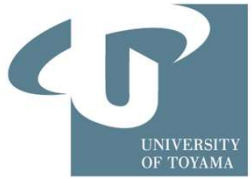
量子暗号通信へのサイドチャネル攻撃

玉木　潔

富山大学　学術研究部工学系



玉木の自己紹介

- ✓ 大学では物理を勉強しました
- ✓ 大学院修士課程入学試験の前に量子暗号と偶然出会い、そのまま量子暗号の世界へ
  （量子暗号が本当に安全かな？やどうやったら安全になるかな？
  などを考える理論の研究をしています）
- ✓ 総合研究大学院大学の博士課程を卒業し、ポスドクをペリメータ理論物理学研究所やトロント大学でやった後、NTT物性科学基礎研究所に2006年に入所
- ✓ 2017年から富山大学で働いています

話の流れ

1. 導入 ― ワンタイムパッドと微視的な世界の不思議な性質（量子力学）
2. 量子暗号の仕組みと安全性の意味
3. 国内外の開発状況
4. 安全性の意味 ―『理想的な量子暗号の安全性』と『実際の装置での安全性』
5. 実際の装置を使った量子暗号を安全にする研究

暗号って何？

一言でいうと、情報を隠すためのテクニック

通信における暗号の例

送信者（アリス）

クレジットカード情報
XXXX-XXXX-XXXX-XXXX

エ夫せずに送ると。。。

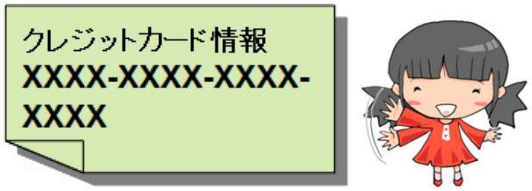
盗聴者
（イブ）

正規受信者（ボブ）

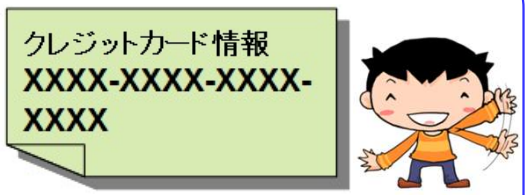
クレジットカード情報
XXXX-XXXX-XXXX-XXXX

通信における暗号の例

送信者（アリス）

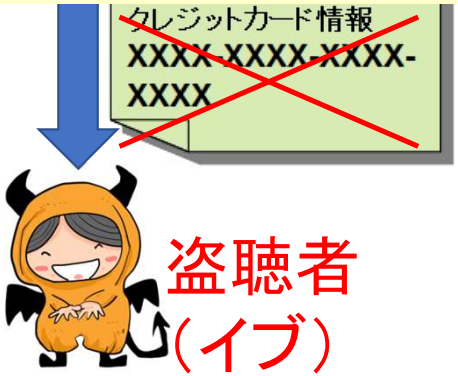


正規受信者（ボブ）



送受信者の目標

正規受信者にはクレジットカードの番号を伝えたいけれど、盗聴者には隠したい



盗聴者
（イブ）

通信における暗号の例

送信者（アリス）

クレジットカード情報
XXXX-XXXX-XXXX-XXXX

現代暗号

暗号文を解読するためにはイブが数学の問題を解かなければならない

!2R#>*0
@a#FWJ
=?/1”2/…

盗聴者（イブ）

正規受信者（ボブ）

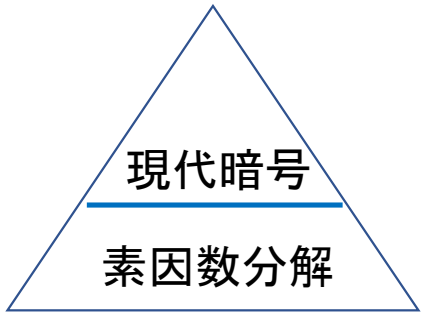
クレジットカード情報
XXXX-XXXX-XXXX-XXXX

盗聴するために解くべき問題の例：素因数分解

252097800623×2038074743＝ 513794160215585964889

66615592657 × 11430838429 ＝ 761472076514245815853

数学の問題（素因数分解）の難しさが安全性の礎



素因数分解に関してのビッグニュース

1994年にピーター・ショアが量子計算機を使えば素因数分解は短時間で解けることを発見した！

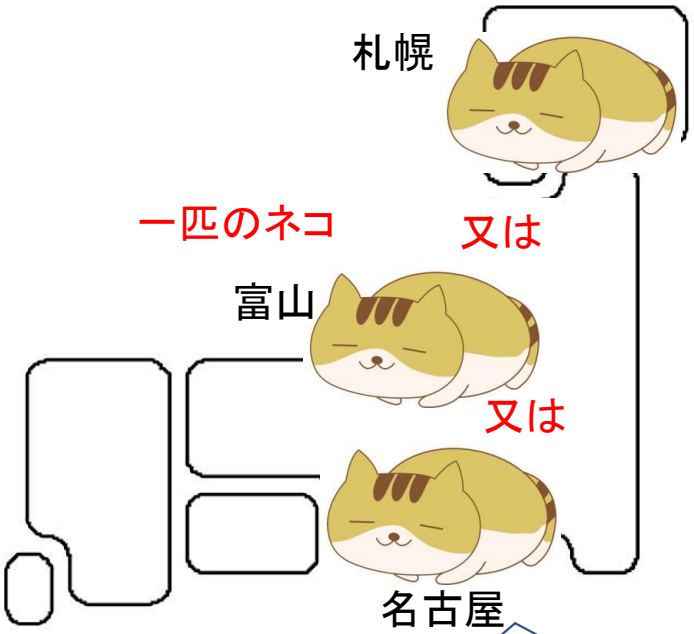
量子計算機

量子力学の原理を利用している計算機

量子力学って何？

⇒ 電子、分子、光子（光の粒）など主に微小な物の性質を表現する分野

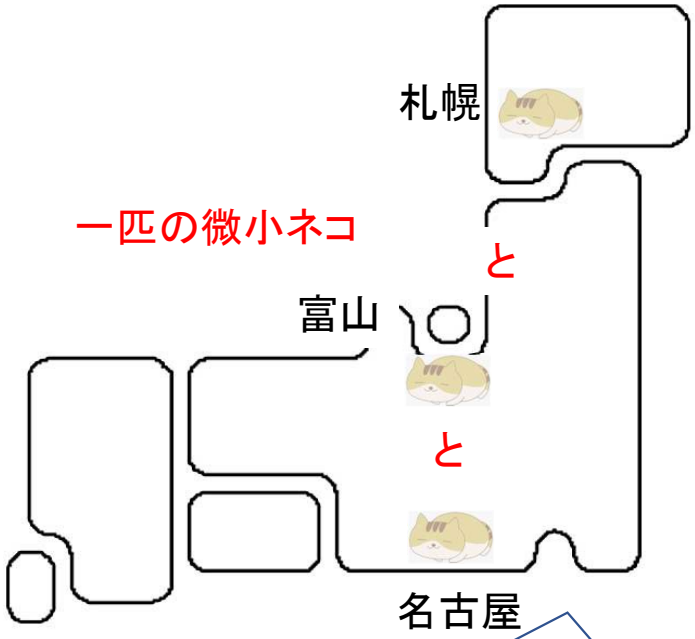
私達の常識



私は札幌か富山か名古屋にいます

微小な物の世界

イメージ図



私は札幌と富山と名古屋に同時にいます

微小な物は同時に複数個所に存在できる！

素因数分解は量子コンピューターに解かれてしまう！

⇒ じゃあ、素因数分解以外の問題を使えば良いのでは？

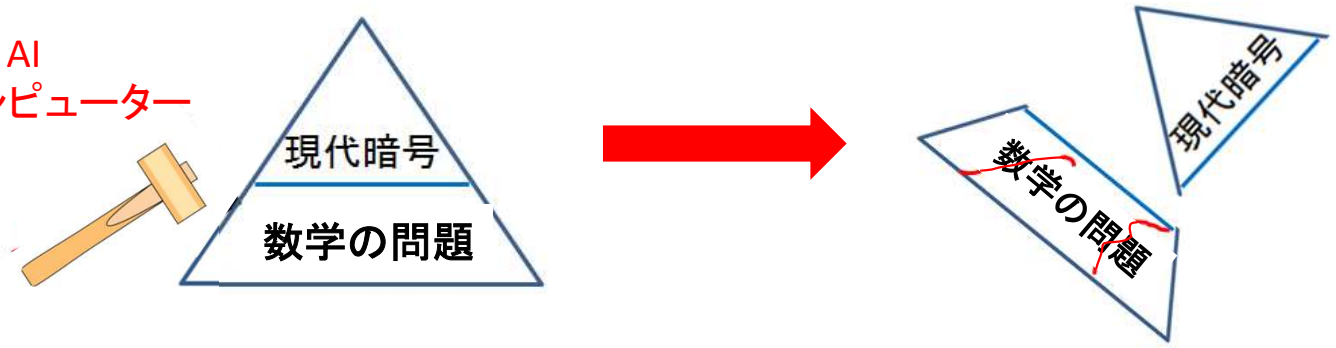
しかし！そもそも

数学の問題

✓ 賢い人やAIが解くことができない、という保証はどこにもない！

⇒ 量子コンピューターなど速い計算機ができなくても解けるかも?！

賢い人、AI
量子コンピューター



数学の問題が安全性の根拠である暗号には、賢い人、AI、高性能なコンピューターなどによって盗聴される恐れが常にある

素因数分解は量子コンピューターに解かれてしまう！

⇒　じゃあ、素因数分解以外の問題を使えば良いのでは？

しかし！そもそも

数学の問題

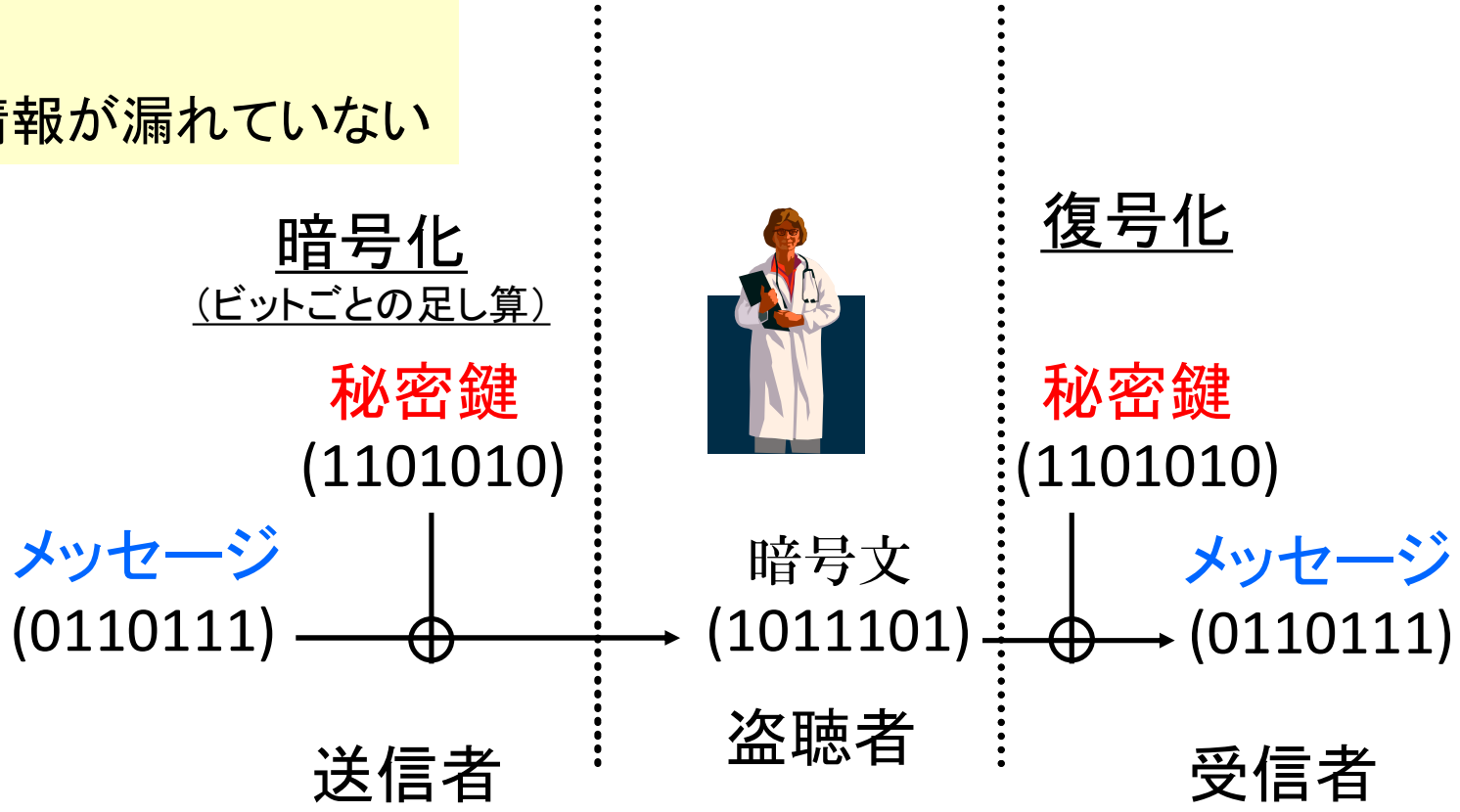
✓　賢い人やAIが解くことができない、という保証はどこにもない！

⇒　量子コンピューターなど速い計算機ができなくても解けるかも?！

安全な通信はあきらめるしかないのかな？？
⇒　ワンタイムパッドがある

秘密鍵は以下を満たすビット列
(1) 同一
(2) ランダム
(3) 盗聴者に情報が漏れていない

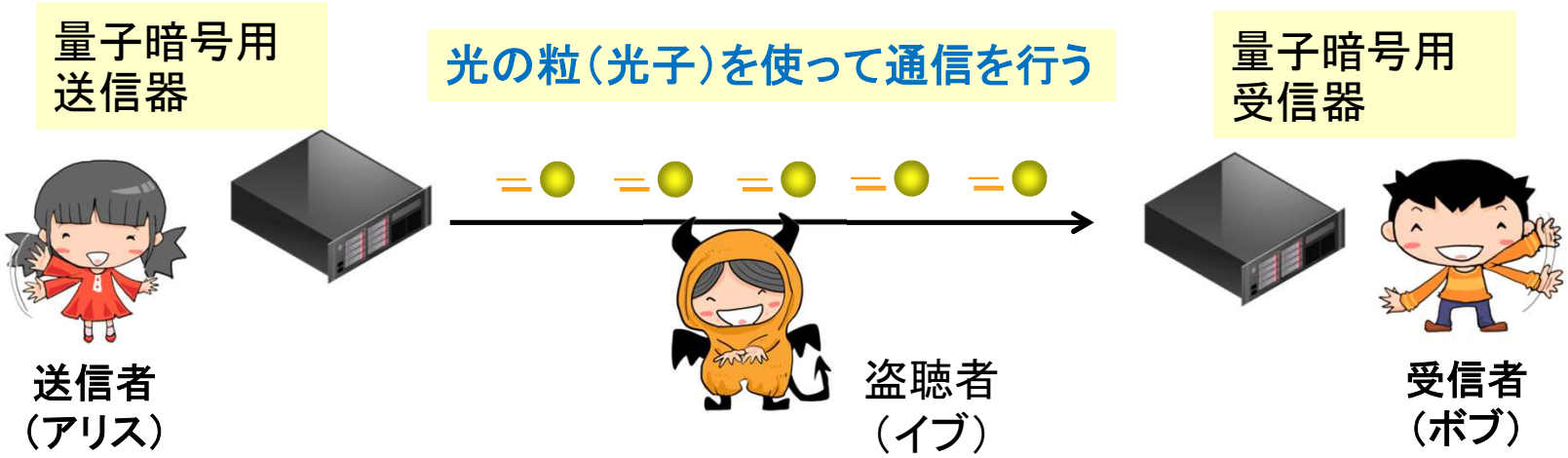
ワンタイムパッド



秘密鍵を知らない盗聴者は暗号文を解読できないので安全

➢ **秘密鍵をどのように配布するか？⇒量子暗号（量子鍵配送）**

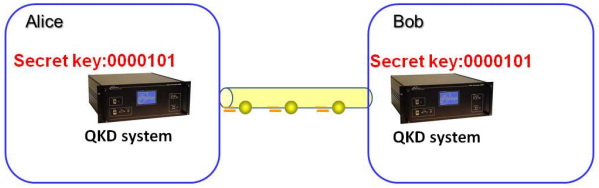
量子暗号
～光子の性質（自然法則）が盗聴を防ぐ！～



- ✓ 量子暗号は秘密鍵を配布するための方法
  - ー　直接メッセージを送っているわけではない
- ✓ 専用装置が必要（量子暗号方式ごとに装置が異なるのが一般的）
- ✓ 原理的に許されるあらゆることが可能な強力な盗聴者に対しても量子暗号は安全！

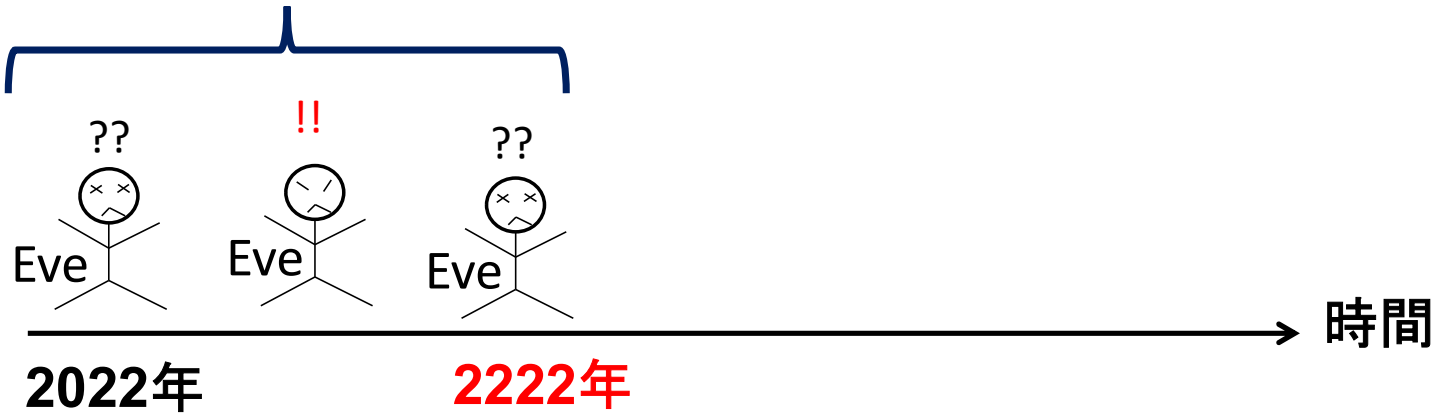
量子暗号の安全性の意味

情報漏れ（理想的な秘密鍵で起きなかった事象）をどのくらいの頻度で許すのかをユーザーが自由に選べる（安全性パラメータε）



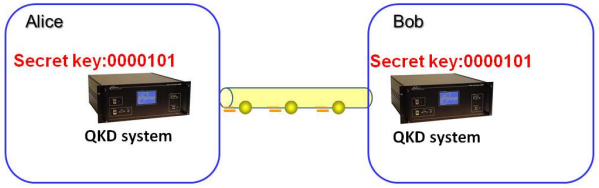
$\varepsilon=10^{-8}$

Eveがどのような技術をもっていようが200年に平均一度しか情報漏れが起きない(10分に鍵が1セットできると仮定)



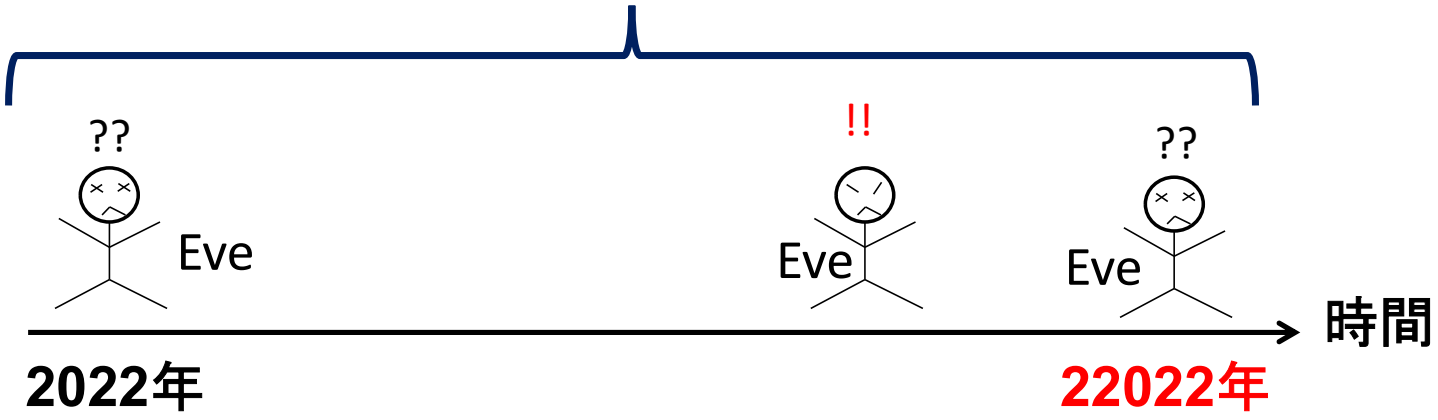
量子暗号の安全性の意味

情報漏れ（理想的な秘密鍵で起きなかった事象）をどのくらいの頻度で許すのかをユーザーが自由に選べる（安全性パラメータε）



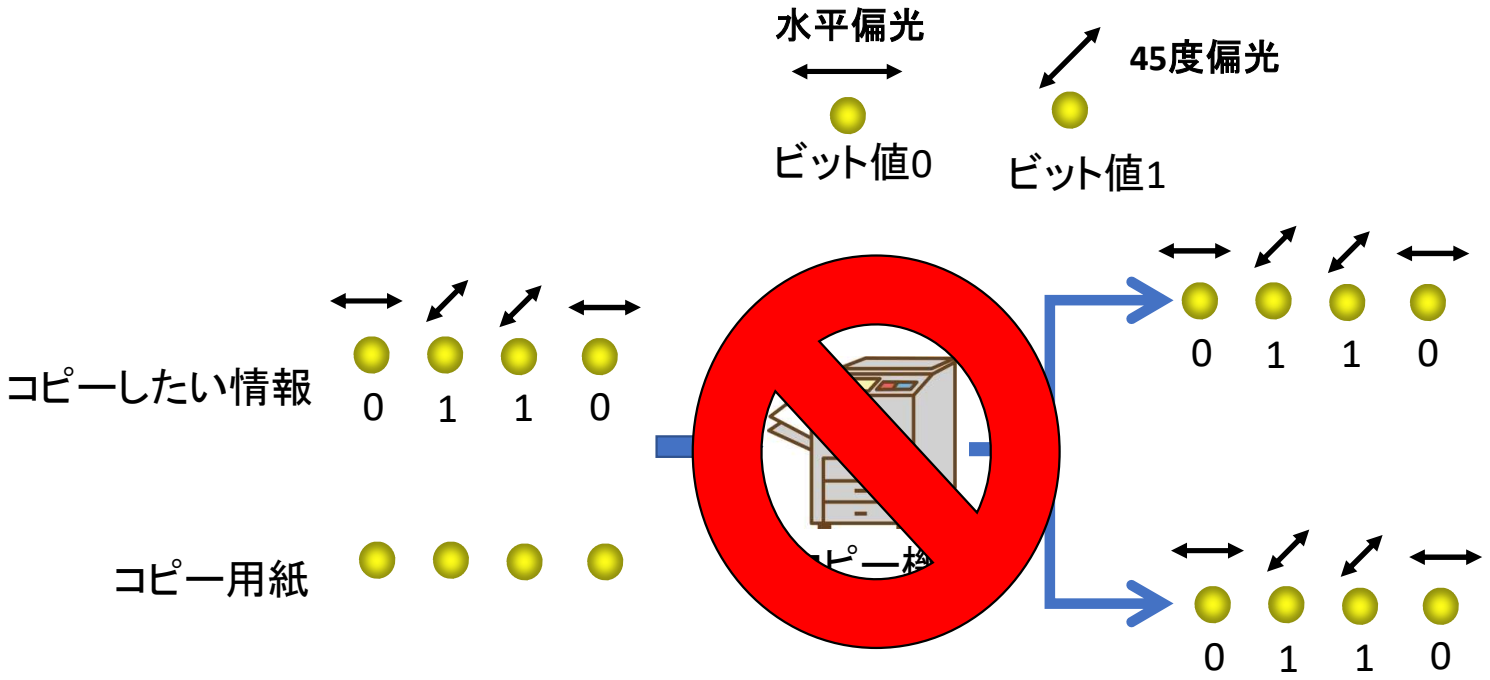
$\varepsilon=10^{-10}$

Eveがどのような技術をもっていようが2万年に平均一度しか情報漏れが起きない(10分に鍵が1セットできると仮定)



量子力学の奇妙な性質の例

✓　光は光子と呼ばれる粒の集まり（1粒、2粒、、と数えられる）

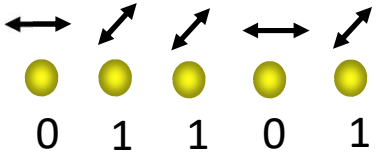


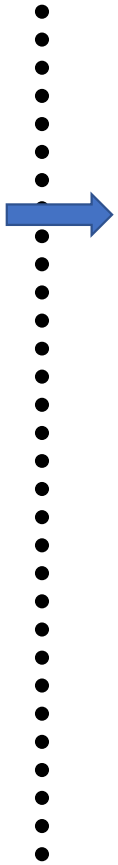
光子に書かれた情報はコピーできない

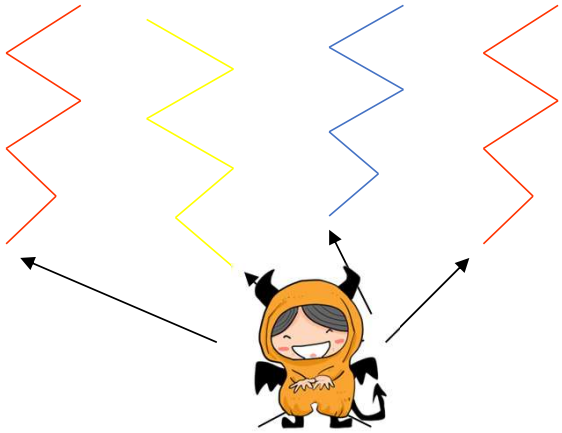
量子力学の奇妙な性質の例

送信者（アリス）

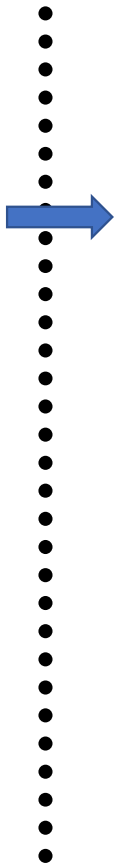
送信情報







盗聴者



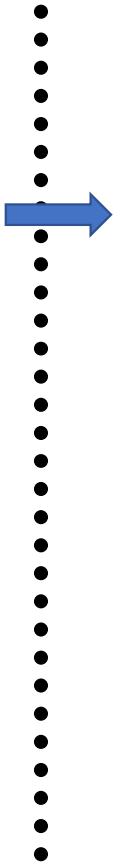
受信者（ボブ）

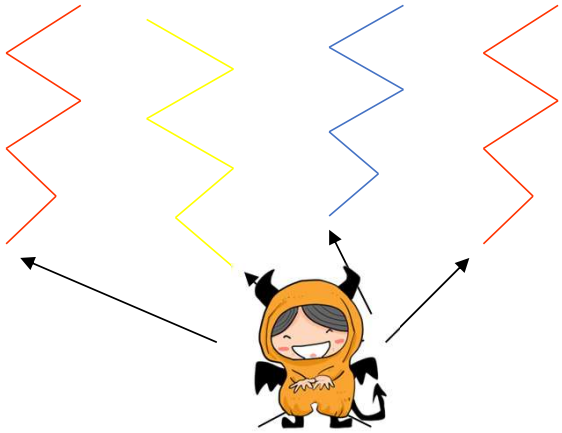
量子力学の奇妙な性質の例

送信者（アリス）

送信情報

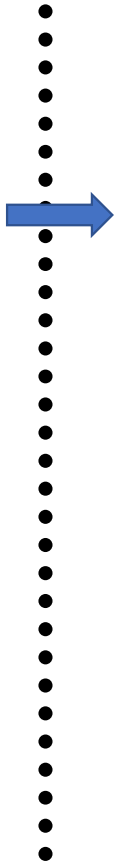
0 1 1 0 1





盗聴者

0 1 1 0 1



受信者（ボブ）

0 1 1 0 1

量子力学の奇妙な性質の例

送信者（アリス）

送信情報

0 1 1 0 1

光子のコピーはできない

受信者（ボブ）

0 1 1 0 1

0 1 1 0 1

量子力学の奇妙な性質の例

送信者（アリス）

送信情報

0 1 1 0 1

光子のコピーはできない

受信者（ボブ）

0 1 1 0 1

盗聴すると送信情報の一部を得れるが。。。

0 1 1 0 1

量子力学の奇妙な性質の例

送信者（アリス）

送信情報

0 1 1 0 1

受信者（ボブ）

? 1 1 0 ?

光子の状態が乱される！

盗聴者（イブ）

? 1 1 ? ?

量子力学の奇妙な性質の例

送信者（アリス）

送信情報

0 1 1 0 1

受信者（ボブ）

? 1 1 0 ?

盗聴者は送信情報の一部を得る代償として、送信された光子の状態を乱してしまう！

光子の状態が乱される！

盗聴者（イブ）

? 1 1 ? ?

量子暗号でのデータ処理

量子暗号送信器

乱数の情報が載った光子を多数送信

量子暗号受信器

送信者（アリス）

盗聴者（イブ）

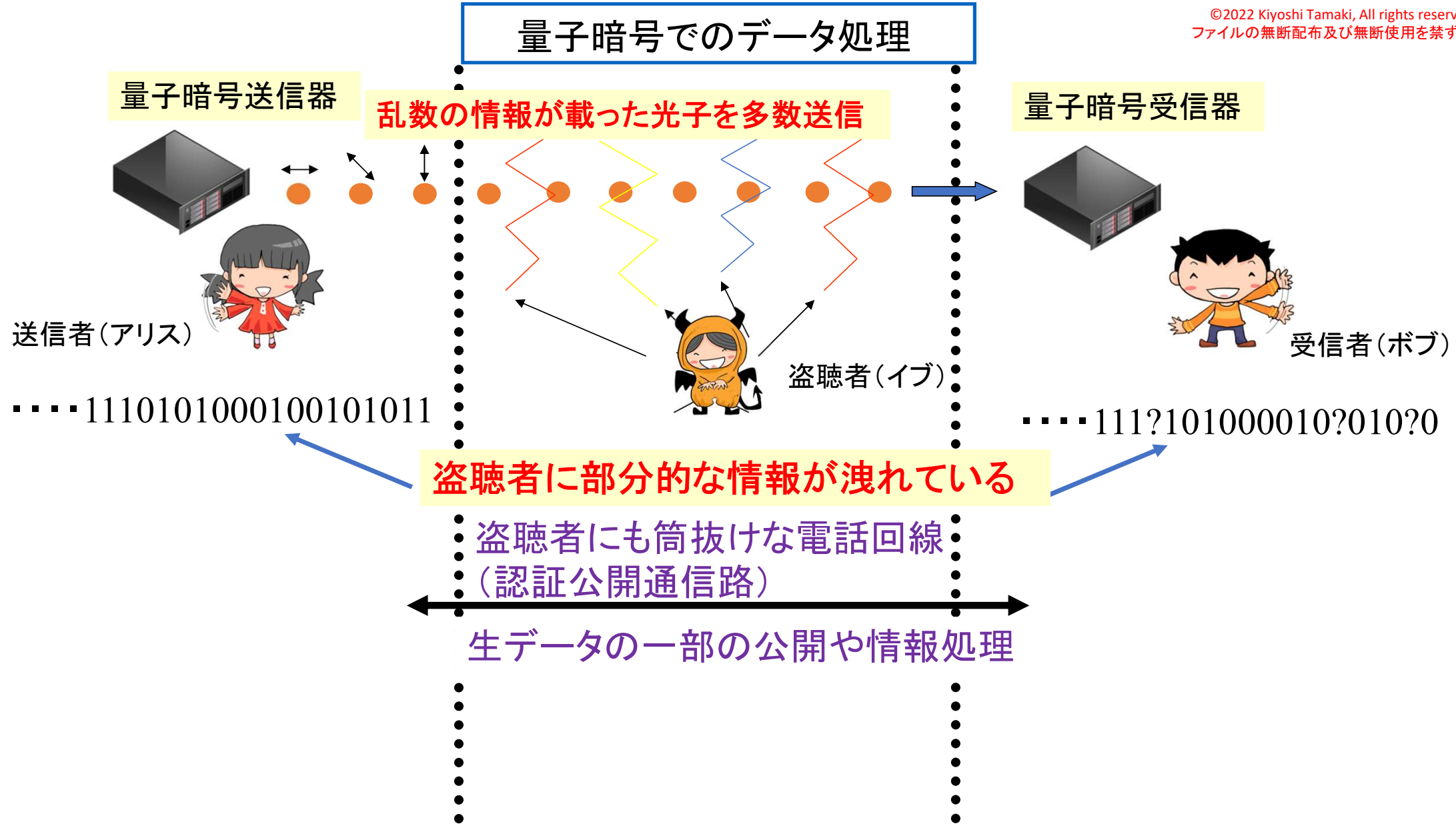
受信者（ボブ）

・・・・1110101000100101011

・・・・111?10100001O?010?0

盗聴者に部分的な情報が洩れている

量子暗号でのデータ処理

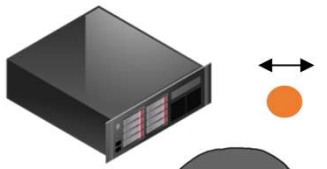


量子暗号でのデータ処理

量子暗号送信器

乱数の情報が載った光子を多数送信

量子暗号受信器



送信者（アリス）

盗聴者（イブ）

受信者（ボブ）

・・・・1110101000100101011

・・・・111?10100001O?010?0

盗聴者に部分的な情報が洩れている

盗聴者にも筒抜けな電話回線
（認証公開通信路）

生データの一部の公開や情報処理

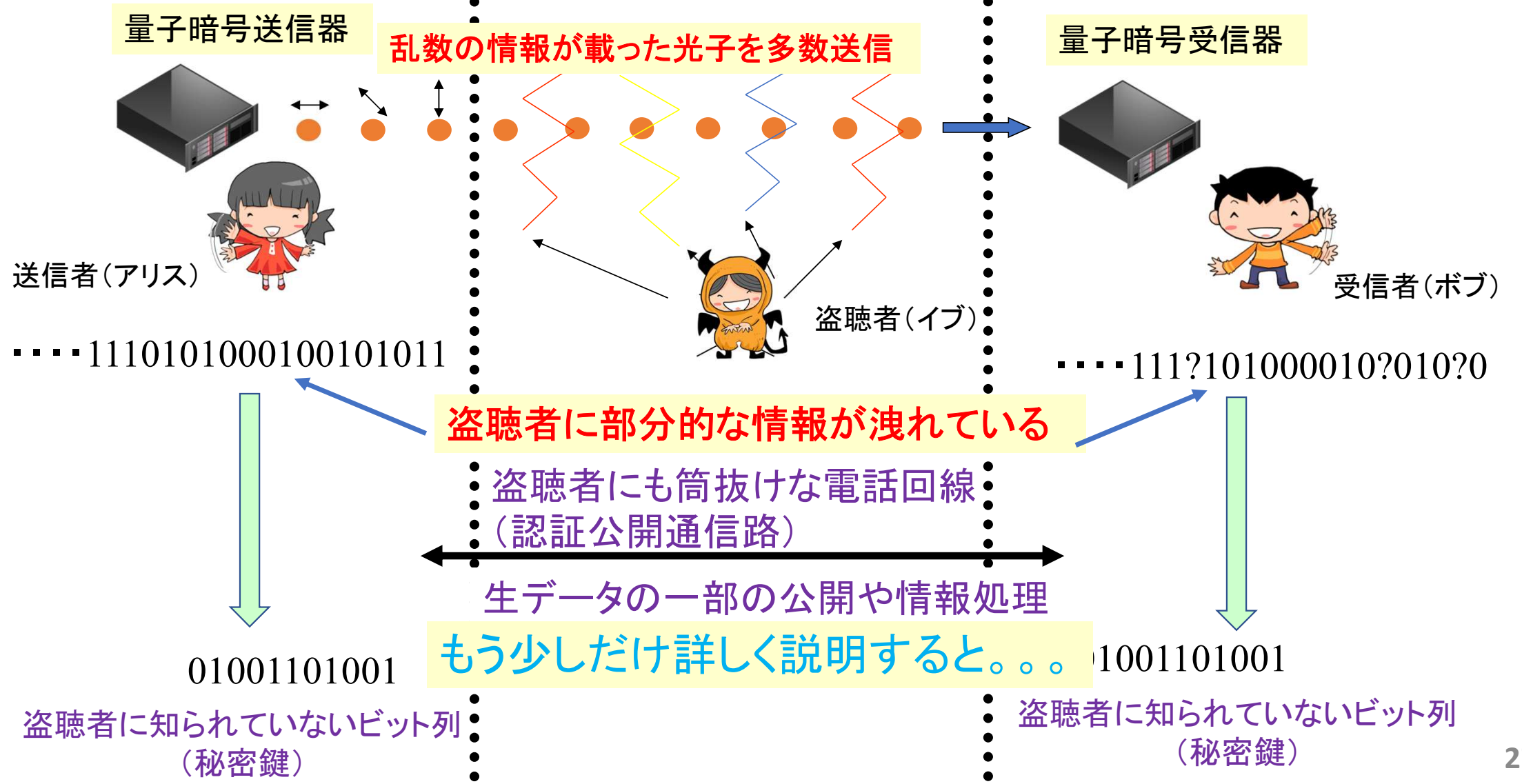
01001101001

盗聴者に知られていないビット列
（秘密鍵）

01001101001

盗聴者に知られていないビット列
（秘密鍵）

量子暗号でのデータ処理

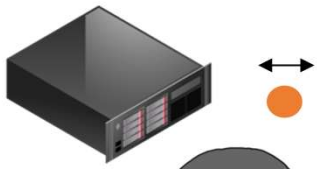


量子暗号でのデータ処理

量子暗号送信器

乱数の情報が載った光子を多数送信

量子暗号受信器



送信者（アリス）

盗聴者（イブ）

受信者（ボブ）

・・・・1110101000100101011

・・・・111?10100001O?010?0

公開認証通信路

ビットエラー訂正
（Eveに部分的な情報がさらに漏れる）

・・・・1101001101011O1

・・・・1101001101011O1

ビット列を適切に縮める
（秘匿性増強）

01001101001
盗聴者に知られていないビット列
（秘密鍵）

01001101001
盗聴者に知られていないビット列
（秘密鍵）

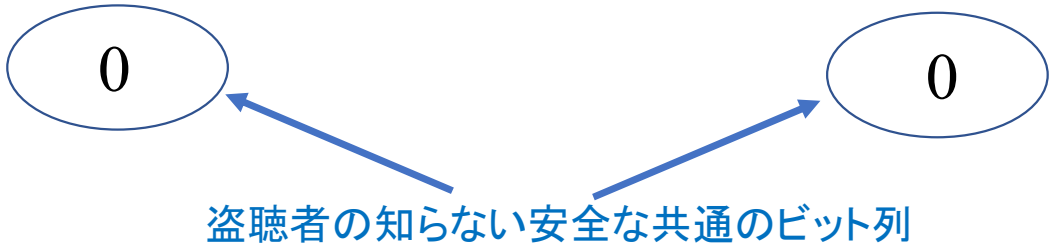
秘匿性増強の例

エラー訂正の後、アリスとボブが同一のビット列(011)を持っているとする。さらに、光子に対しての盗聴やエラー訂正の過程により盗聴者が3ビット中2ビットを知っているとする。アリスとボブは2ビット情報が漏れていることを知っているが、どの2ビットかは知らない、とする。

送信者　　受信者

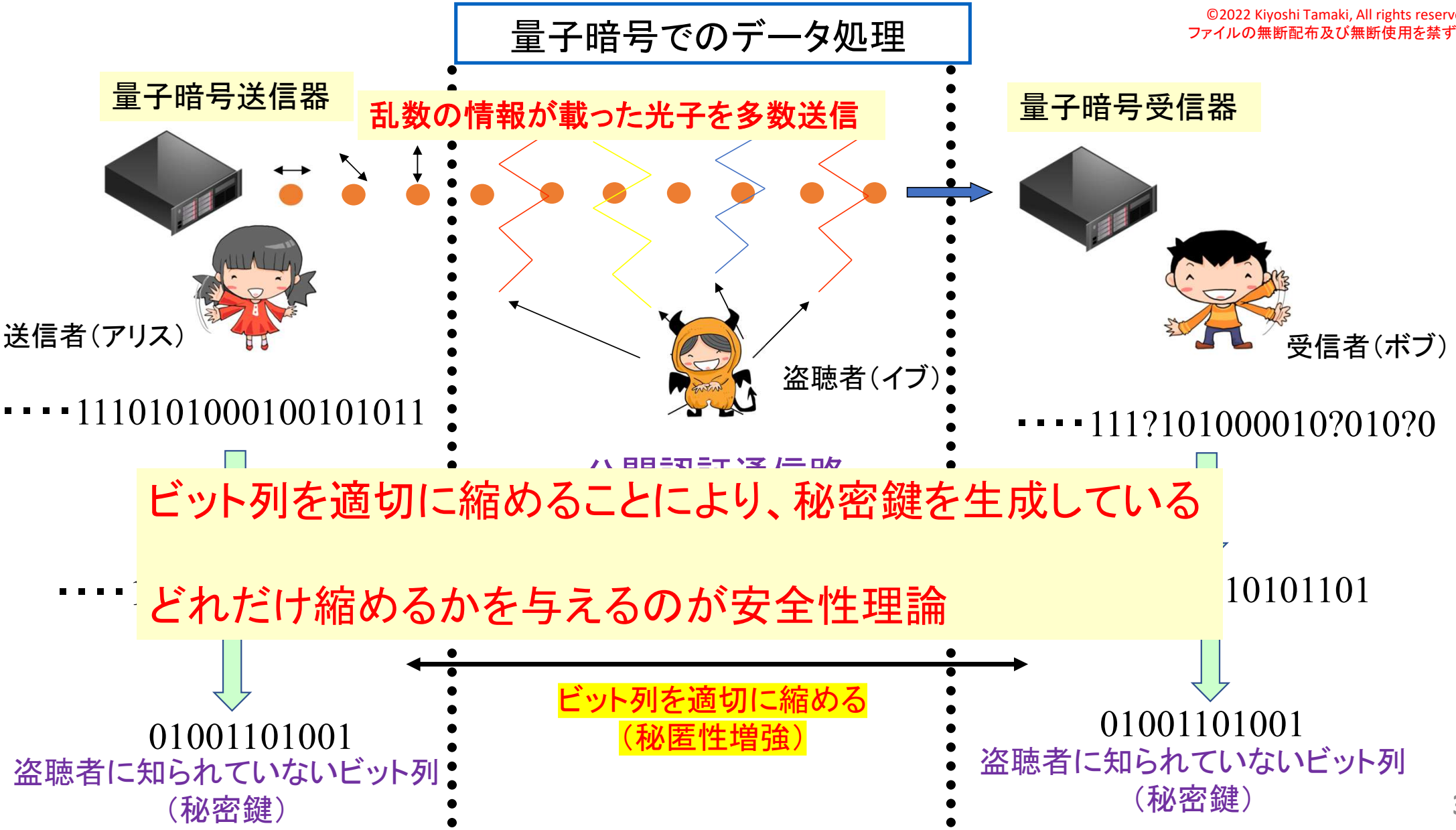
011　　011

公開の話し合いで
『3ビットの足し算をしましょう』
と合意



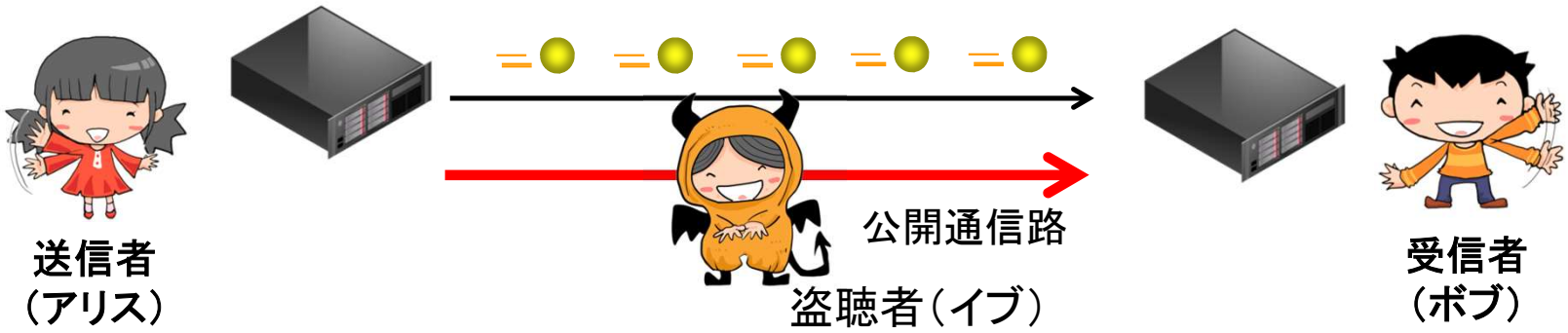
元のビット列を適切に縮めれば、公開での話し合いで安全な鍵へ変換できる
（どれだけ縮めれば良いかを考えるのが理論研究）

量子暗号でのデータ処理



量子暗号
～光子の性質（自然法則）が盗聴を防ぐ！～

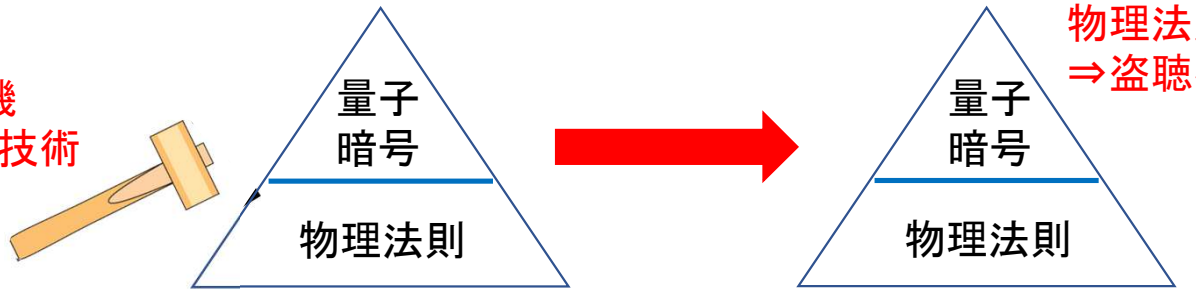
量子暗号専用装置　　光の粒（光子）を使って通信を行う　　量子暗号専用装置



送信者（アリス）　　受信者（ボブ）

どのような盗聴者に対しても量子暗号は安全！

賢い人,AI
量子計算機
1万年後の技術



物理法則は崩れない
⇒盗聴不可能！

量子暗号研究開発の世界情勢

中国

・大規模量子暗号ネットワーク（北京・上海間）
・量子暗号人工衛星
・2025年までに全国規模量子暗号ネットワーク構築

米国

・複数の量子暗号ネットワーク
　・ワシントン・オハイオ州都間
　・ Quantum Xchange社：ニューヨーク-ニュージャージー間の32km（ウォールストリートがターゲット）東芝も参画

量子暗号研究開発の世界情勢

英国

・複数都市間（ケンブリッジ–ロンドン–ブリストル）を量子暗号ネットワークで接続

・BTと東芝が共同で、ロンドンにおいて世界初の量子暗号通信の商用メトロネットワークを構築

EU (OPENQKD)

・オーストリア、チェコ、フランス、ドイツ、ギリシャ、イタリア、オランダ、ポーランド、スペイン、スイス、英国が参画

・40ノード、総距離1000kmのQKDリンク、量子暗号人工衛星も運用

韓国

・SK Telcomが自社5G/LTEネットワーク（ソウル-デジョン間）へQKDを適用

・量子暗号通信網構築モデル事業を推進し、2025年までに16兆円を投じ約190万人の雇用創出を目指す

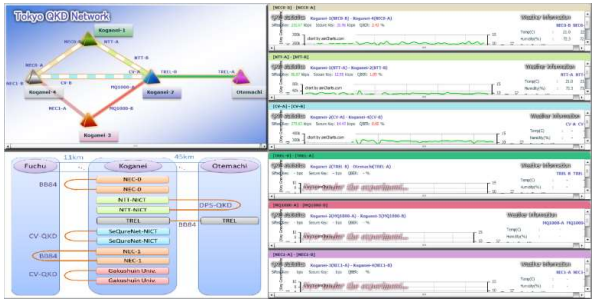
量子暗号研究開発の世界情勢

日本

・東京量子暗号ネットワーク

2010年度～ NICTが主導

主に小金井、大手町など首都圏のQKDネットワーク
最近は、名古屋、大阪、高知とも接続され電子カルテ分散バックアップ実証などを行っている



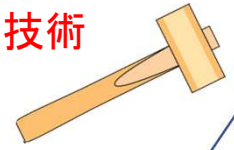
http://www.tokyoqkd.jp/

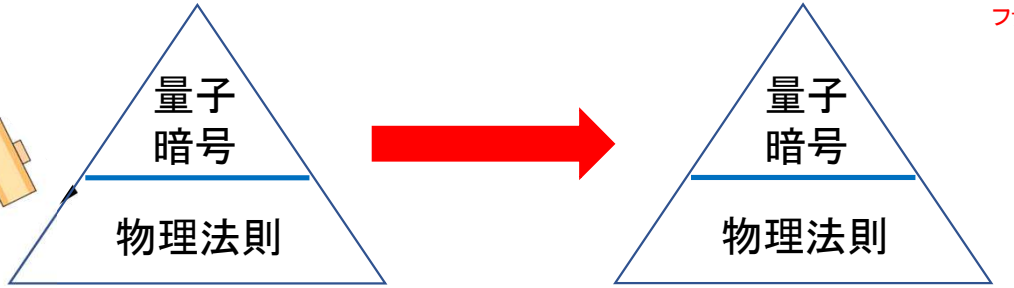
岸田内閣が約90億円を計上（2021度補正予算）

・量子暗号人工衛星も開発中

岸田内閣が約50億円を計上（2021度補正予算）

賢い人,AI
量子計算機
1万年後の技術

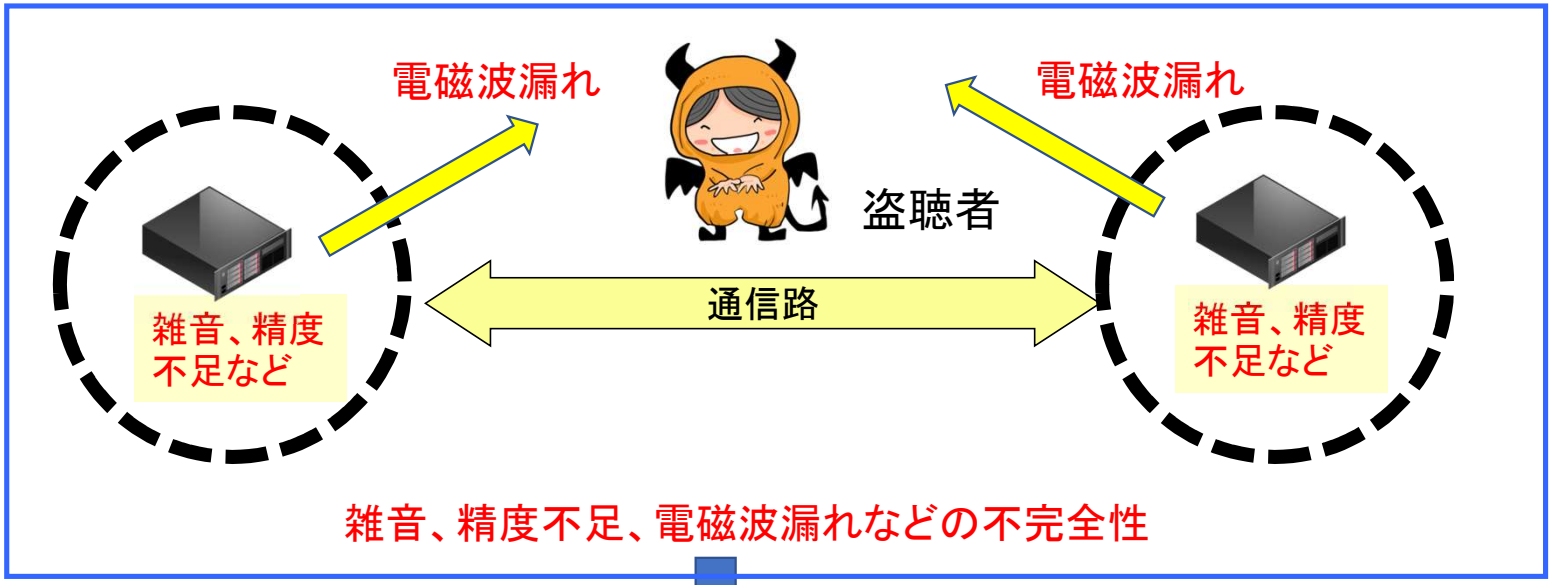




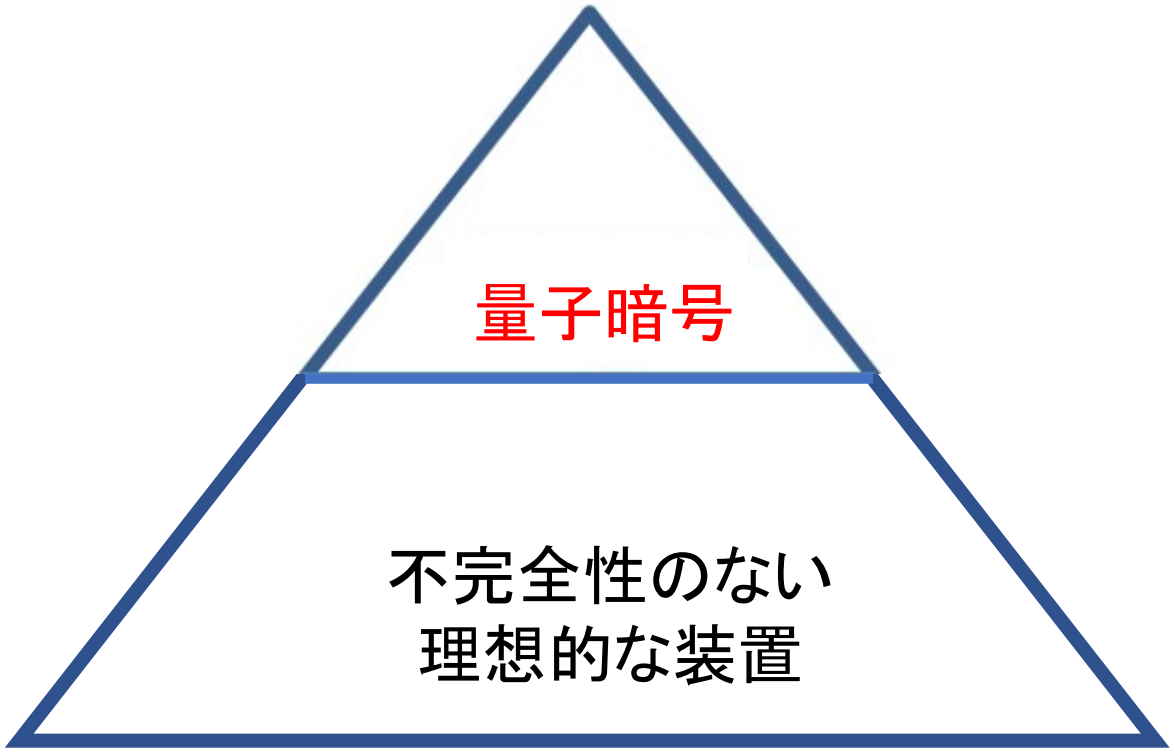
どのような盗聴者に対しても量子暗号は安全！

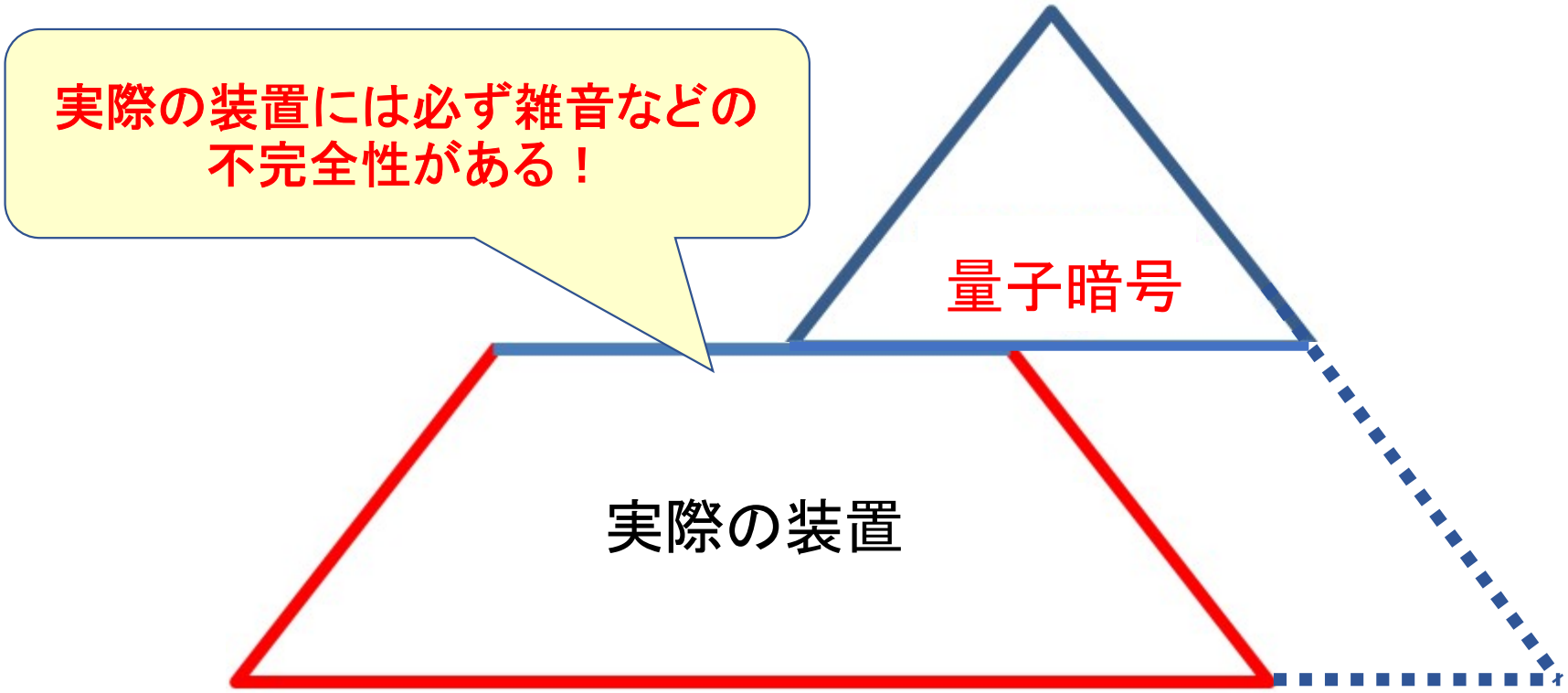
本当？？？

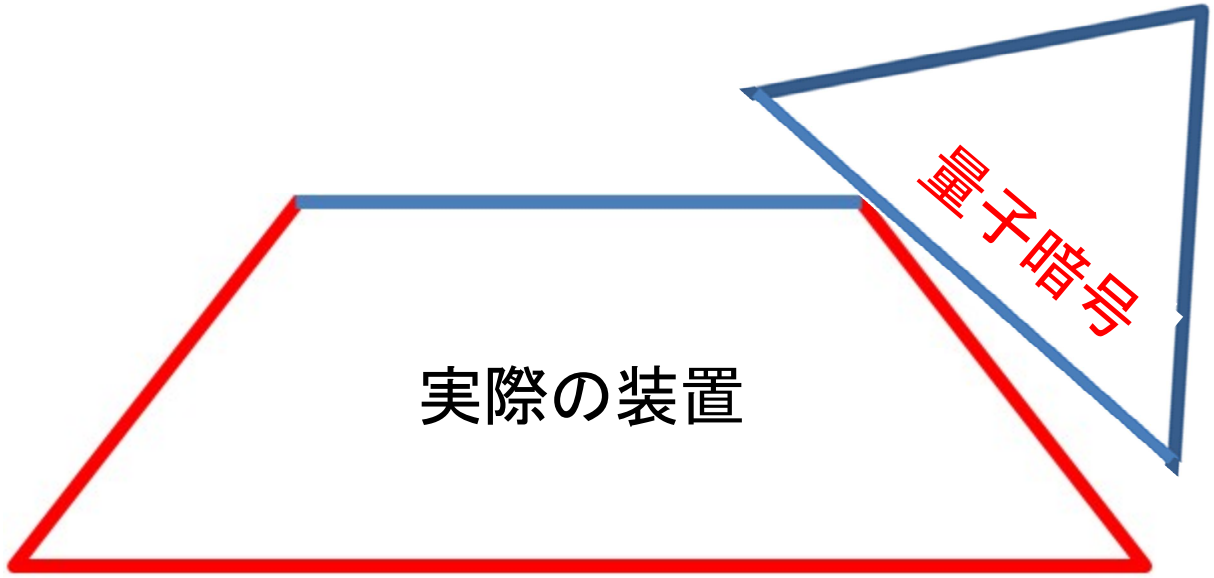
実際の量子暗号装置



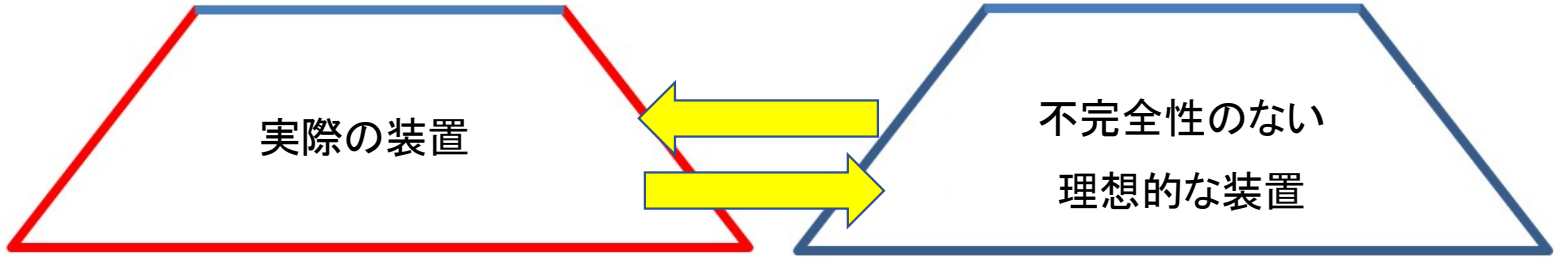
量子暗号は不完全性のない理想的な装置を使えば安全







量子暗号は理想的な装置を使えば安全



実際の装置を使ってどのようにしたら安全な通信ができるか？
（実装安全性の研究）

二つの対策方法

ハードウエアによる対策
実際の装置を理想装置に近づける努力

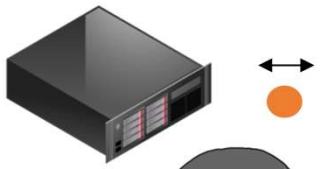
理論による対策
実際の装置の不完全性から漏れる情報量を見積り、ビット列の適切な縮め量を決める

量子暗号でのデータ処理

量子暗号送信器

乱数の情報が載った光子を多数送信

量子暗号受信器



送信者（アリス）

盗聴者（イブ）

受信者（ボブ）

・・・・11101010001001010 11

公開認証通信路

ビットエラー訂正
（Eveに部分的な情報がさらに漏れる）

・・・・110100110101101

ビット列を適切に縮める
（秘匿性増強）

01001101001
盗聴者に知られていないビット列
（秘密鍵）

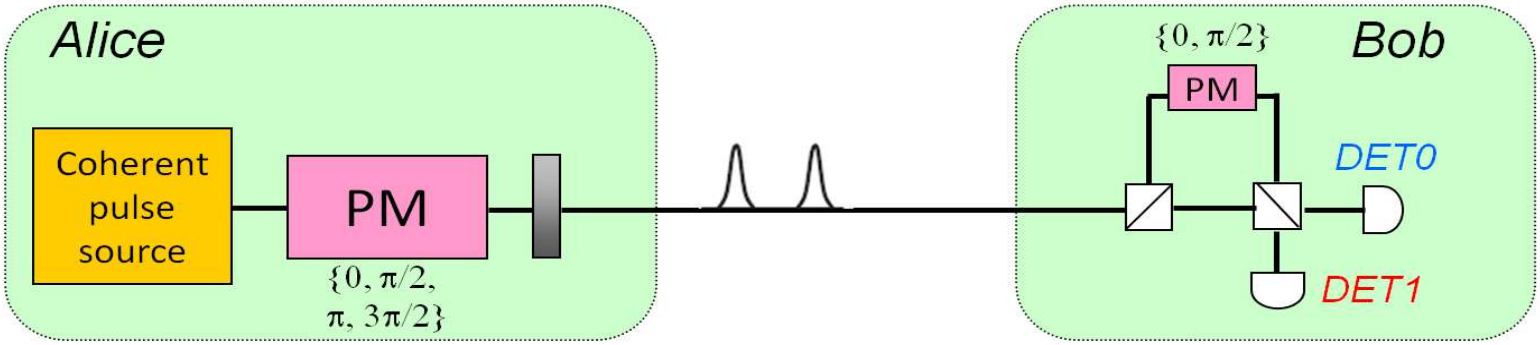
・・・・111?10100001 0?010?0

・・・・110100110101101

01001101001
盗聴者に知られていないビット列
（秘密鍵）

不完全性のない理想的な暗号装置（任意の盗聴に対して安全）

アリスとボブから想定外の情報漏れはない



変調が厳密な値（精度無限）: $\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$

所望の単一光子が放出される

測定の数学的な記述

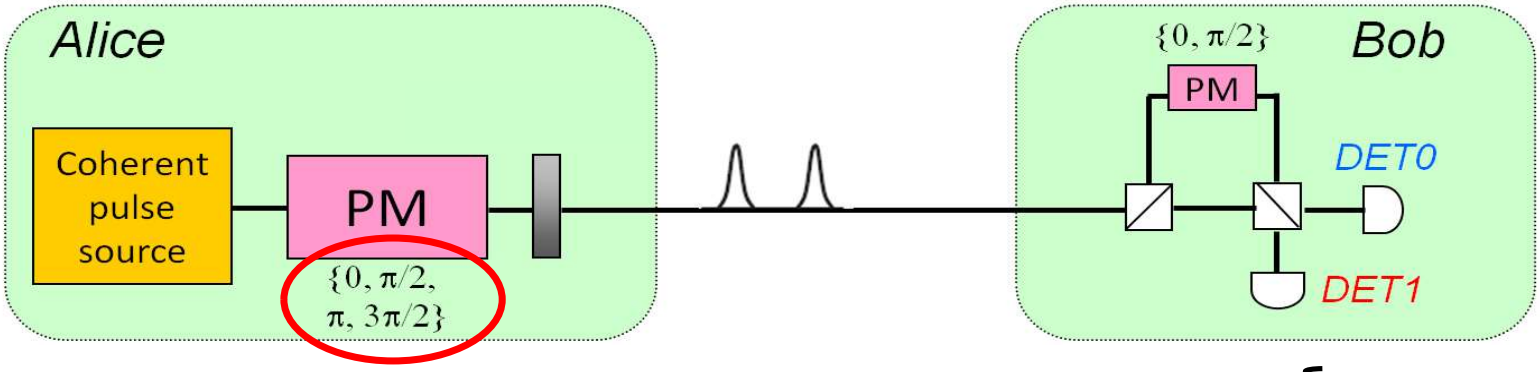
- Z-basis: $\{\widehat{M}_{0Z}, \widehat{M}_{1Z}, \widehat{M}_f\}$
- X-basis: $\{\widehat{M}_{0X}, \widehat{M}_{1X}, \widehat{M}_f\}$

上記のことを仮定すると、上の装置からは安全な鍵が生成できることが量子力学や情報理論を用いて証明することができます（安全性証明）

(疑問): 上記の仮定は実際の装置では成り立ちますか？

実際の暗号装置

アリスとボブから想定外の情報漏れはない



変調が厳密な値（精度無限）: ~~$\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$~~

所望の単一光子が放出される

測定の数学的な記述

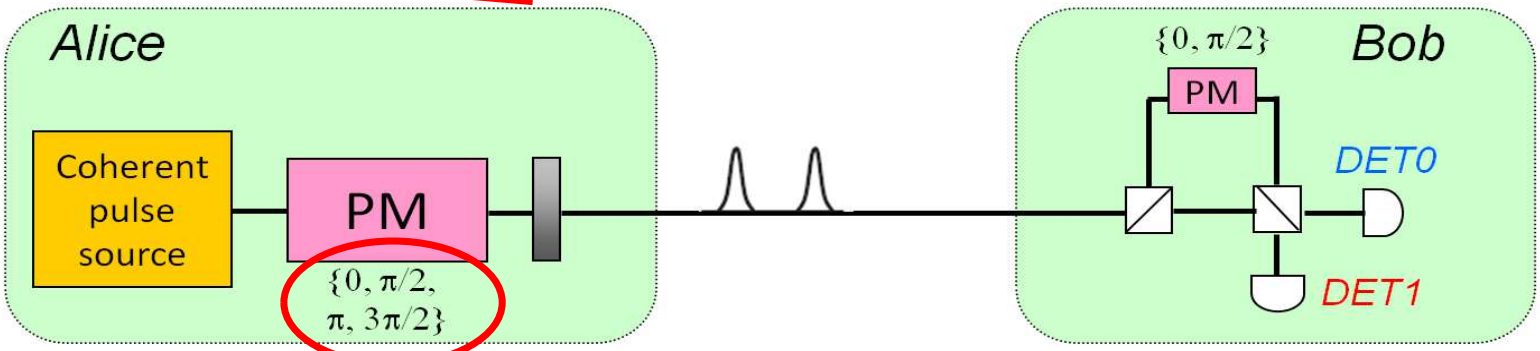
- Z-basis: $\left\{\hat{M}_{0Z}, \hat{M}_{1Z}, \hat{M}_f\right\}$
- X-basis: $\left\{\hat{M}_{0X}, \hat{M}_{1X}, \hat{M}_f\right\}$

我々が提案したロス耐性プロトコルにより解決

K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014)

実際の暗号装置

~~アリスとボブから想定外の情報漏れはない~~



変調が厳密な値（精度無限）: ~~$\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$~~ OK

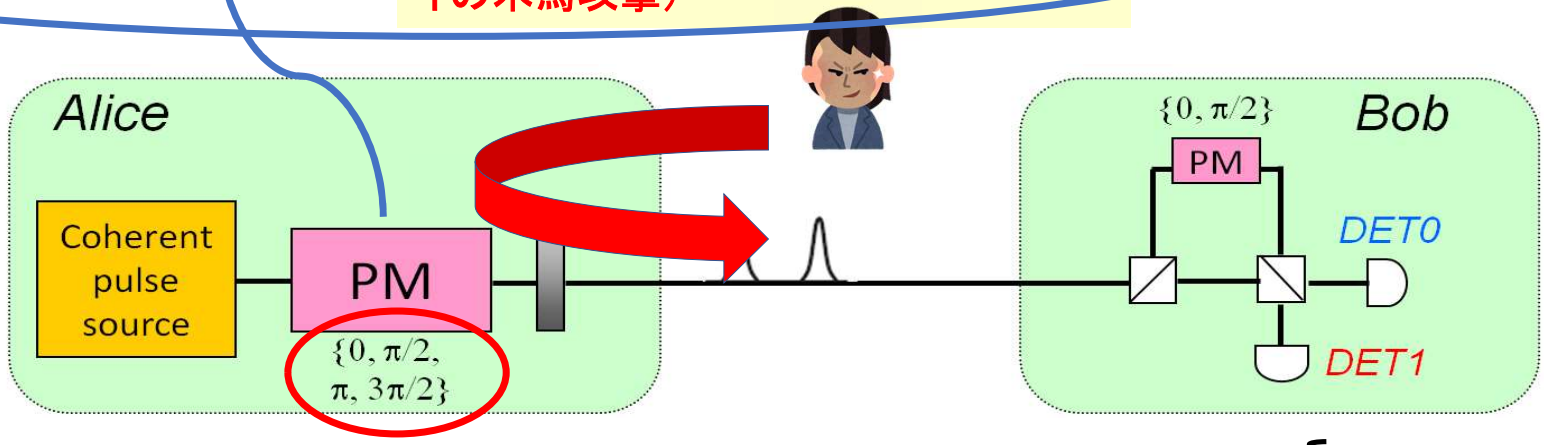
~~所望の単一光子が放出される~~

・所望の偏光、周波数など以外の成分が混ざる
・パルス間に相関がある！

測定の数学的な記述
- Z-basis: $\{\hat{M}_{0Z}, \hat{M}_{1Z}, \hat{M}_f\}$
- X-basis: $\{\hat{M}_{0X}, \hat{M}_{1X}, \hat{M}_f\}$

電子機器からの電磁波漏れ、振動などによる情報漏れ

イブは強い光を送り付け、その反射光から内部情報を読み取ろうとする（トロイの木馬攻撃）



変調が厳密な値（精度無限）: $\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$ OK

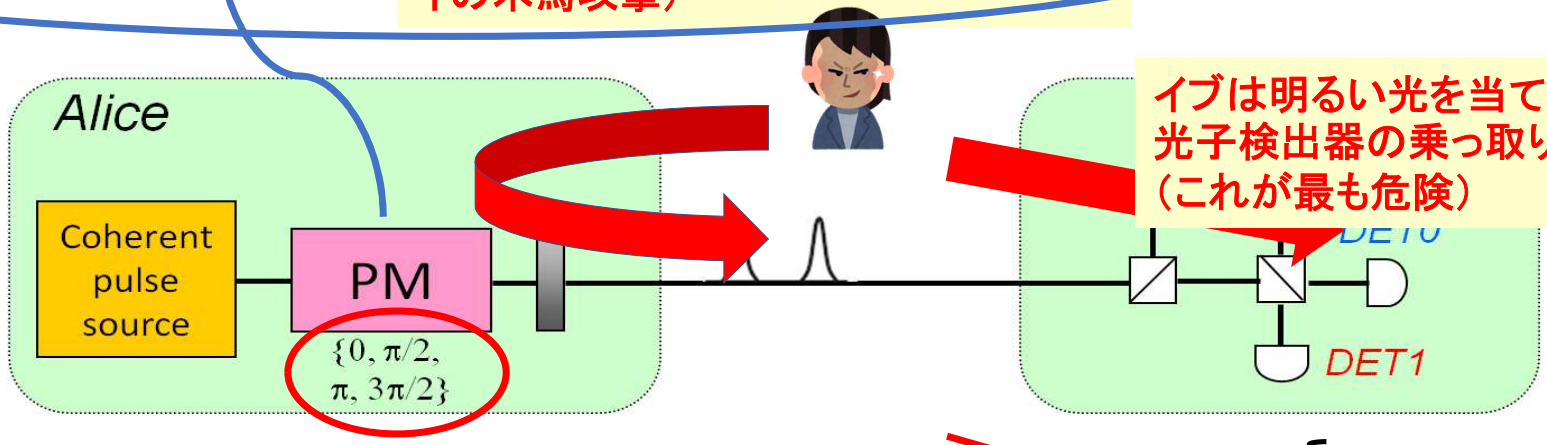
~~所望の単一光子が放出される~~

測定の数学的な記述
- Z-basis: $\{\hat{M}_{0Z}, \hat{M}_{1Z}, \hat{M}_f\}$
- X-basis: $\{\hat{M}_{0X}, \hat{M}_{1X}, \hat{M}_f\}$

・所望の偏光、周波数など以外の成分が混ざる
・パルス間に相関がある！

電子機器からの電磁波漏れ、振動などによる情報漏れ

イブは強い光を送り付け、その反射光から内部情報を読み取ろうとする（トロイの木馬攻撃）



イブは明るい光を当てることによる光子検出器の乗っ取り*（これが最も危険）

変調が厳密な値（精度無限）：$\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$ OK

~~所望の単一光子が放出される~~

・所望の偏光、周波数など以外の成分が混ざる
・パルス間に相関がある！

~~測定の数学的な記述~~

~~Z-basis: $\{\hat{M}_{0Z}, \hat{M}_{1Z}, \hat{M}_f\}$~~

~~X-basis: $\{\hat{M}_{0X}, \hat{M}_{1X}, \hat{M}_f\}$~~

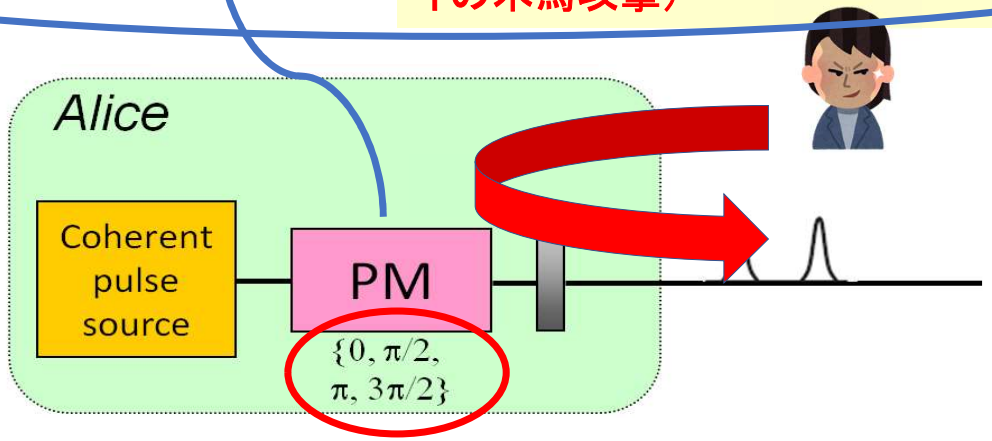
実際の量子暗号装置は穴（セキュリティーループホール）が多かった

強力な対策がある！

*L. Lydersen,et. al, Nature Photonics 4, 686 - 689 (2010)

電子機器からの電磁波漏れ、振動などによる情報漏れ

イブは強い光を送り付け、その反射光から内部情報を読み取ろうとする（トロイの木馬攻撃）

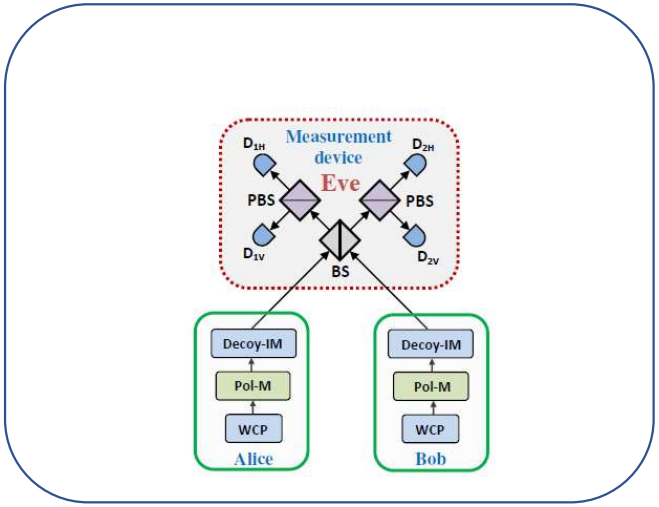


変調が厳密な値（精度無限）：$\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ OK

~~所望の単一光子が放出される~~

・所望の偏光、周波数など以外の成分が混ざる
・パルス間に相関がある！

H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012)



測定装置無依存量子暗号

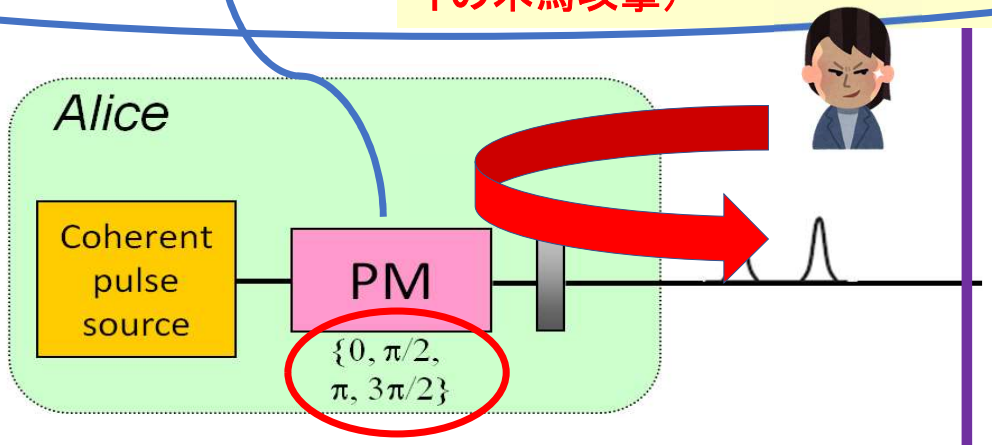
⇒ 受信器のセキュリティーループホールは完全に防げる！（仮想的量子相関の利用）

実際の量子暗号装置は穴（セキュリティーループホール）が多かった

強力な対策がある！

電子機器からの電磁波漏れ、振動などによる情報漏れ

イブは強い光を送り付け、その反射光から内部情報を読み取ろうとする（トロイの木馬攻撃）

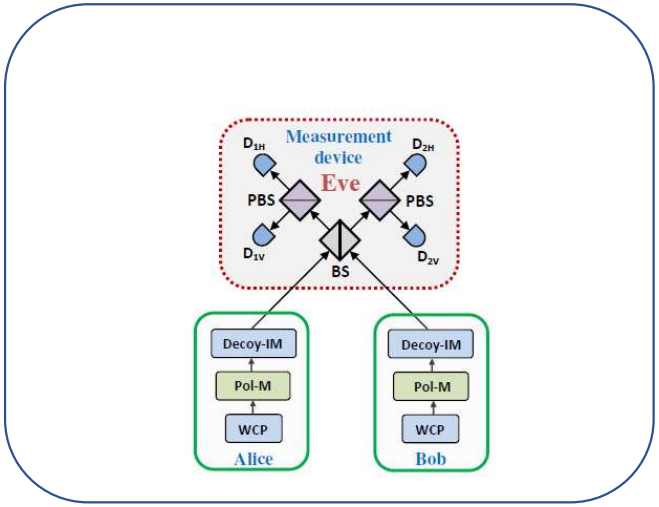


変調が厳密な値（精度無限）: ~~$\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$~~ OK

~~所望の単一光子が放出される~~

・所望の偏光、周波数など以外の成分が混ざる
・パルス間に相関がある！

H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012)



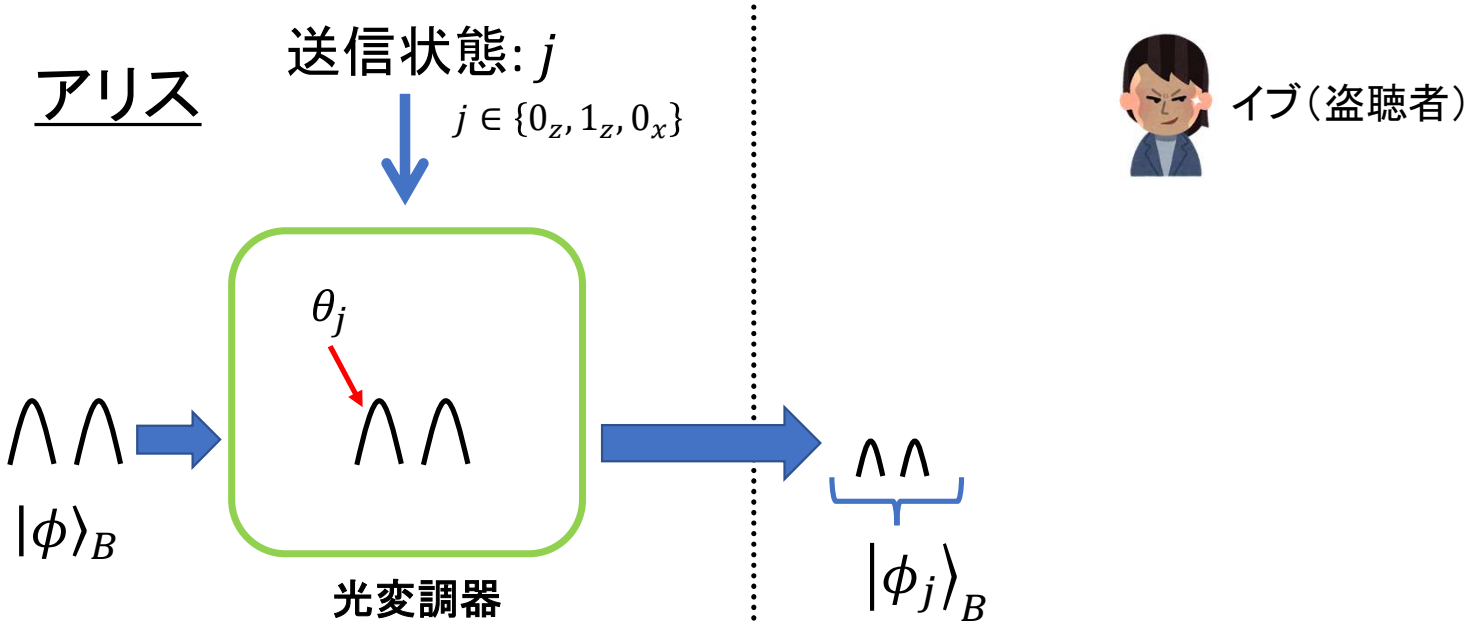
測定装置無依存量子暗号

⇒ 受信器のセキュリティーループホールは完全に防げる！（仮想的量子相関の利用）

残った仕事は、送信器を安全にすること！

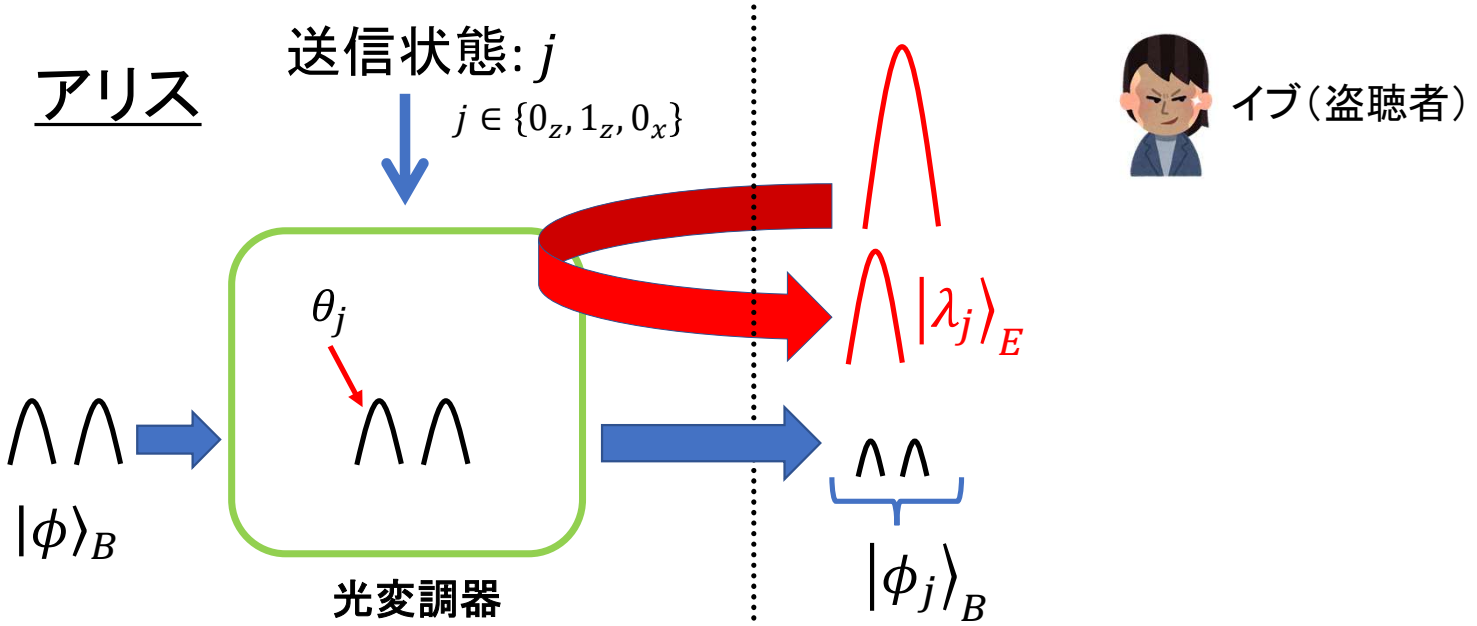
数多くある不完全性をどのように表すか? その表現を元にどのように安全性を証明するか？

トロイの木馬攻撃や電磁波などによる情報漏れ



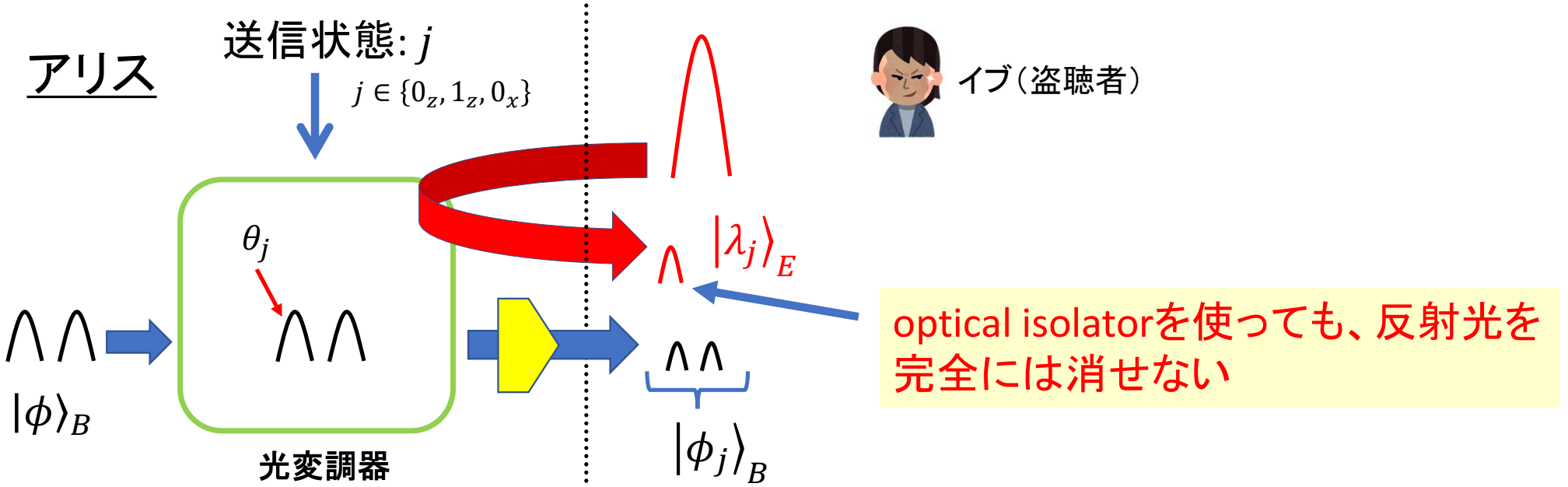
イブ（盗聴者）

トロイの木馬攻撃や電磁波などによる情報漏れ



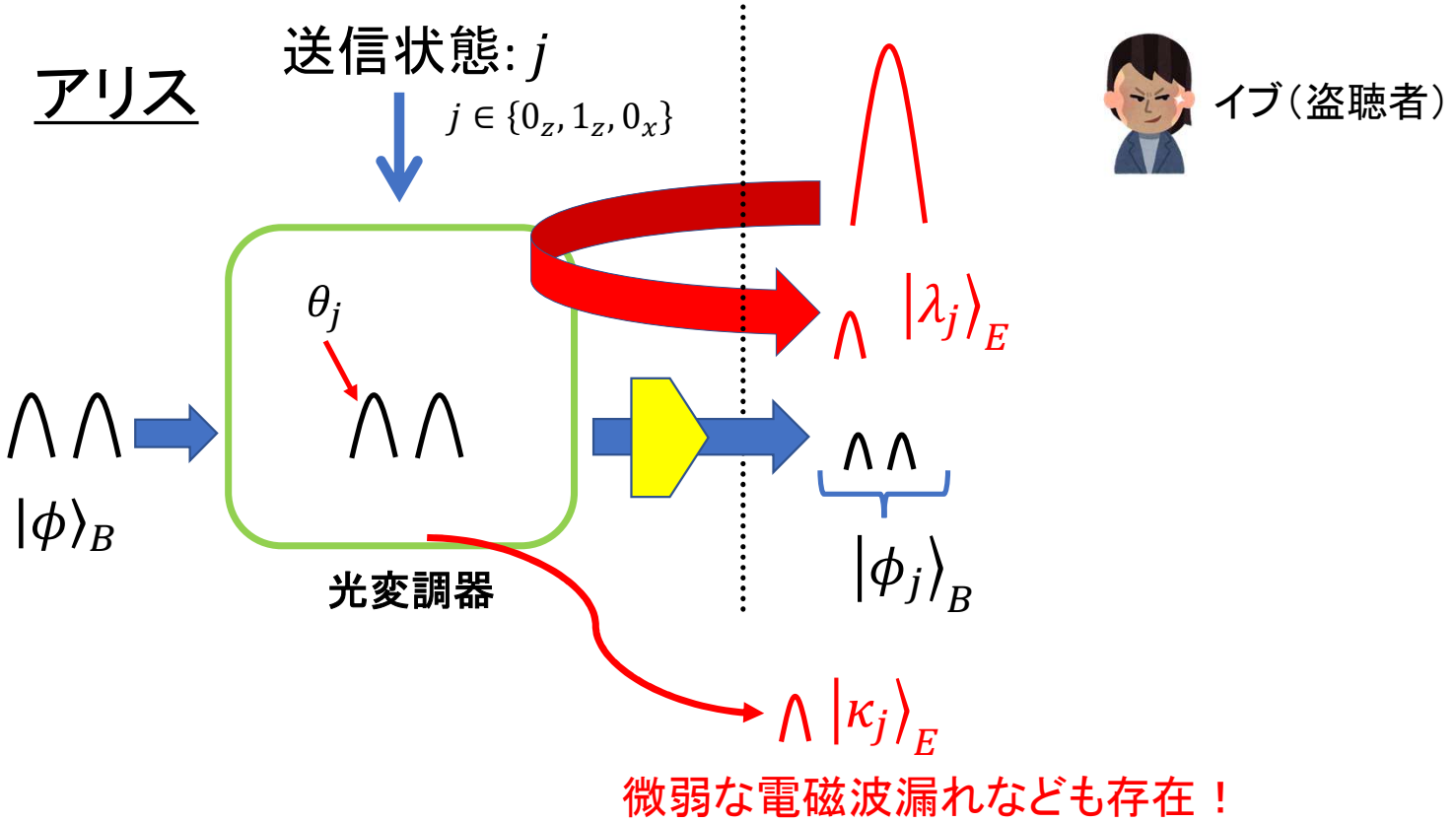
イブ（盗聴者）

トロイの木馬攻撃や電磁波などによる情報漏れ



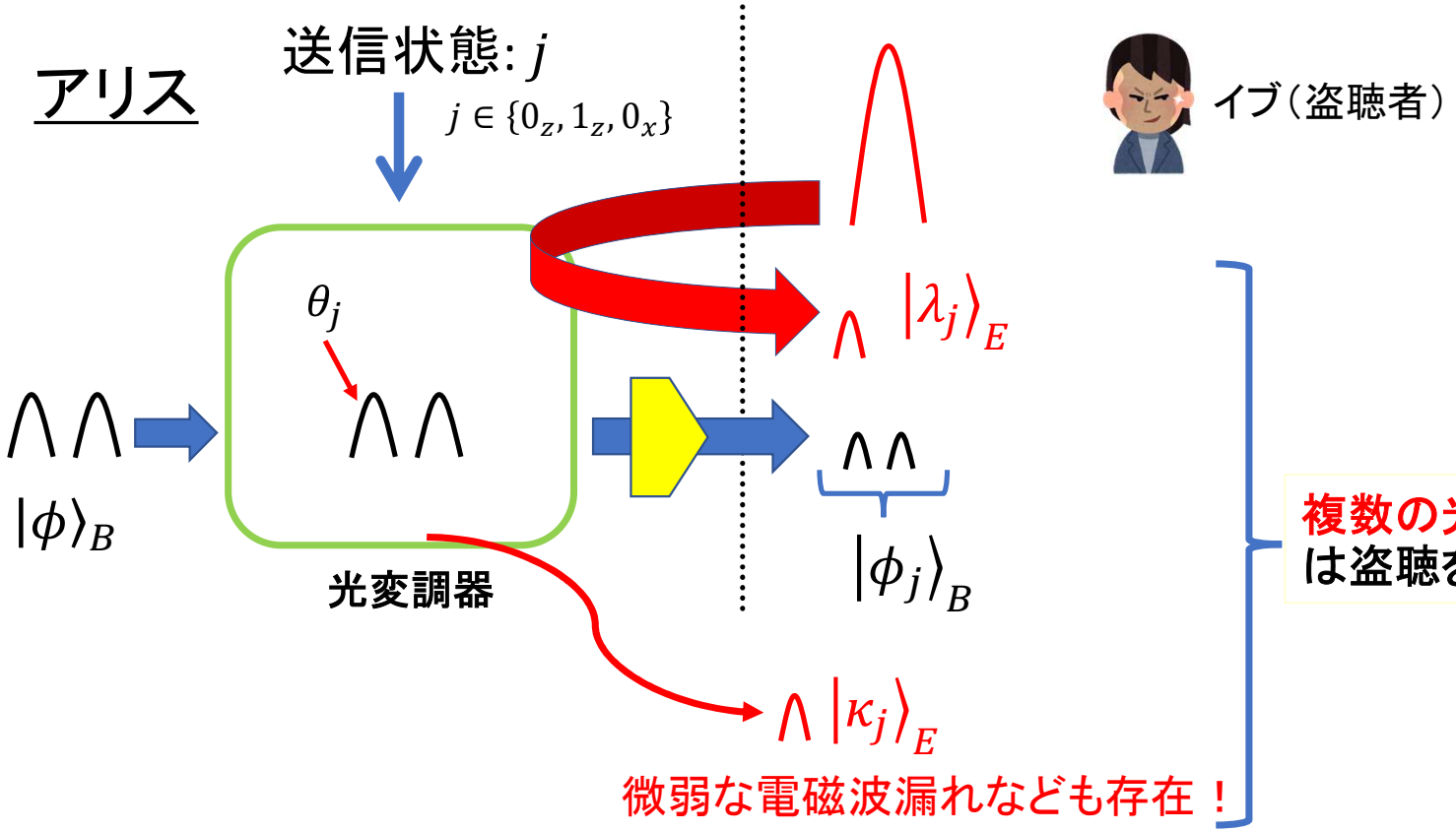
ハードウエアでの対策：optical isolatorを使う（イブからアリスへの照射光の強度を下げる）

トロイの木馬攻撃や電磁波などによる情報漏れ



ハードウエアでの対策：optical isolatorを使う（イブからアリスへの照射光の強度を下げる）

トロイの木馬攻撃や電磁波などによる情報漏れ

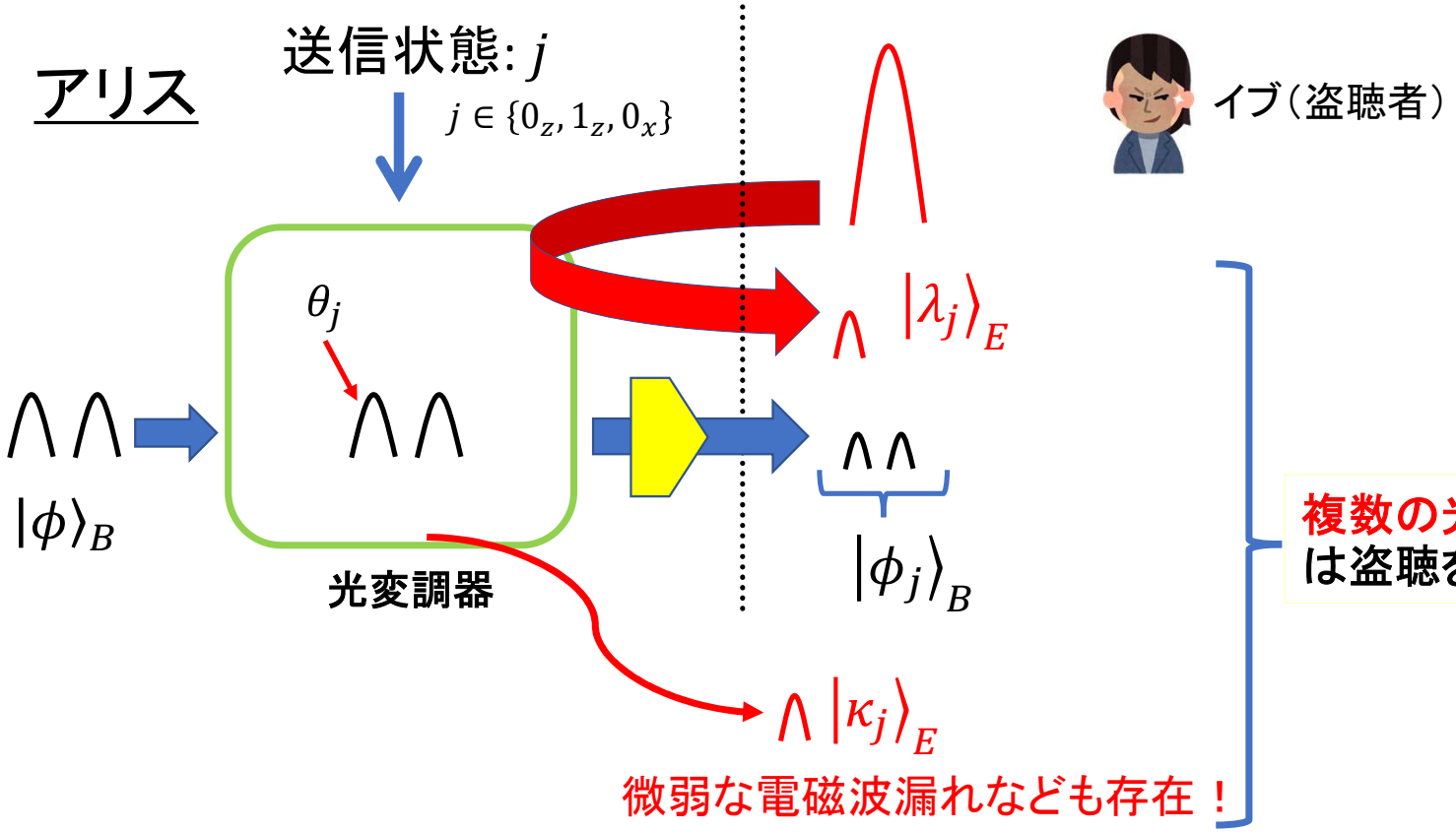


イブ（盗聴者）

複数の光（多モード）を得ることにより、イブは盗聴をしやすくなる

ハードウエアでの対策：optical isolatorを使う（イブからアリスへの照射光の強度を下げる）

トロイの木馬攻撃や電磁波などによる情報漏れ



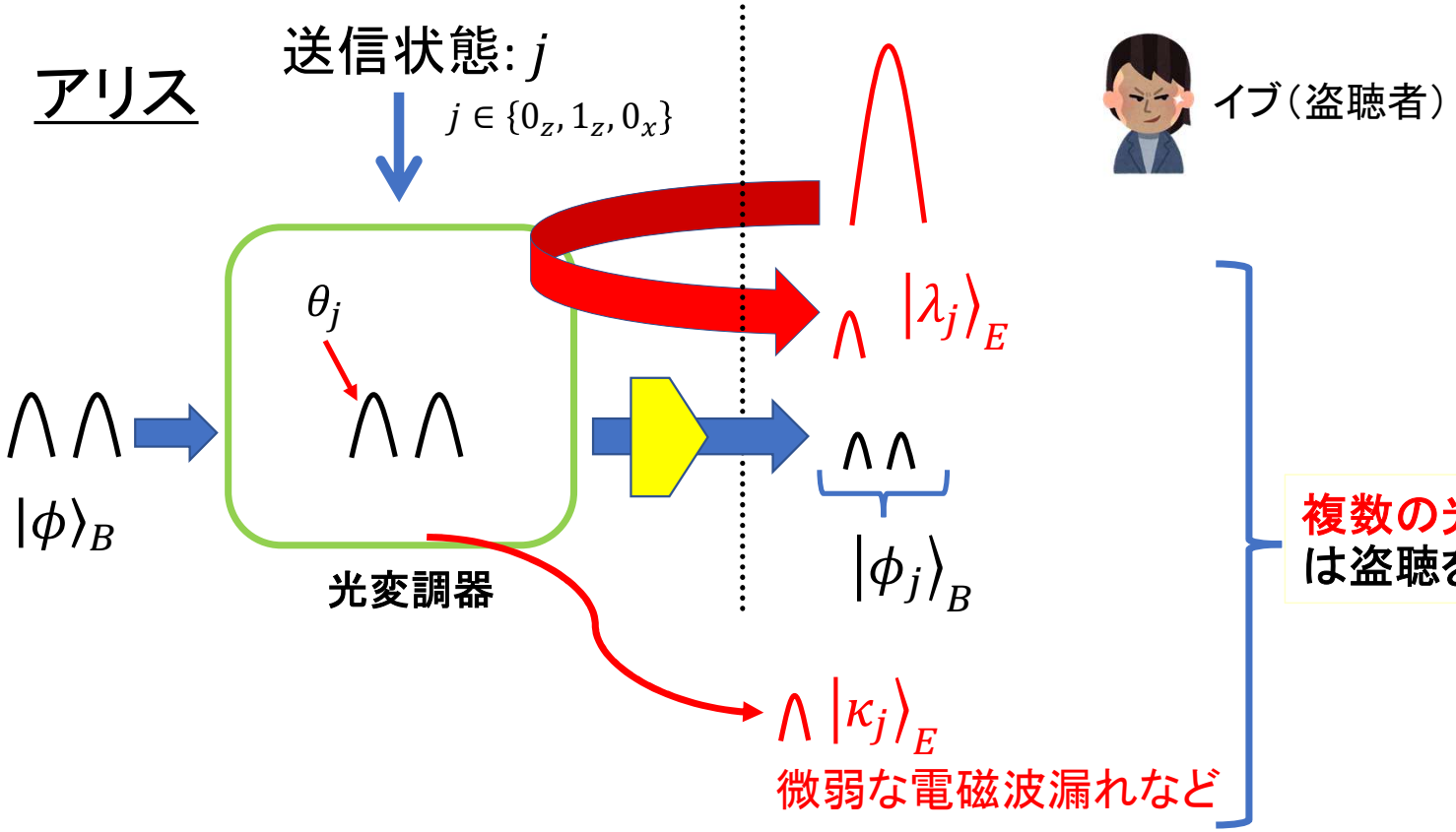
イブ（盗聴者）

複数の光（多モード）を得ることにより、イブは盗聴をしやすくなる

ハードウエアでの対策：optical isolatorを使う（イブからアリスへの照射光の強度を下げる）

理論的対策のヒント：送信器からの情報漏れは多モードを使ったQKDと見なせる！

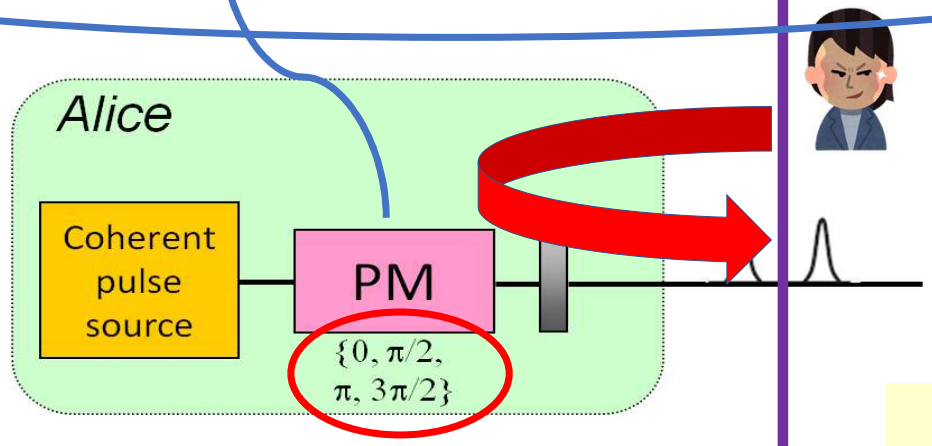
トロイの木馬攻撃や電磁波などによる情報漏れ



あらゆる情報漏れが
理想状態（$|\phi_j\rangle_B$）に少しだけ変更した状態で簡潔に表せることが分かった！

電子機器からの電磁波漏れ、振動などによる情報漏れ

イブはトロイの木馬攻撃によって一部の情報を不正に得ることができる



変調が厳密な値（精度無限）: $\left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$ OK

~~所望の単一光子が放出される~~

・所望モード以外の成分が混じる
(偏向、周波数などの揺らぎによる)
・パルス間に相関がある！

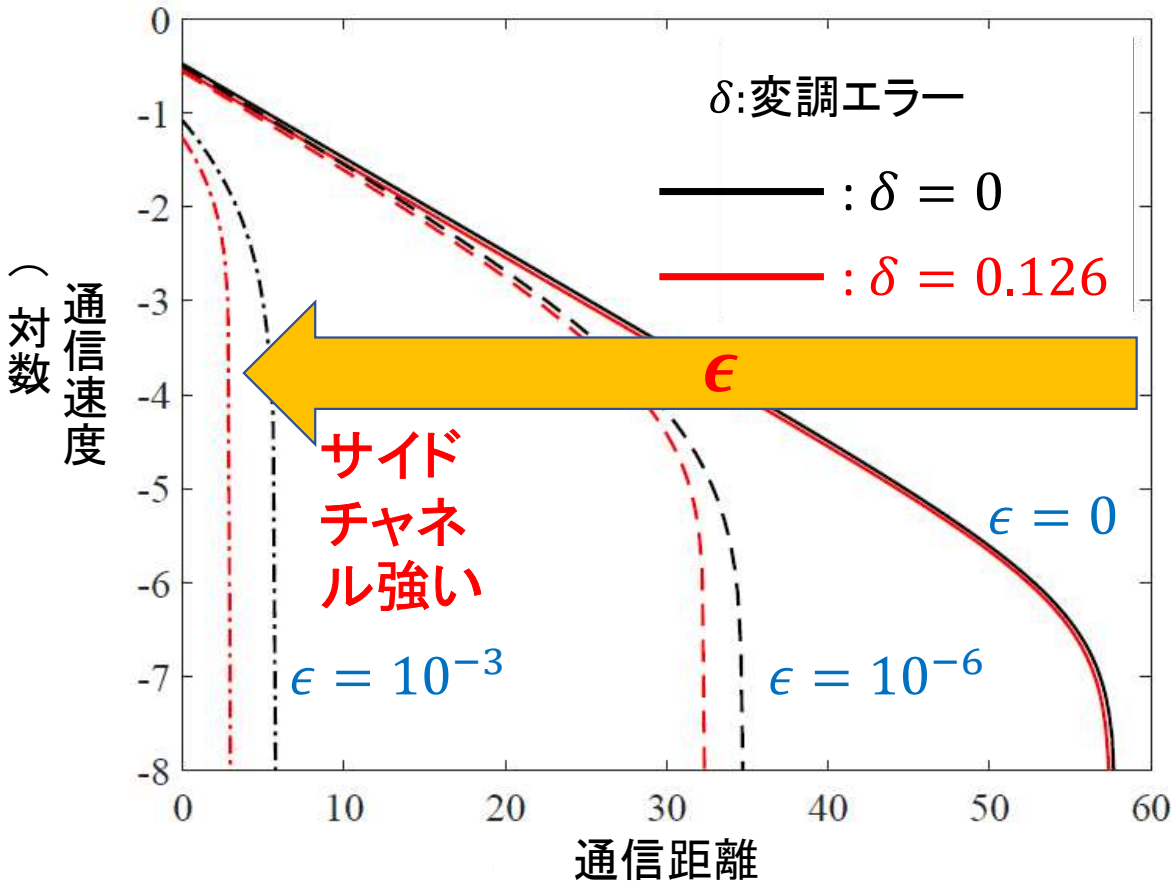
$$\sqrt{1-\epsilon_j}\left|\phi_j\right\rangle_B\left|\lambda\right\rangle_E + \sqrt{\epsilon_j}\left|\Lambda_j^{\perp}\right\rangle_{BE}$$

どのような情報漏れもこの式で表せる

この表現をもとにした安全性証明も開発・発展してきている

M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Science Advances 6, no. **37**, eaaz4487 (2020)
Á. Navarrete, M. Pereira, M. Curty, and K. Tamaki, Phys. Rev. Applied **15**, 034072 (2021)

安全性証明から算出される通信距離の例



通信距離向上のためにはハードウエアによる対策が必要
（例：性能の高いoptical isolator を使う、電磁波漏れを防ぐためのシールドを強化するなど）

ハードウエアだけでサイドチャネルを防いでいるわけではない！（理論による保証とハードによる影響低減）

まとめ

サイドチャネル対策

理論的には任意の不完全性を取り扱えるようになってきた

＋

ハードウエアでの対策により通信速度向上

- ✓ 最も危険とされてきた受信器には完ぺきな対策がある
- ✓ 送信器へのサイドチャネル対策はほぼ完ぺきになりつつある