MITSUBISHI ELECTRIC
Changes for the Better

量子暗号の基礎と その実用化に向けて

鶴丸豊広
三菱電機株式会社
@IBIS2010, 2010/11/06

量子暗号の特徴

量子論を安全性の根拠とする「絶対に破れない」暗号技術

現代暗号 vs. 量子暗号

現代暗号 (AES, MISTY, Camellia, RSA暗号など)

高速：数百Mbps (S/W) ～ 数十Gbps (LSI)

計算量的安全性：現在の計算機を想定した解読に対しては安全だが，
将来超高速な計算機が出現した時に解読される可能性あり.

量子暗号（BB84方式, B92方式，DPSQKD方式ほか）

低速：数十kbps～1Mbps

絶対的安全性：どんなに計算機が進歩しても解読できない.

量子力学の公理から出発して、安全性を数学的に証明する

- この講演ではもっぱら量子鍵配送（quantum key distribution, QKD）の、BB84方式（Bennett-Brassard 1984 protocol）についてのべる
- とくに線型符号の果たす役割、および装置開発の状況を説明する。

市販の量子暗号装置

- **Clavris²** （ id Quantique社）

  プロトコル: BB84, SARG04
  光学系: Plug & Play方式
  通信距離: >50 km
  通信速度: >1Kbps (@25km)

http://www.idquantique.com より

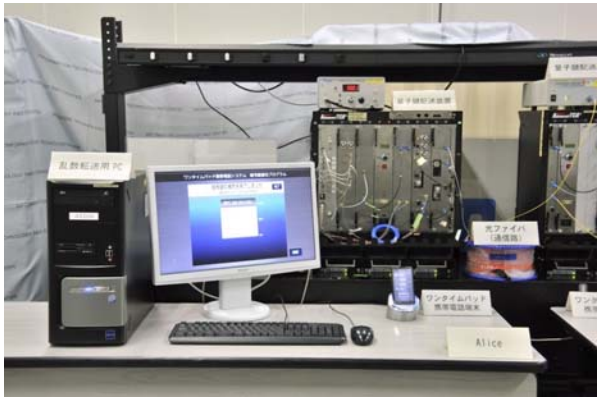
- **QPN 8505** (MagiQ Technologies社)

  プロトコル: BB84方式 with デコイ
  光学系: 不明
  通信距離: ～140km
  通信速度 ～100bps (?)

http://www.magiqtech.com より

三菱電機の量子暗号システム

- プロトコル： BB84方式 with デコイ
- 光学系: 一方向通信
- 通信距離: > 50km
- 通信速度: >20kbps (@20km)



- 携帯電話に秘密鍵を供給し、
  ワンタイムパッド通信を行うことが出来る

- Tokyo QKD Networkでも活躍（後述）

※NEC, NTT, 東芝欧州研なども試作機開発済（後述）

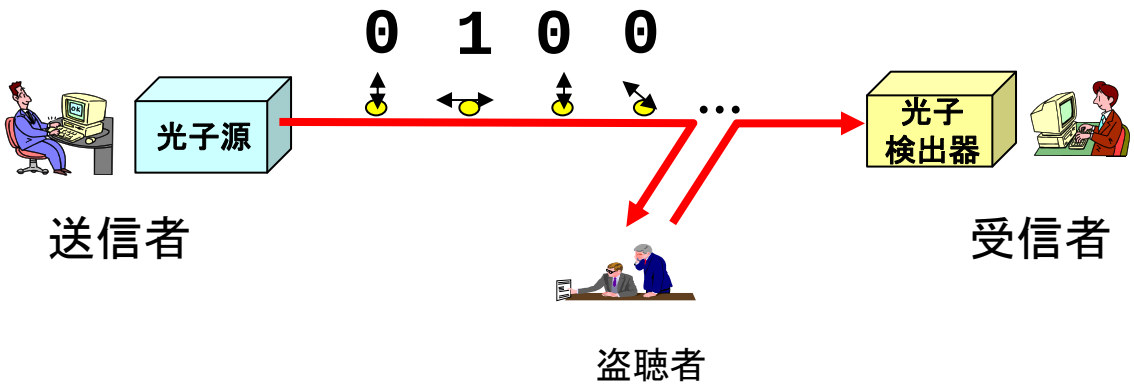
量子暗号の無条件安全性 （イメージ）

量子暗号では、光の粒子（光子）に0,1の乱数を乗せて送る

この乱数値は「測定すると必ず影響を受けて変化」← 量子論

→ 盗聴があればノイズが増加し、あとで必ず露見する

通信路を全て盗聴者にのっとられても安全という状況を実現するのが目的

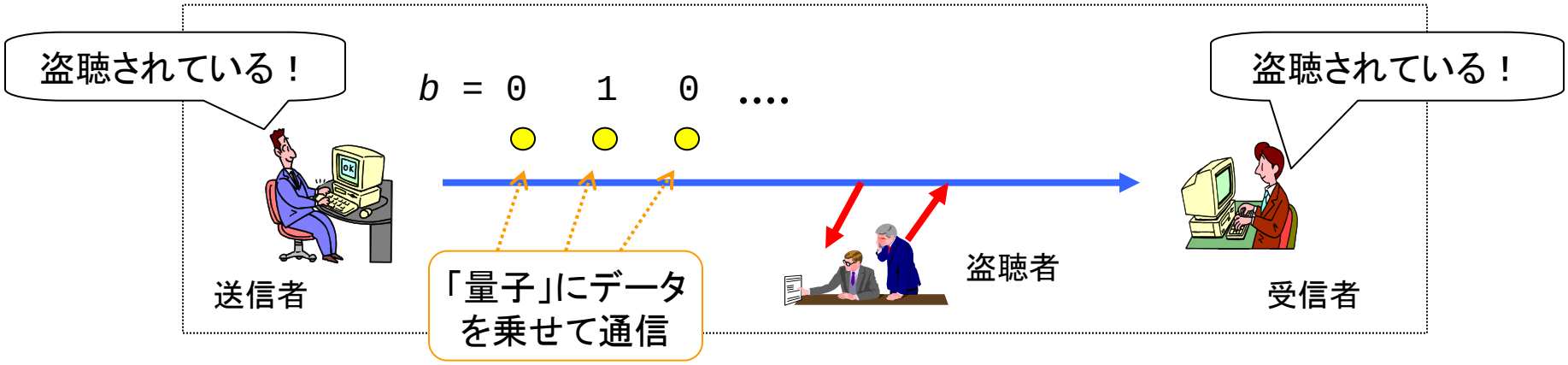


したがって通信路ノイズには敏感 → 通信距離と安全性に相関がある

- 長距離化 → 通信路ノイズ増加 → 盗聴ノイズとの区別がより困難になる
- 光を強める → 光子の数を増やすことに相当 → コピーが作れて盗聴が容易に
- 中継点での増幅も困難 …増幅には測定がともなう

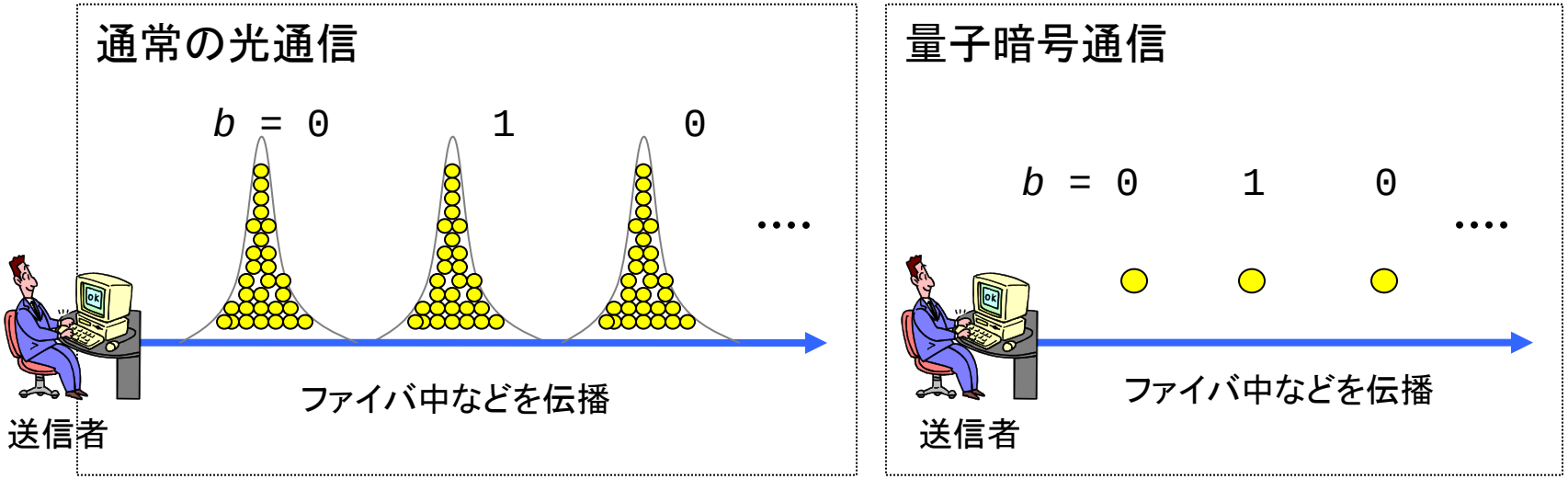
「量子」に乱数ビットをのせる

- 量子とは？
  - この世の物質は全て量子であり、
    波としての性質と、粒子としての性質の両方を併せ持つ
  - 精密測定を行うと，量子としての性質が現れる
    → 測定によって、状態が乱される
- この性質から
  - Eveが盗聴を行うと、Bobが受け取る信号に必ず変化がおきる
  - それを送信者と受信者が検出できる.



「量子」に乱数ビットをのせる

- 通常用いる量子は「光」
  - 光は粒子である （これを「光子」(photon)と呼ぶ）
  - 我々が通常見ているのは粒々の集まり（粒子の数 ～ エネルギー）
  - 量子暗号では，粒子ひとつずつに0，1のデータを乗せる

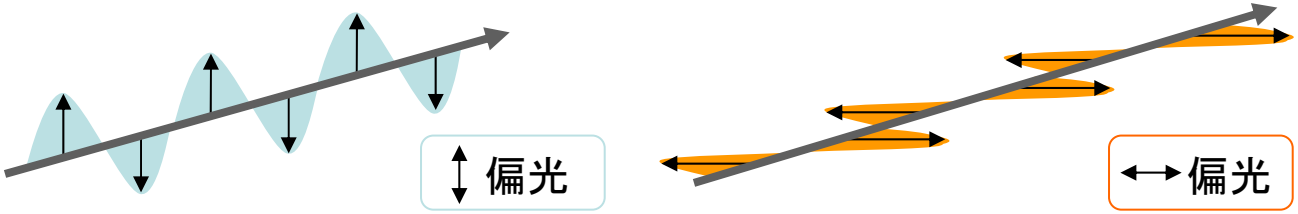


※ 1パルス辺り10^7個程度の光子

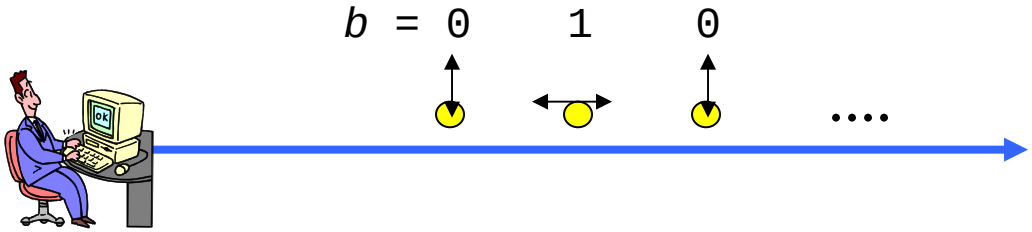
どうやって乱数ビットをのせるか？

符号化の方法： 偏光変調

- 光は波であり，振動の方向が複数ある



- この偏光を使って，光子ひとつずつに情報をのせる



- 同様に ⤢ 偏光，⤡ 偏光もある（装置を45度傾ける）

＋基底

×基底

ウォームアップ

通信路雑音がない場合の BB84プロトコル

量子暗号のデファクト方式は、BB84方式 (Bennett-Brassard 1984 protocol)である。

まずはその簡単版として、
通信路雑音がない場合をみてみる。

基底をランダムにふって光子を送る

	b=0	b=1
＋基底	↕	↔
×基底	↗	↘

受信者が正しい基底で観測してもエラーが起こる ⇒ 盗聴者検出

基底をランダムに選んで光子を送る
確率 { 50% ⇒ ×基底
50% ⇒ ＋基底

＋基底で b ＝ 0

送信者

盗聴者

受信者

＋基底で観測

確率＝p → ↔ を観測（b=1）

確率＝1-p → ↕ を観測（b=0）

×基底で観測

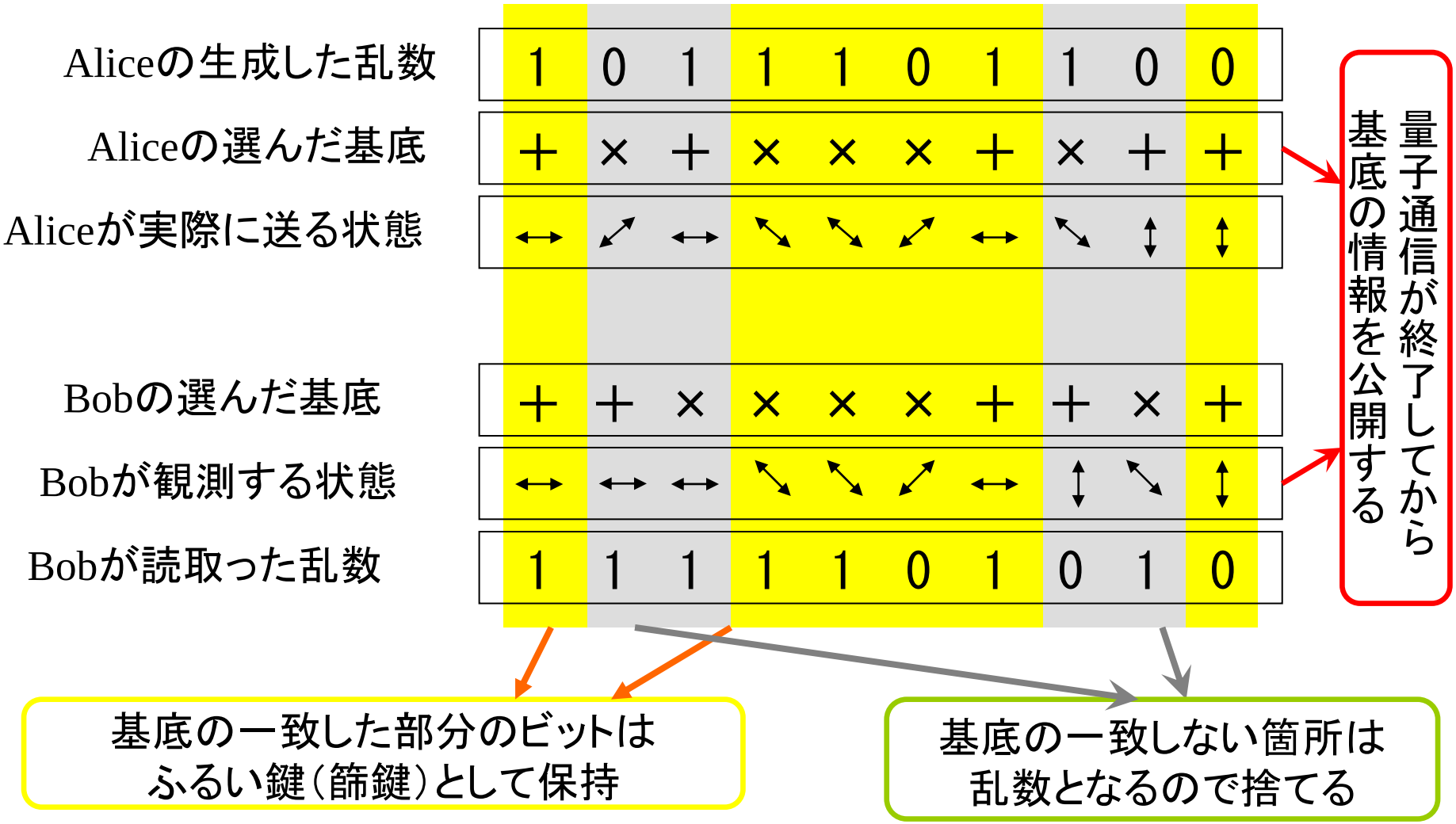
確率＝1/2 → ↗ を観測（b=0）

確率＝1/2 → ↘ を観測（b=1） エラー！

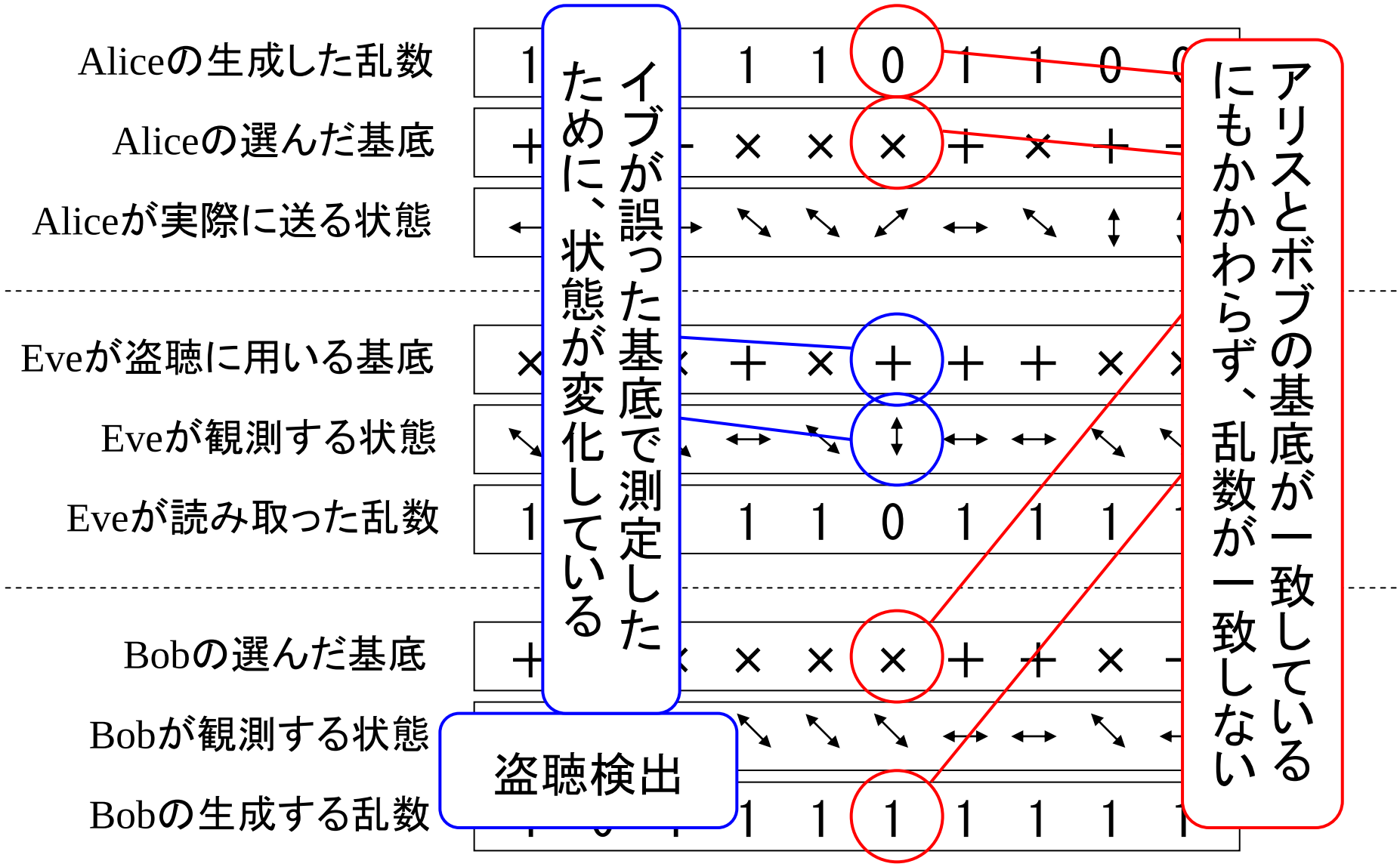
盗聴者Eveは基底を知らずに観測
⇒ 光子の偏光を変えてしまう

盗聴者がいない場合の処理の流れ

	b=0	b=1
＋基底	↕	↔
×基底	⤢	⤡



盗聴者Eveがいる場合　(intercept/resend attack)



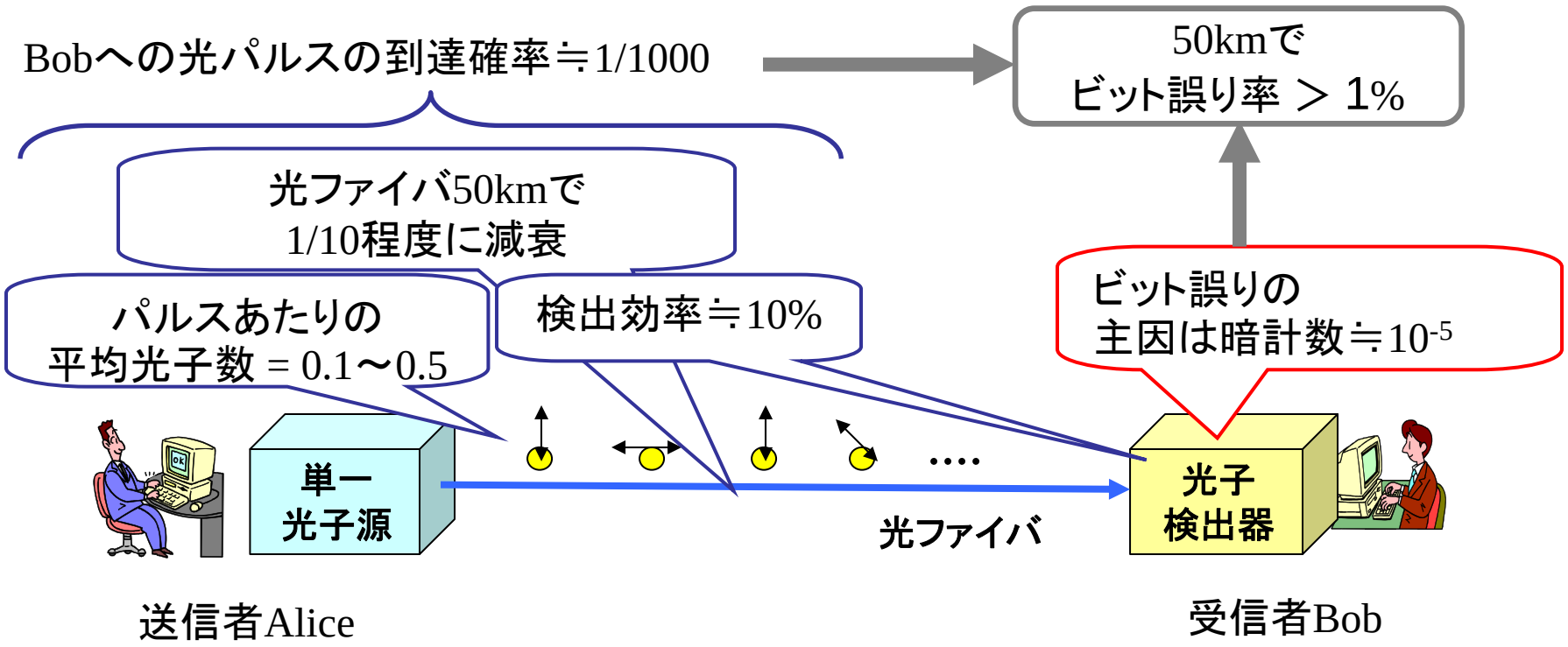
安全性証明

前ページまでの攻撃の話は，ある特定の例
(intercept/resend 攻撃)にたよった，直感的な説明にすぎない.
実際の量子暗号の安全性証明では，攻撃者Eveが，
量子力学によって許されたあらゆる攻撃を行うと想定する.

さらに現実の装置や通信路では、盗聴者がいなくとも雑音がある

現実の通信路にはノイズがある

量子暗号装置は、減衰や雑音の巣窟
敵がいないときでも通信路上でエラーが起こる



※暗計数(dark count) = 信号が来ていないのに、検出器が反応する事象

安全性証明で示したいこと

<u>このノイズを全て敵によるものであると想定する</u> (安全サイドに倒すことに相当)

このときビット誤り率 $e = 11\%$以下（※）であれば、
盗聴者Eveに情報が漏洩する確率を任意に小さくできる

Mayers1998; Shor-Preskill 2000;

※鍵生成レート $R = 1 - 2H_2(e) \geq 0$

量子誤り訂正符号を使った仮想的プロトコル

安全性証明の考え方

- まずは、証明のしやすいシンプルなプロトコルを考える
  - 実はこのプロトコルは盗聴者からすれば、現実のBB84プロトコルと等価
- このプロトコルの目的は、完全なBell状態をAliceとBobで共有すること

Bell状態とは？

- EPR状態，最大もつれあい状態などとも呼ばれる

$$|\Psi\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

- Alice, Bobの2者間で「共有できれば」、威力を発揮する。
  - Alice, Bobの純粋状態なので、盗聴者Eveと相関がない
  - Alice, Bobが個別に測定すると、同じ乱数が得られる

得られた乱数は、完全に秘密な暗号鍵となる

量子誤り訂正符号を使った仮想的プロトコル

しかしただ普通にBell状態をAliceからBobに送っても、盗聴や雑音により劣化する

→ 量子誤り訂正符号で修復する

Calderbank-Shor-Steane符号（CSS符号）

(Calderbank-Shor 1996; Steane 1996)

- 量子誤り訂正符号の一種
- 通常のビット誤りに加えて、位相誤り訂正も行う
- 概要:

1. 以下の性質をもつ線型な誤り訂正符号の組 C_1, C_2 を用意する:

   $C_2 \subset C_1$ をみたし、かつ $C_1, C_2^{\perp}$ が良い符号である

2. 以下の演算子を用いて、量子誤りのシンドロームを測定する:

   ビット誤り訂正:

   $$\Sigma_z^r := \sigma_z^{r_1} \otimes \cdots \otimes \sigma_z^{r_n},$$
   $$r = (r_1, \ldots, r_n) \in C_1^{\perp}$$

   位相誤り訂正:

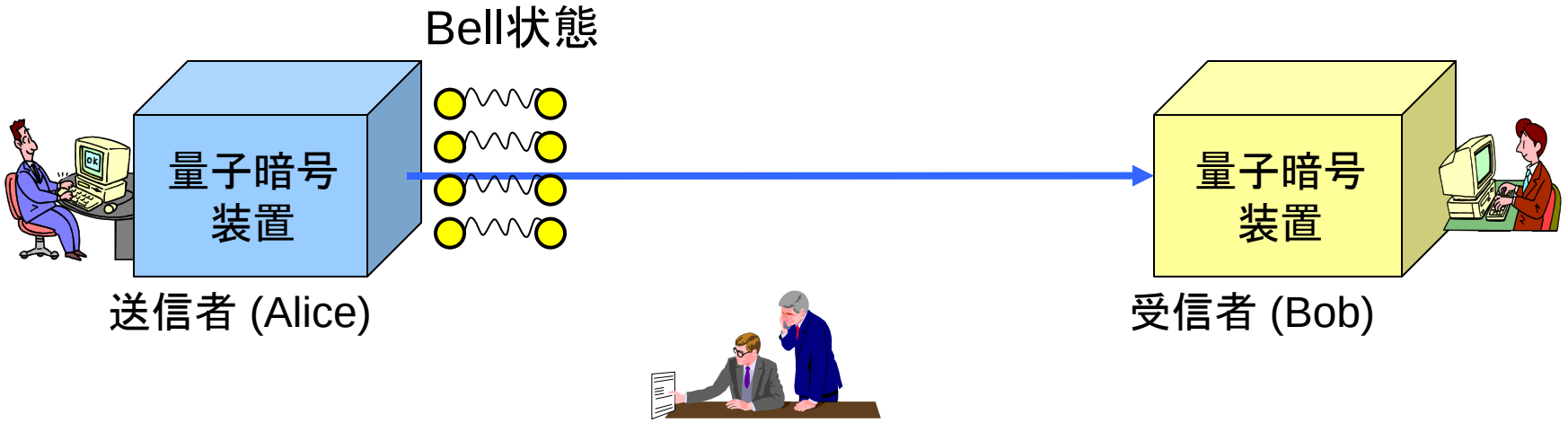
   $$\Sigma_x^s := \sigma_x^{s_1} \otimes \cdots \otimes \sigma_x^{s_n},$$
   $$s = (s_1, \ldots, s_n) \in C_2$$

   $\sigma_x, \sigma_z =$ パウリ行列

3. 測定したシンドロームを元に、ビット誤り、位相誤りパターンを推定し、誤り訂正を行う

量子誤り訂正符号を使った仮想的プロトコル

- Modified Lo-Chau protocol （in Shor-Preskill 2000）
  1. AliceはBell状態（もつれ合い状態）を複数準備する
  2. Aliceはその片割れに、Hadamard変換（＋，×基底の入れ換えに相当）をランダムに施してBobに送る
  3. Bobの受信後Aliceは、どのもつれ合い状態にHamadard変換を施したかを公開する
  4. Bobはそれらの状態に、逆Hadamard変換を施す
  5. AliceとBobは、ランダムサンプリングにより、通信路でのったビット誤り率を推定する
  6. CSS符号を用いて、ビット誤り、位相誤りの両方を訂正する
  7. AliceとBobは、同一の基底でEPR対を測定し、結果を秘密鍵として共有する



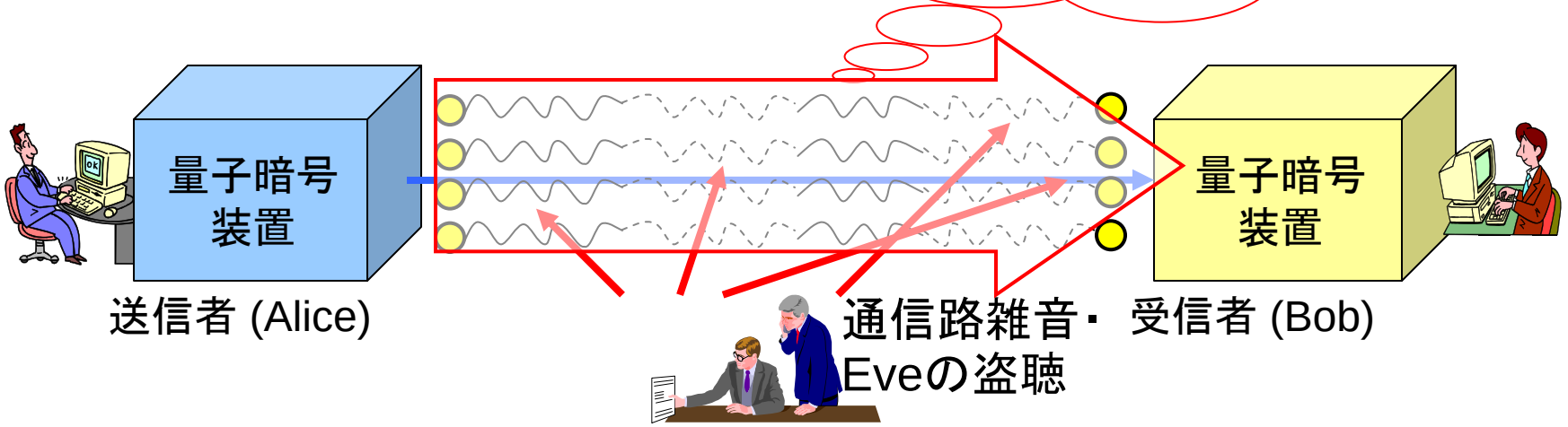
量子誤り訂正符号を使った仮想的プロトコル

- Modified Lo-Chau protocol （in Shor-Preskill 2000）
  1. AliceはBell状態（もつれ合い状態）を複数準備する
  2. Aliceはその片割れに、Hadamard変換（＋，×基底の入れ換えに相当）をランダムに施してBobに送る
  3. Bobの受信後Aliceは、どのもつれ合い状態にHamadard変換を施したかを公開する
  4. Bobはそれらの状態に、逆Hadamard変換を施す
  5. AliceとBobは、ランダムサンプリングにより、通信路でのったビット誤り率を推定する
  6. CSS符号を用いて、ビット誤り、位相誤りの両方を訂正する
  7. AliceとBobは、同一の基底でEPR対を測定し、結果を秘密鍵として共有する

量子誤り訂正符号を使った仮想的プロトコル

- Modified Lo-Chau protocol （in Shor-Preskill 2000）
  1. AliceはBell状態（もつれ合い状態）を複数準備する
  2. Aliceはその片割れに、Hadamard変換（＋，×基底の入れ換えに相当）をランダムに施してBobに送る
  3. Bobの受信後Aliceは、どのもつれ合い状態にHamadard変換を施したかを公開する
  4. Bobはそれらの状態に、逆Hadamard変換を施す
  5. AliceとBobは、ランダムサンプリングにより、
  6. CSS符号を用いて、ビット誤り、位相誤り
  7. AliceとBobは、同一の基底でEPR対を測

通信路雑音だけでなく、
Eveによる盗聴の効果
もろともQECCで訂正



量子誤り訂正符号を使った仮想的プロトコル

- Modified Lo-Chau protocol （in Shor-Preskill 2000）
  1. AliceはBell状態（もつれ合い状態）を複数準備する
  2. Aliceはその片割れに、Hadamard変換（＋，×基底の入れ換えに相当）をランダムに施してBobに送る
  3. Bobの受信後Aliceは、どのもつれ合い状態にHamadard変換を施したかを公開する
  4. Bobはそれらの状態に、逆Hadamard変換を施す
  5. AliceとBobは、ランダムサンプリングにより、通信路でのったビット誤り率を推定する
  6. CSS符号を用いて、ビット誤り、位相誤りの両方を訂正する
  7. AliceとBob　底でEPR対を測定し、結果を　共有する

量子誤り訂正符号を使った仮想的プロトコル

量子暗号の鍵生成レート ＝ CSS符号の符号化率であり、
古典符号 $C_1, C_2^{\perp}$ の性能できまる

ρ_{AB}　Alice, Bobそれぞれ n キュービットずつ

盗聴や通信路ノイズで傷ついたもつれあい状態
（ビット誤り率 = 位相誤り率 = e とする）

ビット誤り訂正

古典符号 C_1 のシンドロームビットと同じ数のキュービットを消費 （ $f_b n H_2(e)$ とおく）

ρ_{AB}^{rec}　$n\left(1 - f_b H_2(e)\right)$ キュービットずつ

位相誤り訂正

古典符号 $C_2^{\perp}$ のシンドロームビットと同じ数のキュービットを消費 （ $f_p n H_2(e)$ とおく）

（一般に $f_b, f_p \geq 1$, 理想的には $f_b = f_p = 1$ ）

ρ_{AB}^{ent}　$n\left(1 - f_b H_2(e) - f_p H_2(e)\right)$ 個のBell状態（＝秘密鍵ビット数）

現実のBB84プロトコル

議論の詳細は省くが、いままでの仮想プロトコルを盗聴者からみた場合、
現実のBB84プロトコルと区別がつかない （Shor-Preskill 2000）

BB84プロトコル （通信路雑音あり）

1. AliceはBobに、基底をランダムに選んで光を送る
2. Bobは基底をランダムに選んで光を測定し、結果を記録 （ふるい鍵）

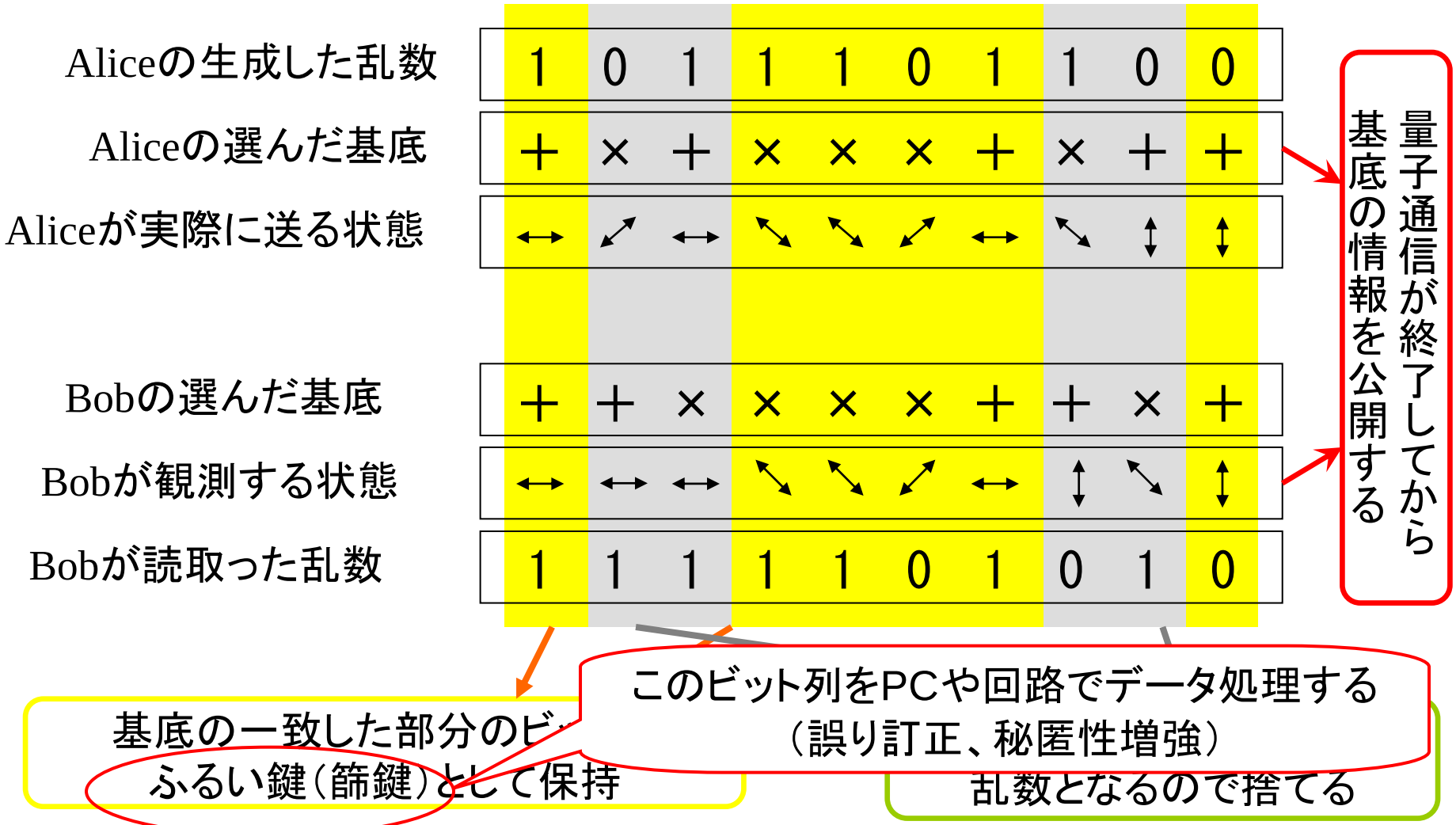
※ ここまでは通信路雑音なしの場合と同じ

3. サンプルビットをランダムに選び、位相誤り率を推定する。
   誤り率が高すぎたら(約11%以上)、プロトコルを中止する。
4. Alice, Bobは符号C_1を用いてビット誤り訂正を行う （訂正鍵）
5. Alice, Bobは符号C_2による同値類C_1/C_2をとる （秘密鍵）

再掲

ふるい鍵生成までの流れ

	b=0	b=1
＋基底	↕	↔
×基底	⤢	⤡



現実のBB84プロトコル

鍵蒸留処理： ふるい鍵に対し、以下のデータ処理をPCやFPGA上で行う

100110100101

ふるい鍵 ： 検出器から出てきたままのビット列，
n ビット
(e = ビット誤り率)

①誤り訂正符号 C_1によるビット誤り訂正

100101011

訂正鍵： 一部の情報がまだ盗聴者に漏洩している，
$n\left(1-f_pH_2\left(e\right)\right)$ ビット

② 得られた符号語 $x\in C_1$に対し、符号C_2で同値類をとる

この操作を「**秘匿性増強**」(privacy amplification)とよぶ
（敵に漏れた情報量 $NH_2\left(e\right)$ ビット分を除去していると解釈）

1001010

秘密鍵： 実際に暗号通信に使う鍵，最終鍵ともよぶ
同値類C_1/C_2の元， $n\left(1-f_bH_2\left(e\right)-f_pH_2\left(e\right)\right)$ ビット

量子暗号における古典CSS符号

- 以下、量子CSS符号の構成にもちいる線型符号の組C_1, C_2を、「古典CSS符号」と呼ぶことにする
- 量子CSS符号の要請から、C_1, C_2には以下の条件が必要
  - $C_2 \subset C_1$
  - C_1および$C_2^{\perp}$が良い符号である （符号化率が高い）
- ただし量子暗号に利用するときは、位相誤り訂正用の$C_2^{\perp}$にさらに「注釈」がいくつか加わる
  - 有利な注釈： ランダム符号が本当に使える
  - 不利な注釈： 符号のビット長が巨大でないとならない（有限長効果）

量子暗号における古典CSS符号

$C_2^{\perp}$に対する有利な注釈

- $C_2^{\perp}$ を用いた位相誤り訂正は実際には行わず、C_2の同値類をとるのみ。
- したがって効率的な復号アルゴリズムは不要。
  情報理論的に $C_2^{\perp}$ が復号可能でありさえすればよい。
- ゆえにランダム符号でもOK （符号C_1内に符号C_2を毎回ランダムにとる）
  このとき符号 $C_2^{\perp}$ のシンドローム長を、最小の値 $nH_2(e)$にできる。

（ $f_p = 1$に相当 ）

量子暗号における古典CSS符号

$C_2^{\perp}$に対する有利な注釈 (つづき)

- C_1で復号した情報ベクトルに、線型なuniversal hash functionをかければ安全 (Renner 2005)

Universal Hash Function

- 以下の条件を満たす関数の集合$F=\left\{f_r \middle| r\in I, f_r : A\to B\right\}$を ε -almost universal2 hash functionとよぶ

$$\forall x\neq y,\ \Pr\left[f_r(x)\neq f_r(y)\right]\leq \varepsilon\frac{|A|}{|B|}$$

- 1-almost …を単にuniversal hash functionと呼ぶ。例：Toeplitz行列演算。

- これをCSS符号の言葉でいうと:
  - C_2をC_1内に1-almost universal2符号族としてとることに相当
  - そのとき、その双対符号$C_2^{\perp}$の集合は、2-almost universal2符号族となる
  - ε -almost universal2符号族は、ランダム符号と類似の復号性能を持つ

ε -almost universal2符号族

- 符号 $C_1\subset \mathbf{F}_2^n$ に含まれる符号の集合 $\mathbf{C}_2=\left\{C_{2r}\subset C_1 \middle| r\in I, \dim C_{2r}\leq t\right\}$ が以下を満たすとき、$\mathbf{C}_2$ を(C_1の部分) ε -almost universal2符号族とよぶ

$$\forall x\in \mathbf{F}_2^n - C_1,\ \Pr\left[x\in C_{2r}\right]=2^{t-n}\varepsilon$$

- このとき, 写像$C_1\to C_1/C_2$は ε -almost universal2 hash functionとなる.

(M. Hayashi 2007; T.T. and M. Hayashi, in preparation)

量子暗号における古典CSS符号

$C_2^{\perp}$に対する不利な注釈

- 有限長効果 (M. Hayashi 2007)
  - 位相誤り訂正を実行しないので、復号失敗を直接検証できない
  - 位相誤り率e_pは、実はサンプルビットの誤り率p_{smp}から推定するもの
  - 推定の統計誤差を抑えるためには、$C_2^{\perp}$のビット長を大きく取る必要がある

数値例

サンプルビットはランダムな非復元抽出であり、超幾何分布に従う

$$P_k(c)=\binom{n}{k-c}\binom{l}{c}\Big/\binom{n+l}{k}$$

仮にC_1のブロック長n, サンプルビット数 l をともに1000とすると,
本来の誤り率e_p=5%に対し, 確率6%以上で推定誤差1%以上

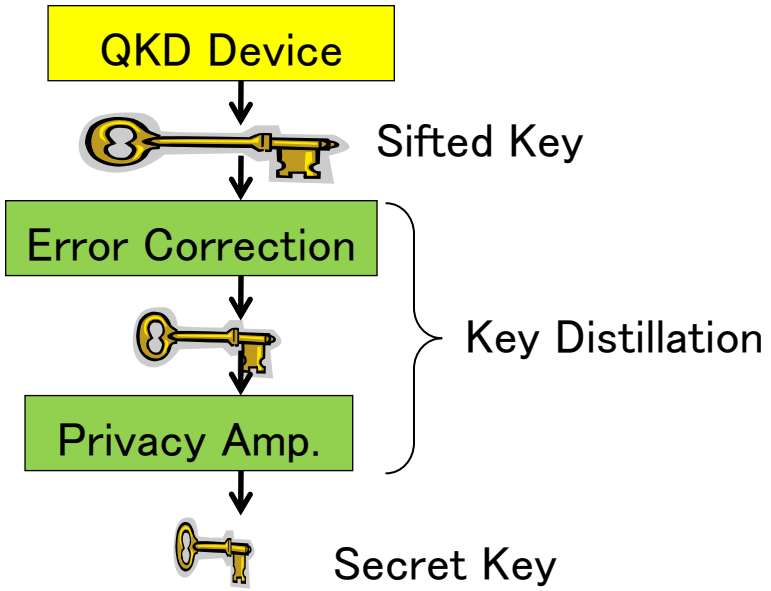
$$\Pr\left\lfloor p_{smp} \le 4\% \right\rfloor \ge 6\%$$

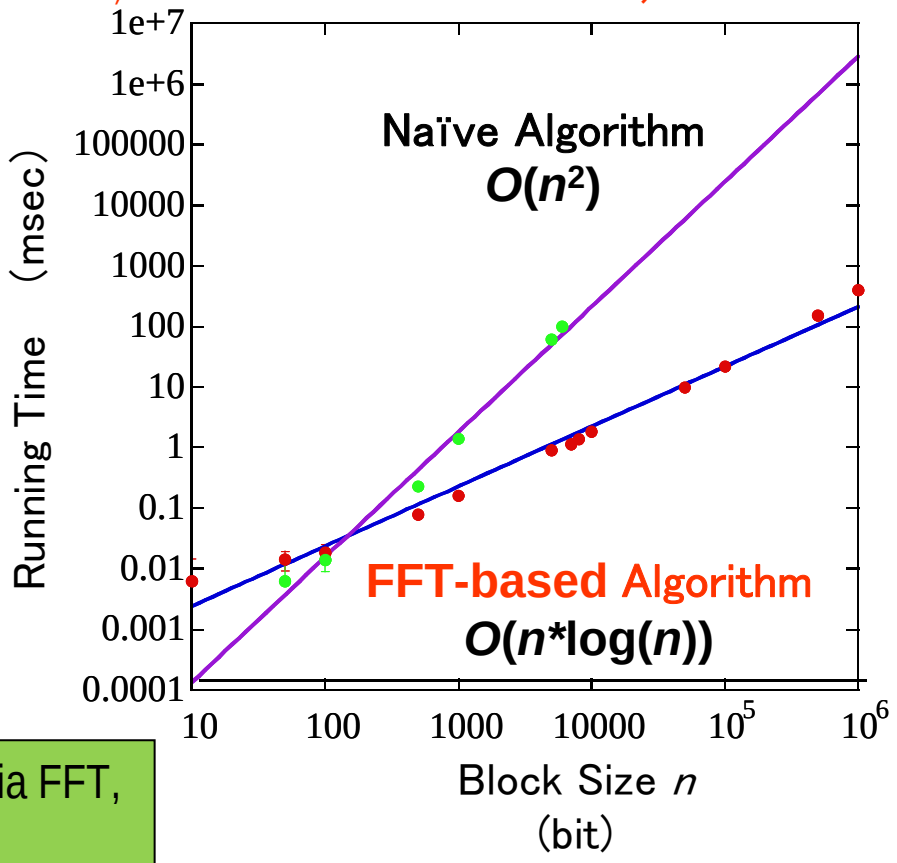
  - 鍵生成レートを無限大と遜色ないレベルにするためには、
    $C_2^{\perp}$のビット長 n を1Mbit以上にとる必要があるとされる
    (Scarani-Renner 2008)

高速秘匿性増強アルゴリズム
（FFTによるToeplitz行列演算）

As a solution to the finite size effect† of key distillation,
we developed a new efficient algorithm for privacy amplification

†Due to statistical fluctuations of phase error, block lengths of privacy amplification must exceed 10^6 (Hayashi 2007; Scarani and Renner 2008)





Running time of PA on software

Efficient multiplication algorithm of Toeplitz matrices via FFT, with an almost constant running time per bit
⇒ Privacy amplification on software for block size $n>10^6$

Tokyo QKD Network

- 国内外各社の量子暗号装置を接続し、東京都内の既設光ファイバ上に、量子暗号ネットワークを構築
  - 情報通信研究機構（NICT）の呼びかけにより、以下の機関が参加
    国内：　NEC、三菱電機、NTT、
    海外：　東芝欧州研（英）、id Quantique社（スイス）、
    All Vienna（オーストリア）
  - ４拠点：大手町、白山、本郷、小金井
  - 古典中継（※）により、総延長200km以上

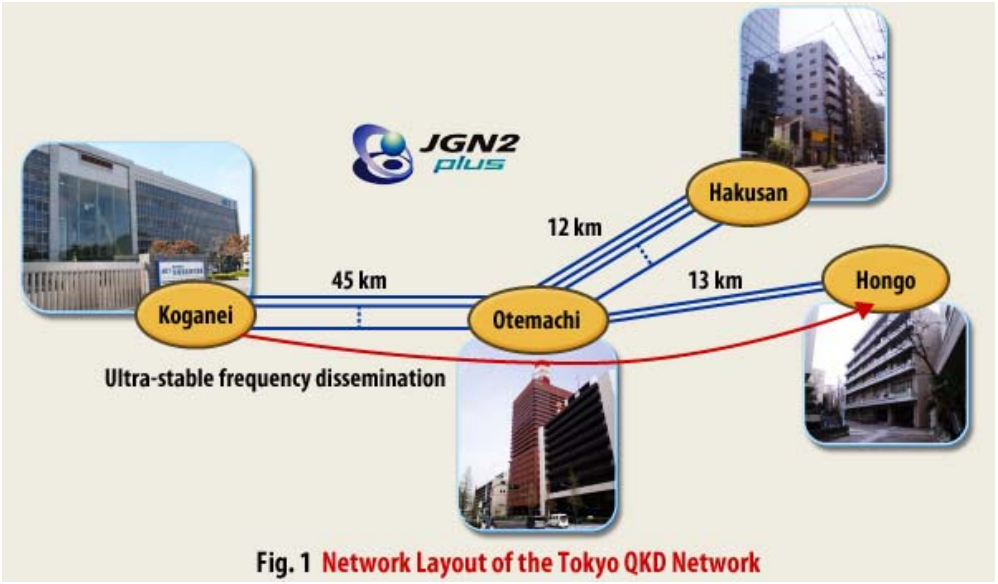


Fig. 1 Network Layout of the Tokyo QKD Network

参考：
UQCCホームページ
http://www.uqcc2010.org/

※各ノードは信頼できるとし
秘密鍵をリレーした

Tokyo QKD Network

- 量子暗号で共有した鍵で暗号化し、動画配信（テレビ会議）を実施
  - 記者発表（10月14日）、および国際会議UQCCでのデモ（18日）
- 通信速度：数kbps～300kbps（通信路により異なる）

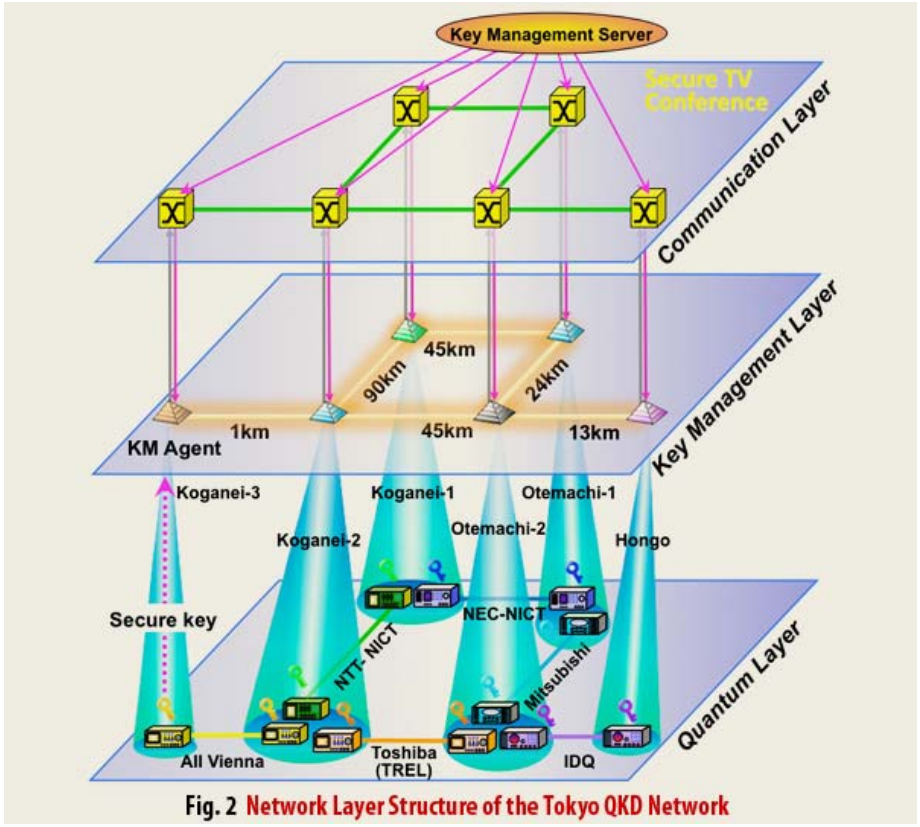


Fig. 2 Network Layer Structure of the Tokyo QKD Network

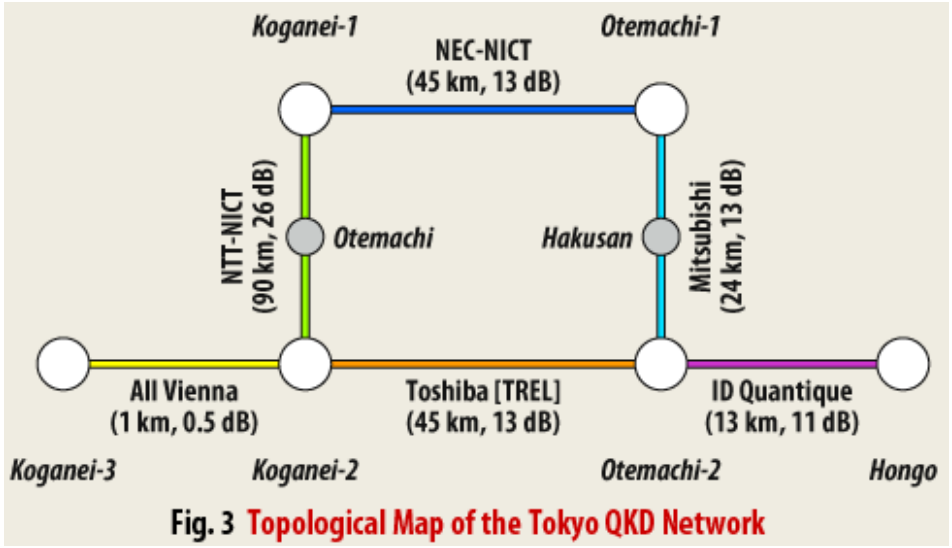
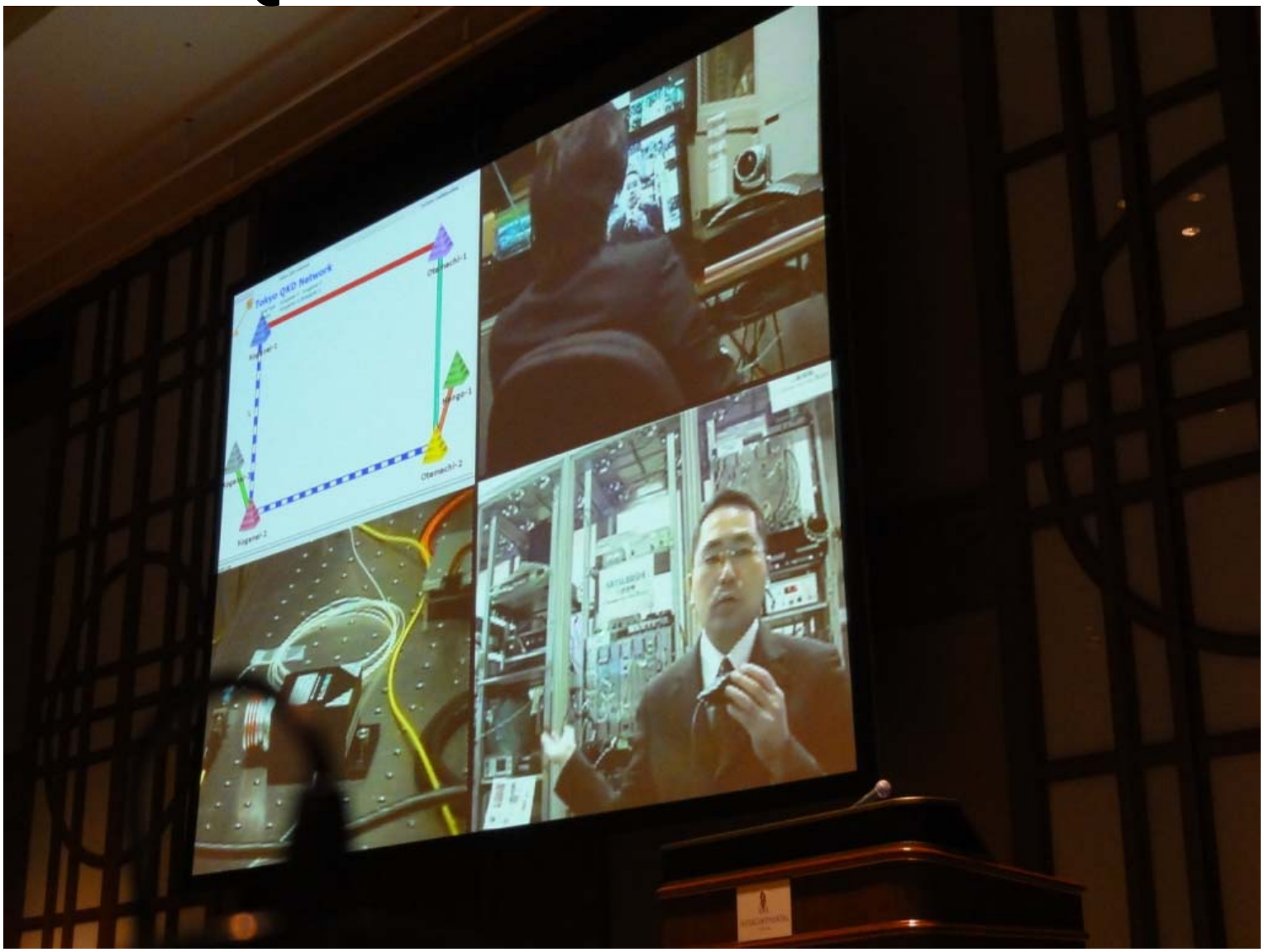


Fig. 3 Topological Map of the Tokyo QKD Network

UQCCホームページ
http://www.uqcc2010.org/ より

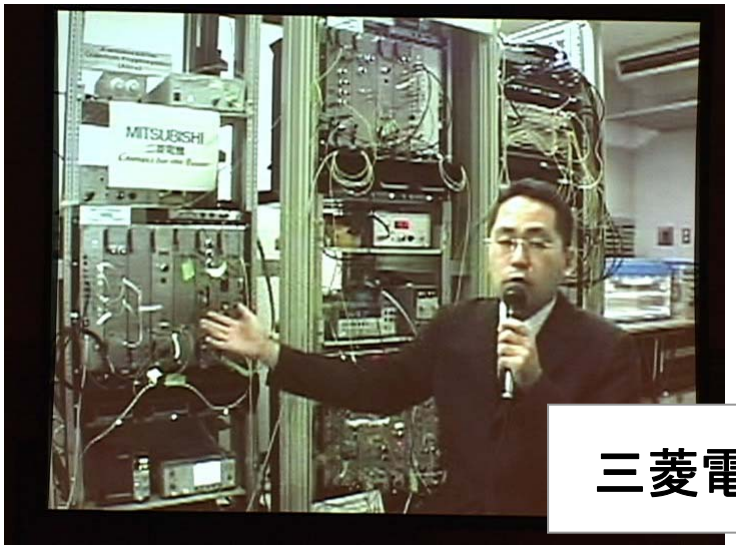
通信デモの様子
UQCC 2010 メイン会場

通信デモの様子
UQCC 2010 メイン会場



通信デモの様子
各社装置の状況を動画中継

NEC



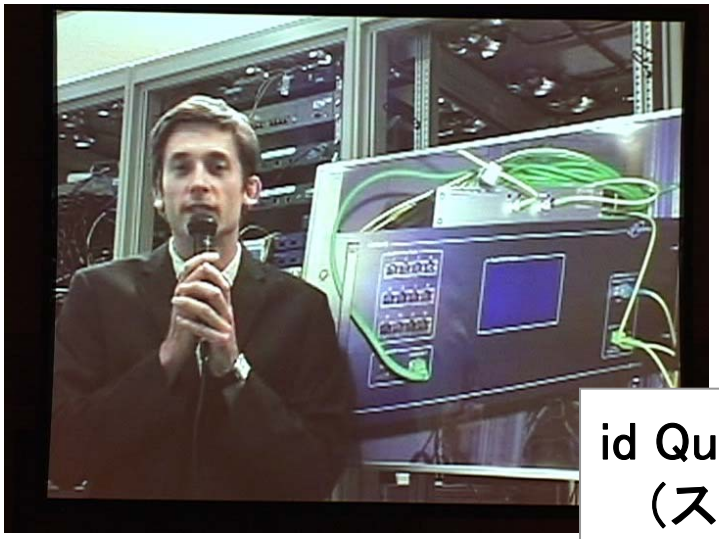
三菱電機

NTT

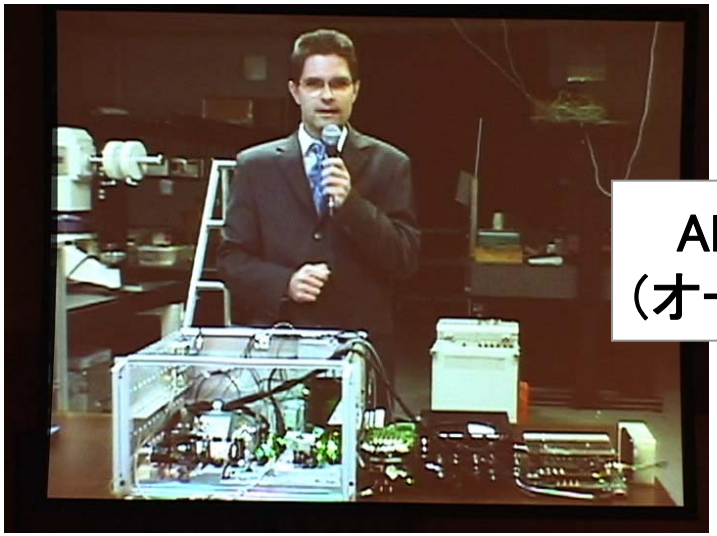
NICT
（超伝導検出器）

通信デモの様子
各社装置の状況を動画中継

東芝欧州研
（イギリス）



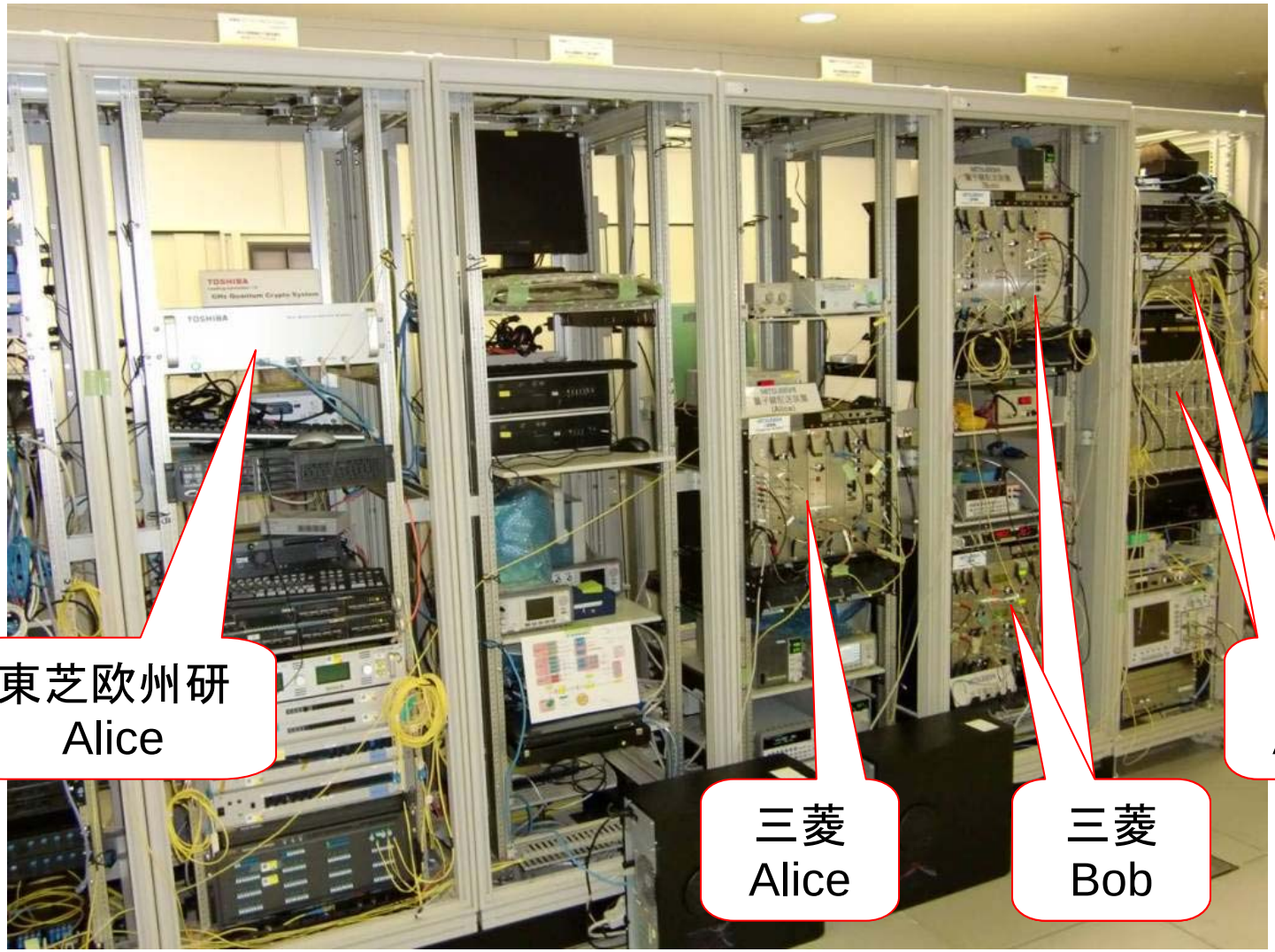
id Quantique
（スイス）



All Vienna
（オーストリア）

Tokyo QKD Network

実際の装置の様子（大手町）



まとめ

- 量子暗号は「絶対に破られない暗号」であり、なおかつすでに実用化レベルに達している
  - 量子暗号≠量子計算機
  - 海外ベンチャー企業による市販品、内外各社による試作品
  - Tokyo QKD Networkにおける接続デモ
- その安全性証明において、誤り訂正符号が重要である
  - 量子誤り符号（量子CSS符号）のコンポーネントとして、従来型の誤り訂正符号（古典CSS符号）がある（$C_2 \subset C_1$かつ$C_1, C_2^{\perp}$がよい符号）
  - 古典CSS符号の性能が量子暗号装置の性能を左右する
- 一方で、量子暗号装置において古典CSS符号を実際に使う必要はない
  - 量子暗号においては、$C_2^{\perp}$による位相誤り訂正を実行しないので、ランダム符号やユニバーサルハッシュ関数で置き換えられる
  - 結果として、通常のビット誤り訂正を行った後に、ユニバーサルハッシュ関数による秘匿性増強を行うことと等価になった