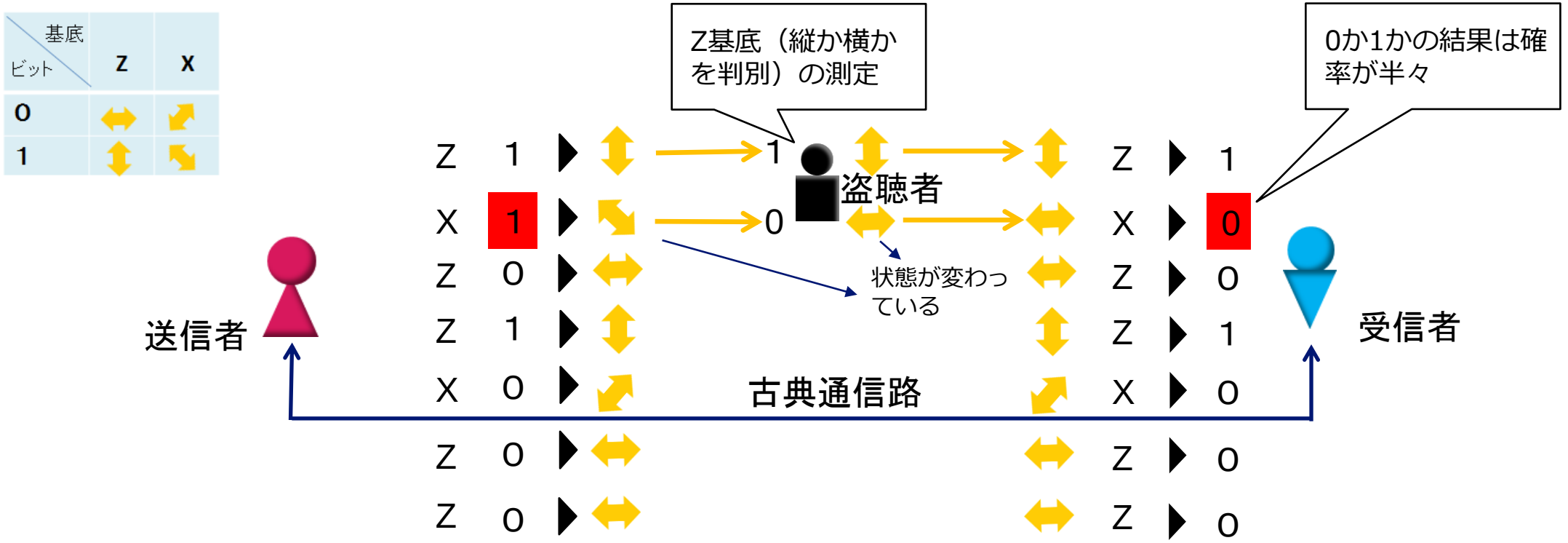


Copyright 2024 NTT CORPORATION

BB84プロトコル（攻撃例とその影響）

不確定性原理により、盗聴者は光子の偏光の任意の方向を測ることはできない。

送信者がX基底の時、盗聴者がZ基底で測定を行うと状態（偏光の向き）を変えてしまう。
変わってしまった状態（横偏光）にBobがX基底（斜め成分）の測定を行うと、結果0/1がランダムになる
→　半分の確率で送信者-受信者間にビットのエラーを発生させる（図の赤の部分）



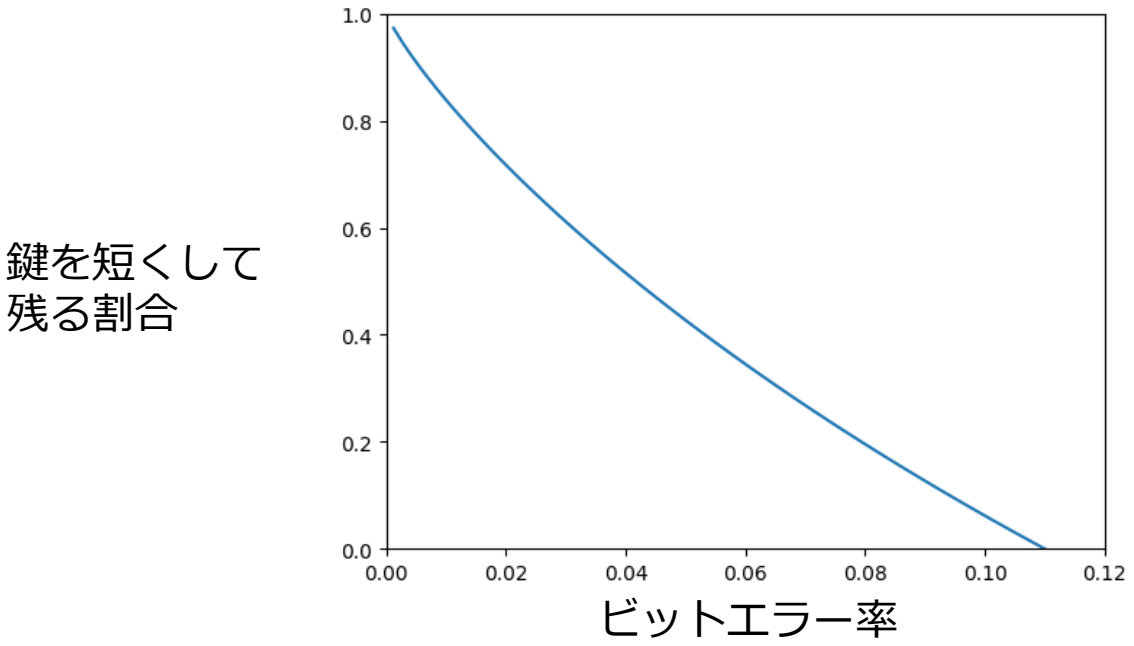
Copyright 2024 NTT CORPORATION

BB84プロトコルの流れ（ポストプロセス）

送信者と受信者は古典通信路を使って以下を行う

1. ビットを一部公開し合い、ビットエラー率を見積もる（公開したビットは捨てる）
2. 残ったビットについて、二者間でエラー訂正を行う
3. ビットエラー率に応じて、二者間で鍵を短くする（これを秘匿性増幅と呼ぶ）

どれだけ鍵を短くすれば安全な秘密鍵になるかは、BB84では理論的に証明されている（以下のグラフ）



※グラフは、ZとXでエラー率が等しく、エラー訂正が理想的な効率でできる場合

Copyright 2024 NTT CORPORATION

第二部：長距離QKD

QKD実装における課題：長距離化

- QKDの課題の一つとして、長距離化がある
- ある距離Lに対して、送信された微弱光が受信側に到達する割合を透過率$\eta(L)$と定義すると、$\eta(L) = 10^{-\alpha L}$のように指数関数的に減少する（※1）
- 理論的な提案により、以下のように長距離化を可能にしてきた（※2）
  1. おおよそ150km以下
  2. おおよそ300km以下
  3. おおよそ600km以下

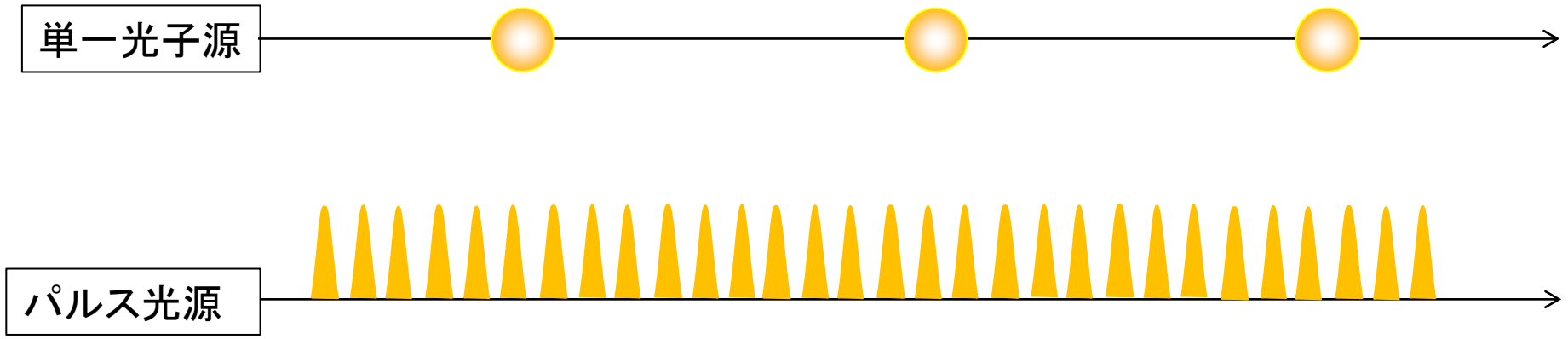
※1: 光ファイバであれば、$\alpha = 0.02$ 程度

※2：距離はあくまで発表者のシミュレーションによる参考値。どのような装置や環境で行うかによって変わる。

Copyright 2024 NTT CORPORATION

QKD実装の実際（送信側）

- BB84提案時は送信側では単一光子を準備できるものと仮定されていた
- しかし、実装容易性や繰り返しスピード等の観点から、微弱なレーザーパルスが実装に用いられることが多い。

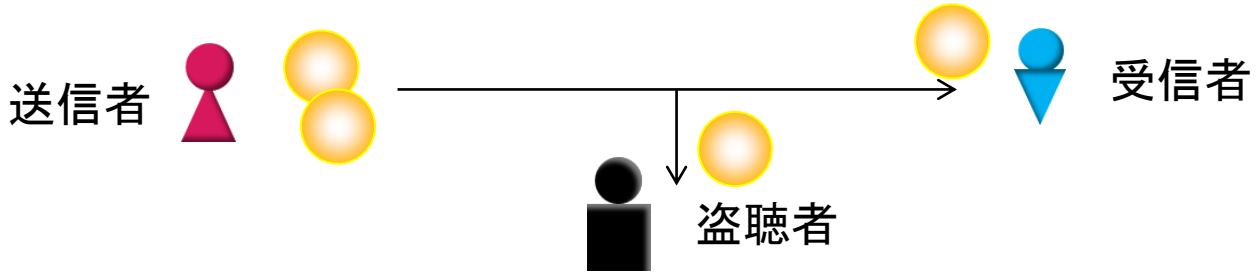


Copyright 2024 NTT CORPORATION

微弱光QKDにおける脅威：光子分離攻撃

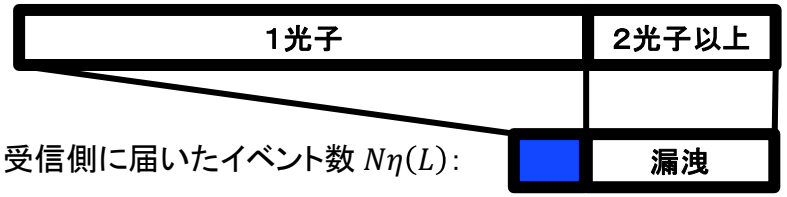
- 微弱光には、1光子成分だけでなく2光子以上の成分も含まれている（※）
- 2光子以上の成分のうち1光子を抜き取り、その他は受信者に検出させる攻撃を光子分離攻撃という

→BB84においては、盗聴者が受信者と全く同じ情報を得られてしまう強力な攻撃



- この光子分離攻撃を想定すると、2光子以上の成分は全て盗聴者に漏洩していると考えざるを得なかった

送信側で1光子以上を出すイベント数 N:



受信側に届いたイベント数 $N\eta(L)$:

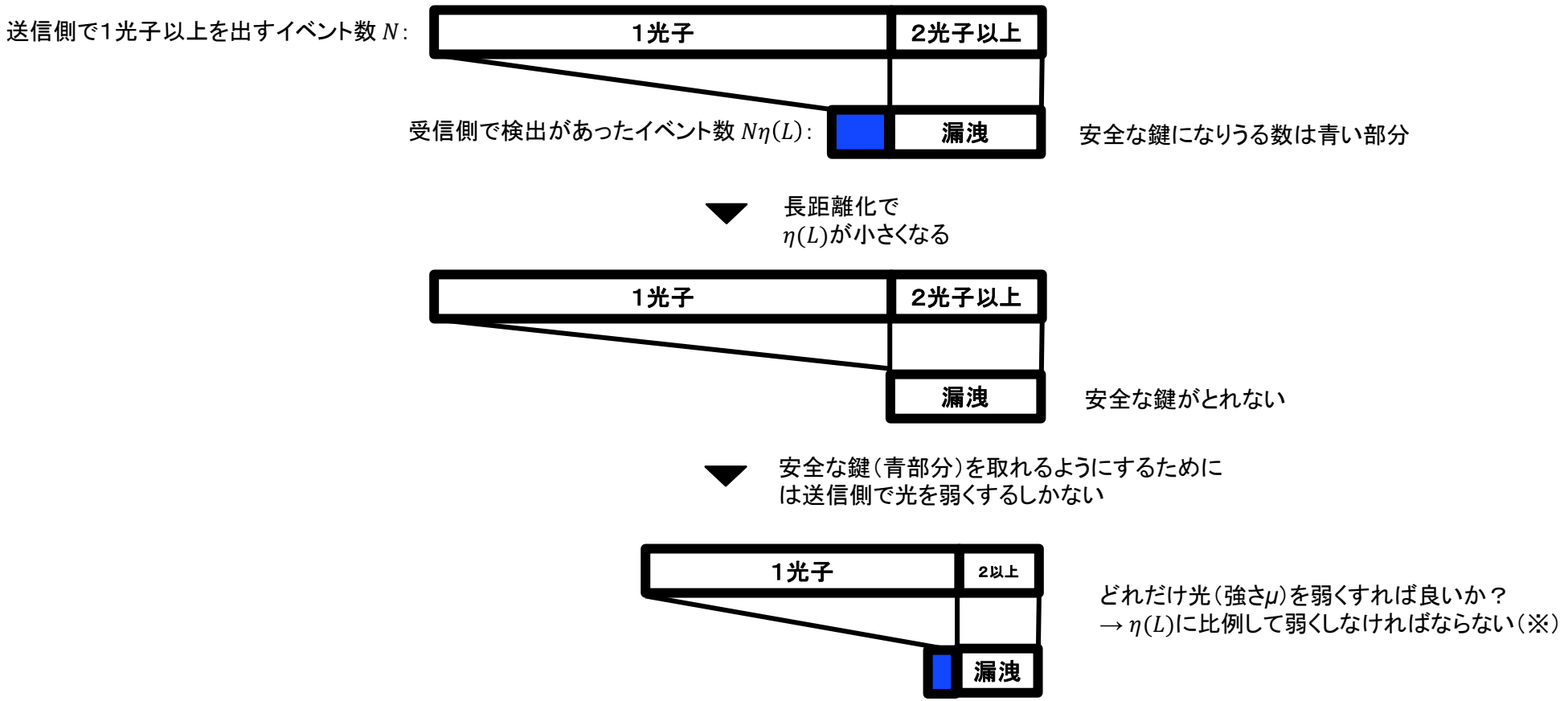
安全な鍵になりうる数は青い部分しかない。。

Copyright 2024 NTT CORPORATION

※μを強度、nを光子数として、一般にはn光子の割合はポアソン分布$e^{-\mu}\frac{\mu^n}{n!}$に従う

微弱光QKDにおける脅威：光子分離攻撃

光子分離攻撃により、距離が伸びると（$\eta(L)$が小さくなると）安全な鍵がすぐとれなくなってしまう
距離Lが伸びても安全な鍵がとれるようにするには、**光強度を$\eta(L)$に比例して弱める必要がある（※）**

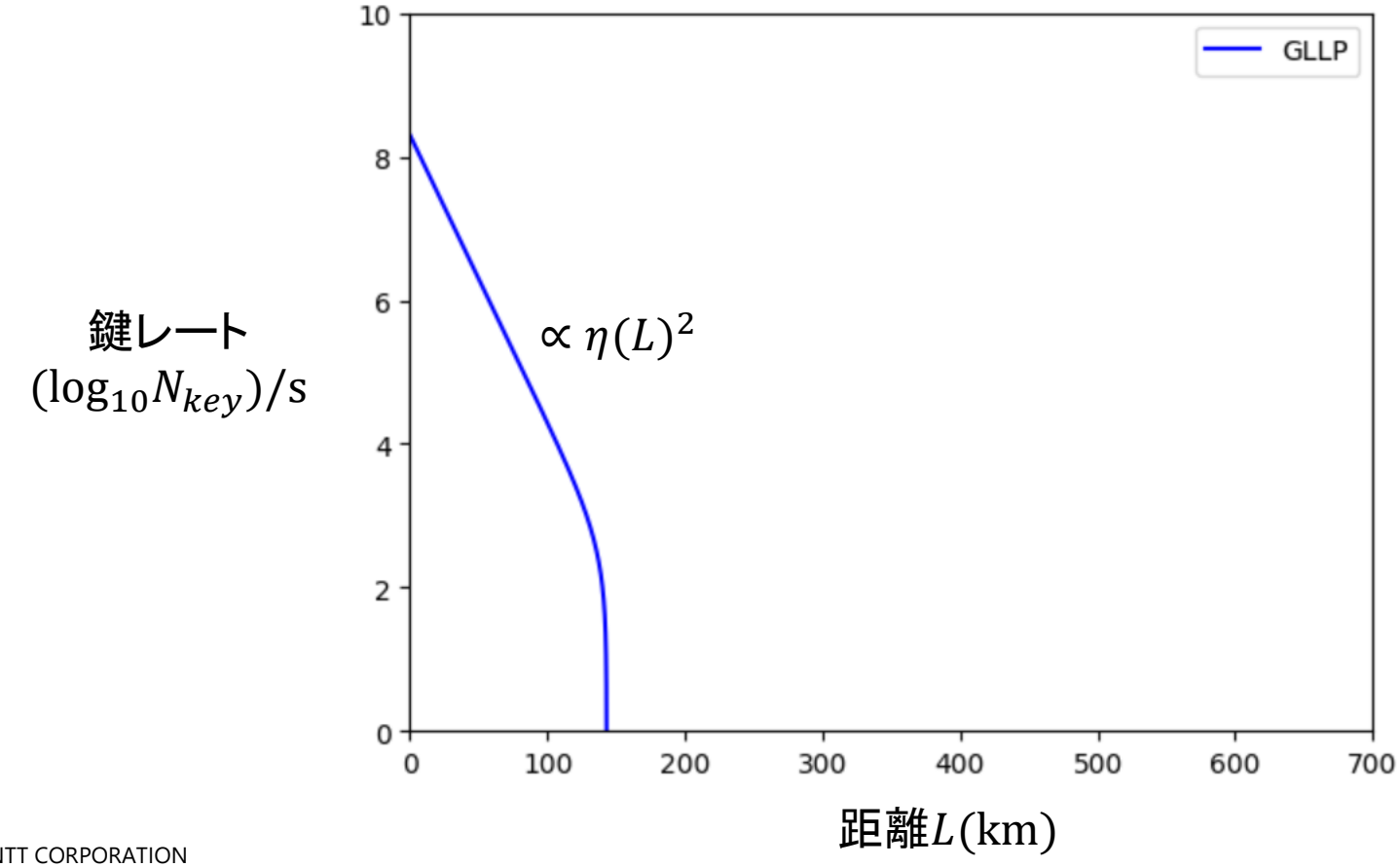


（※）安全な鍵がとれる条件は$\eta(L)(\mu + O(\mu^2)) > \frac{\mu^2}{2} + O(\mu^3)$のため

Copyright 2024 NTT CORPORATION

微弱光を用いたBB84の鍵レート

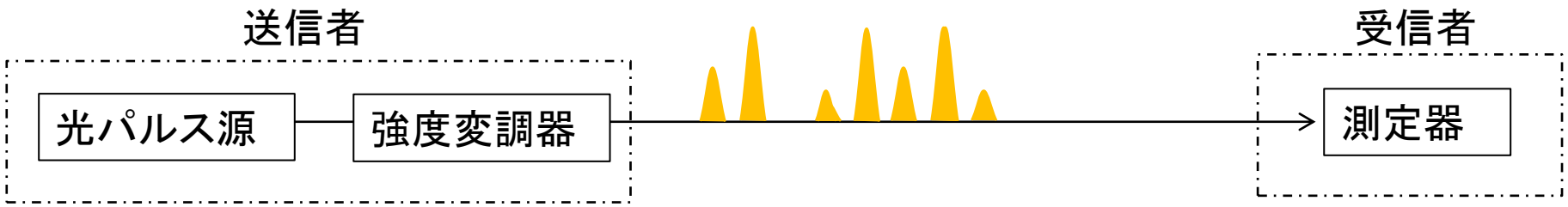
- そもそも光子が受信者に到達する割合が$\eta(L)$。加えて送信者が光強度を$\eta(L)$に比例して下げる。
- よって秘密鍵のレートは$\eta(L)^2$に比例する



Copyright 2024 NTT CORPORATION

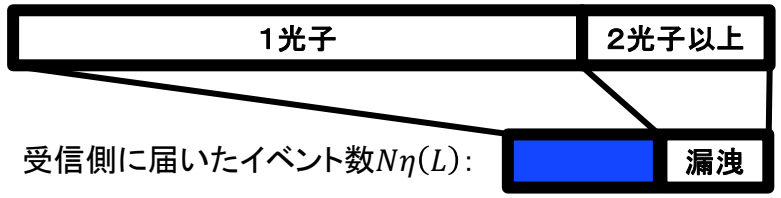
Decoy法

- 送信者が出す光パルスの強度を複数種類で変化させる



- 実効的に（n光子成分が届く確率を変数とした）連立方程式を増やしているのと同じ効果がある（詳細は参考）
- 受信側で検出するイベントのうち、1光子由来の数、2光子以上由来の数がより正確に見積もれるようになる

送信側で1光子以上を出すイベント数N:

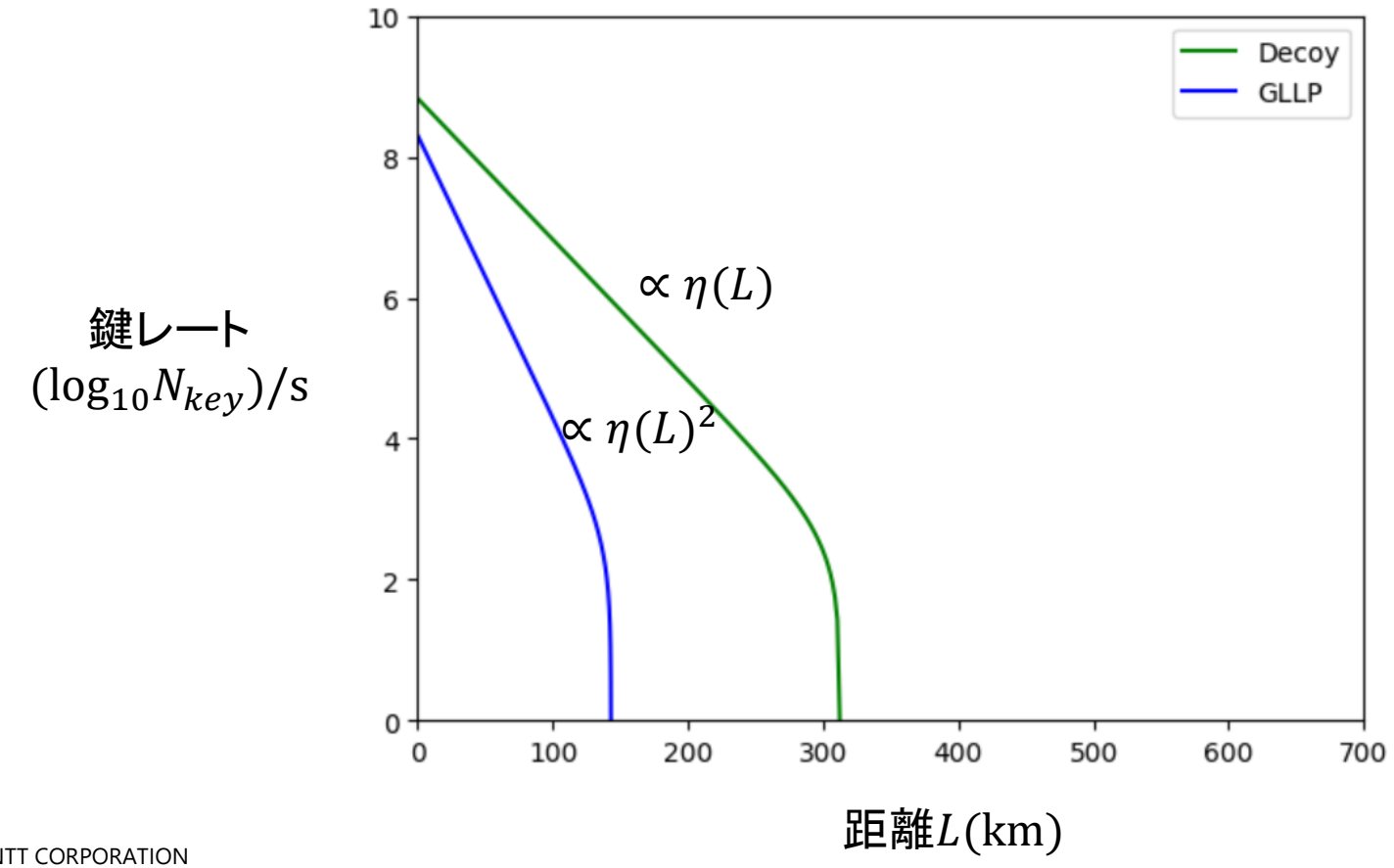


安全な鍵になりうる数（青部分）が増える！

Copyright 2024 NTT CORPORATION

Decoy法を用いたBB84の鍵レート

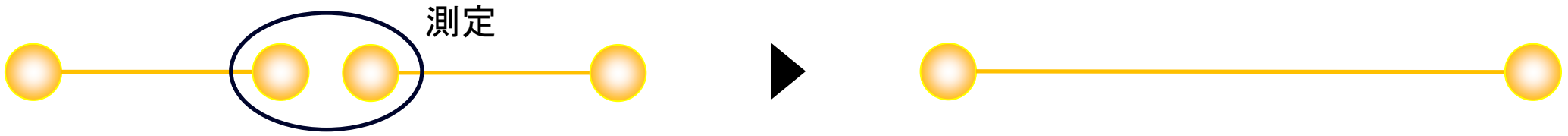
- 結果として、距離Lを伸ばしても、2光子成分を減らすために光強度を弱める必要がなくなる
- 秘密鍵レートは透過率$\eta(L)$に比例するようになり、鍵が取れる距離もおおよそ2倍になる



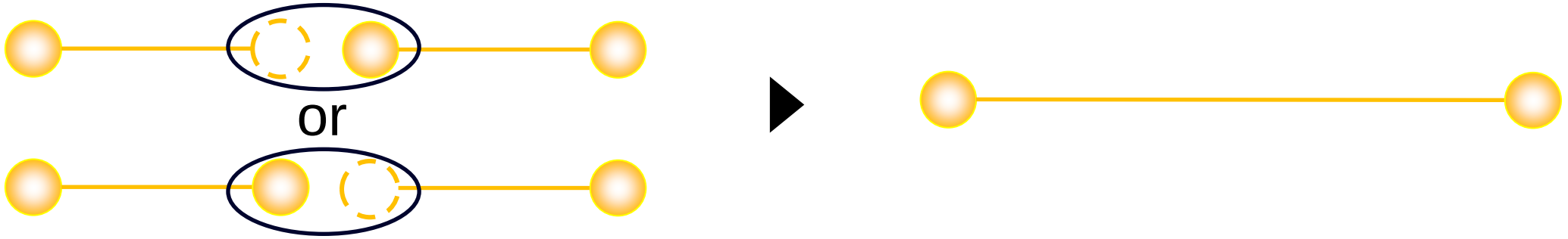
Copyright 2024 NTT CORPORATION

量子通信の長距離化：量子中継

- 量子中継のイメージ（黄色線は量子もつれを表す）



- 量子力学の性質から、片側が失われる確率が高くても、どちらが失われたのか判別できない測定をすれば、中継が成功することが知られていた（※）



- これにより通信可能な距離が実効的に2倍に（透過率依存性が$\eta(L) \to \sqrt{\eta(L)}$ に）

（※）例としてDuan *et al.*, Nature (2001)など

Copyright 2024 NTT CORPORATION

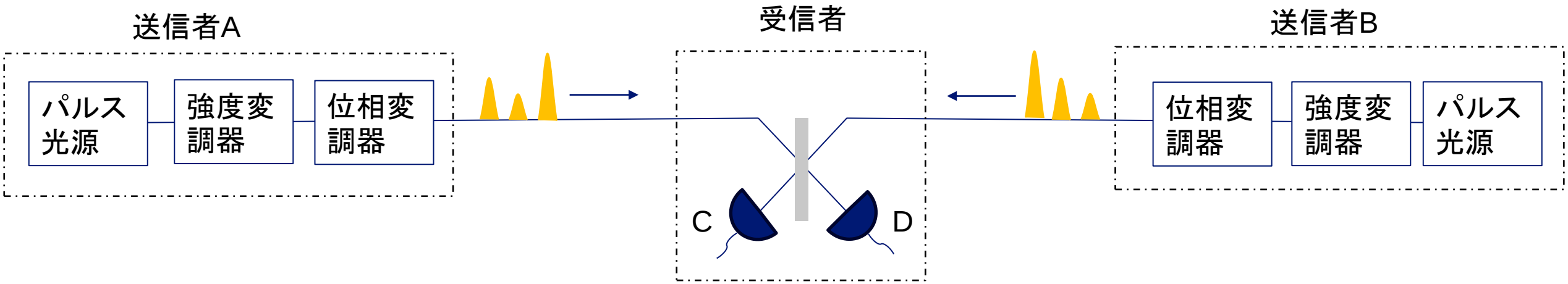
Twin-Field QKD(※)

- 送信者Aと送信者Bの間で鍵共有を行う
- 受信者は信頼できなくても構わない

送信者(二者)は以下を繰り返す

1. 基底Z/Xを選択する
2. 基底Zならビット0/1をランダムに選択する
3. 表の関係を使って、対応する状態を送る
4. 受信者からC/Dどちらで検出されたか聞く
   (両方鳴るor両方鳴らない場合は捨てる)
5. Cの場合はそのまま、Dの場合は一者がビットを反転させる
6. 後はBB84と同じ(sifting…)

	Z	X
0	パルス $\|\alpha>$	$\|\alpha>$の位相ランダム化 + Decoy(強度変調)
1	逆位相パルス $\|-\alpha>$	

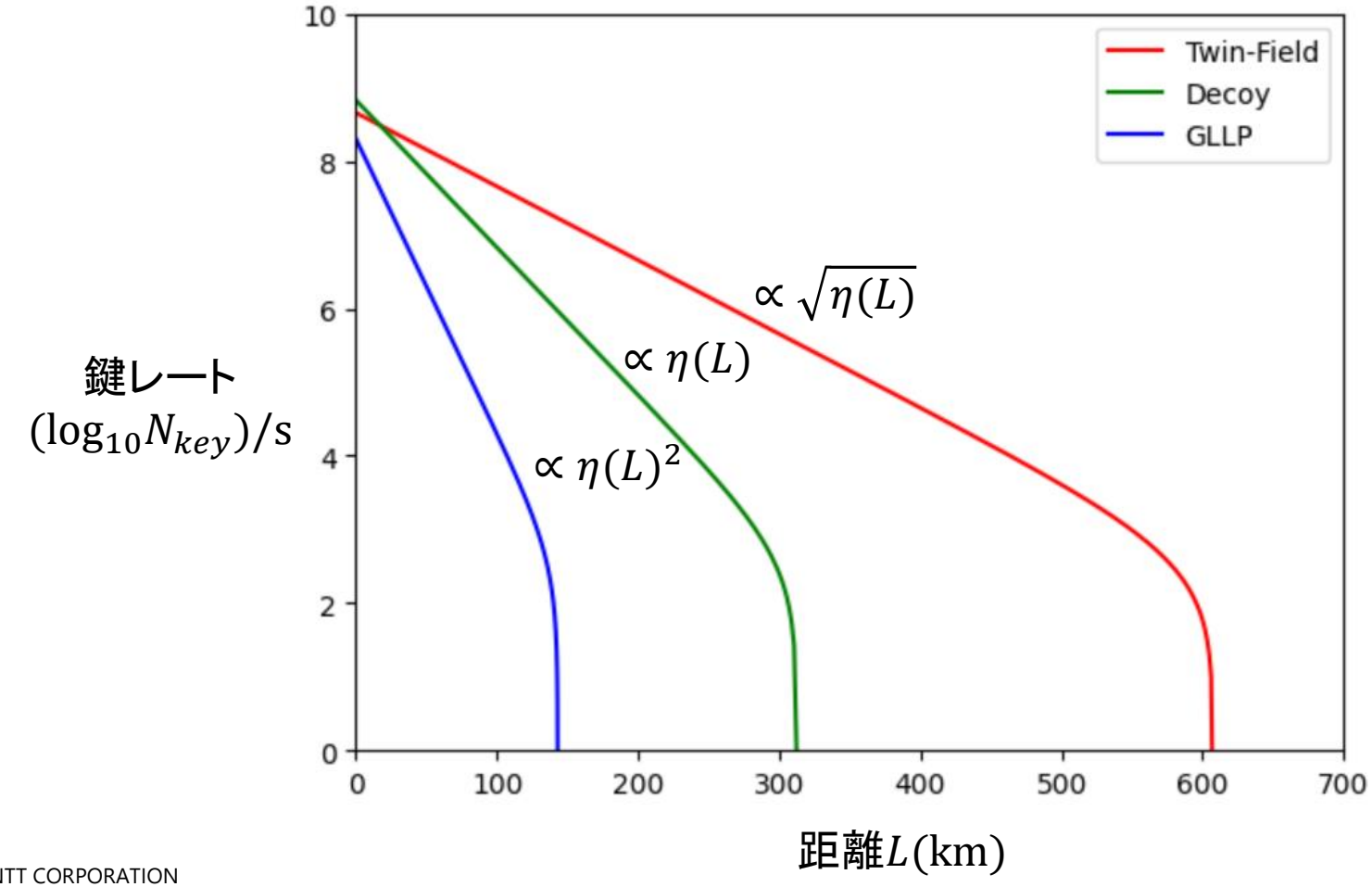


(※)ここではCurtyらによって提案されたプロトコルを扱う

Copyright 2024 NTT CORPORATION

Twin-Field QKDの鍵レート

- 結果として、秘密鍵レートは透過率$\eta(L) \to \sqrt{\eta(L)}$に比例するようになり、鍵が取れる距離もおおよそ2倍になる



Copyright 2024 NTT CORPORATION

今後の展望

- 長距離化についての論点
  - 信頼できるノード / 量子中継
    - 課題：量子中継は基本的には量子メモリが必要
- 長距離化以外でも実装していくうえでの論点はある。例えば
  - One time padを用いるのか
  - 認証はどうするか
- 量子暗号の普及について
  - 量子暗号は、量子コンピュータなどと比べて、どの程度の性能があれば誰が使ってくれるか、が難しい
  - 上記のような論点も意識しつつ、産官学の連携が非常に重要になる認識

Copyright 2024 NTT CORPORATION

まとめ

- 実装が容易な直接伝送型のQKDプロトコル（特にBB84）を紹介した
- QKDの課題である長距離化に対する進展を理論的側面から紹介した

Copyright 2024 NTT CORPORATION

（参考）Decoy法の直感的理解

- 送信側が出す光パルスの強度を複数種類で変化させる → 連立方程式の数を増やしているのと同じ
- 送信側の強度を4種類(a, b, c, d)とすると以下が成り立つ

$$
\begin{aligned}
q_a &= p_a^{(0)} x^{(0)} + p_a^{(1)} x^{(1)} + p_a^{(2)} x^{(2)} + \cdots \\
q_b &= p_b^{(0)} x^{(0)} + p_b^{(1)} x^{(1)} + p_b^{(2)} x^{(2)} + \cdots \\
q_c &= p_c^{(0)} x^{(0)} + p_c^{(1)} x^{(1)} + p_c^{(2)} x^{(2)} + \cdots \\
q_d &= p_d^{(0)} x^{(0)} + p_d^{(1)} x^{(1)} + p_d^{(2)} x^{(2)} + \cdots
\end{aligned}
$$

q_w: 受信者に届いたシグナルのうち、送信者が強度wに設定していた割合
$p_w^{(n)}$: 送信者が強度wに設定したときのn光子成分の割合
$x^{(n)}$: 送信者のn光子成分が受信者でシグナルとして検出される確率

- このうち、q_wは通信後に測定可能、$p_w^{(n)}$は光源の性質として既知
- 変数は$x^{(n)}$のみ。特に$x^{(1)}$（1光子成分がどれだけ届くか）を知りたい。→連立方程式により下限を知ることができる

Copyright 2024 NTT CORPORATION

（参考）シミュレーションに用いたパラメータ

パルス繰り返しレート：10GHz

減衰係数（$\eta(L) = 10^{-\alpha L}$のα）：0.02

検出器の検出効率：30%

検出器の暗検出率：100Hz

エラーレート：3% + 暗検出由来のエラー

エラー訂正の効率係数：1.1（1が最良）

Copyright 2024 NTT CORPORATION