Field Test of Classical Symmetric Encryption with Continuous Variable Quantum Key Distribution

Paul Jouguet, Sébastien Kunz-Jacques, Thierry Debuisschert, Simon Fossier, Eleni Diamanti, Romain Alléaume, Rosa Tualle-Brouri, Philippe Grangier, Anthony Leverrier, Philippe Pache and Philippe Painchault

Optics Express, Vol. 20, Issue 13,
pp. 14030-14041 (2012)

平野研究室
09041044　羽田　昌也

量子鍵配送とは

- 現代暗号　→　計算量的安全性

  例)素因数分解

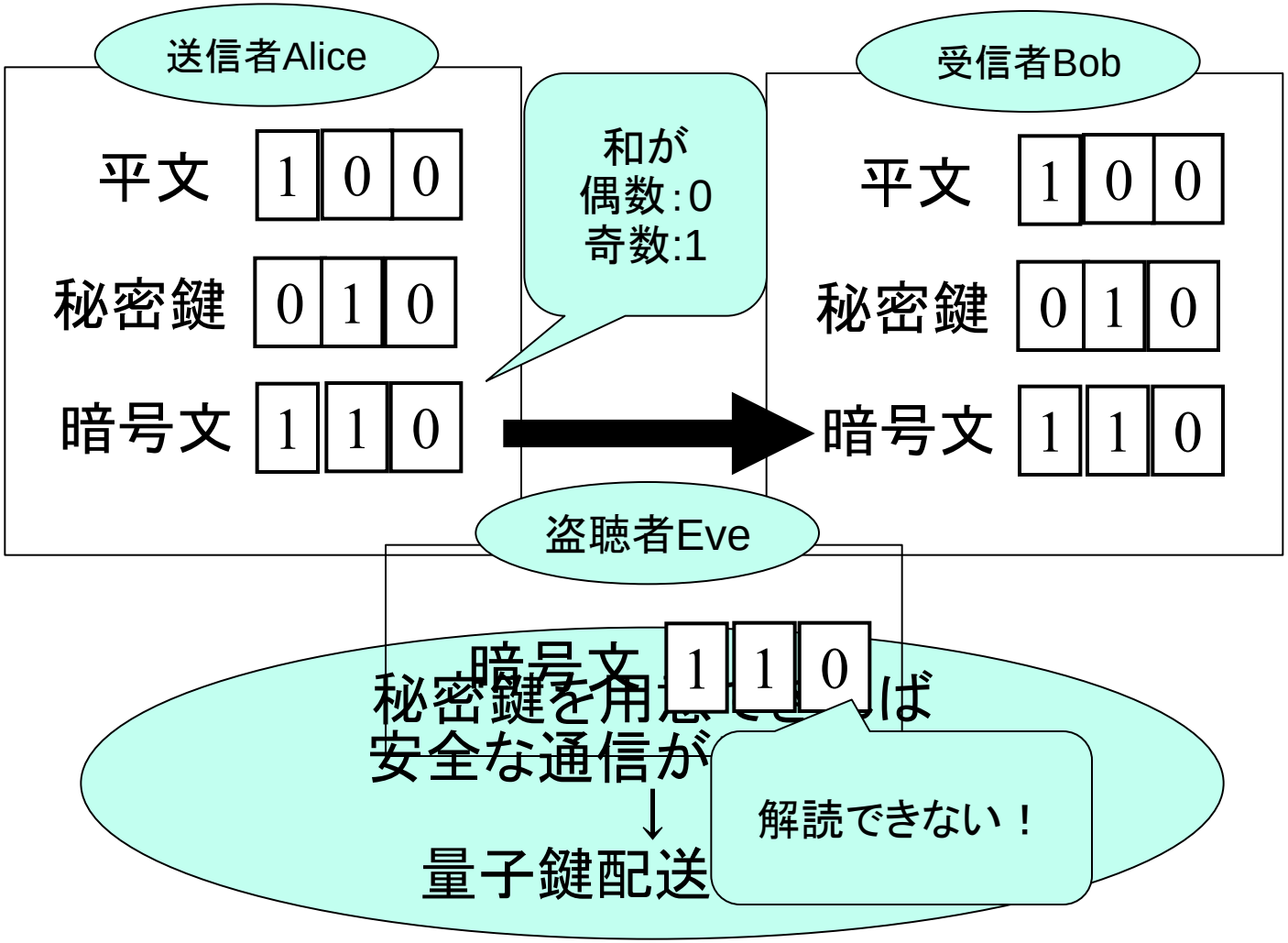
  67*97=6499

  6499=x*y

  計算機の高速化や効率的なアルゴリズムの
  開発により解読される可能性！

- 量子鍵配送(Quantum Key Distribution)
  - ✓ 共通鍵暗号に用いる秘密鍵の配送
  - ✓ 量子力学の性質を利用して秘密鍵の安全性を保証

QKDとは– 共通鍵暗号について



QKDの2種類の実現方法

離散変数QKD
Discrete-Variable QKD

- 単一光子検出器
  - ✓ 低温で動作→冷却が必要
- 単一光子状態を用いる

佐藤君・小栗君が説明

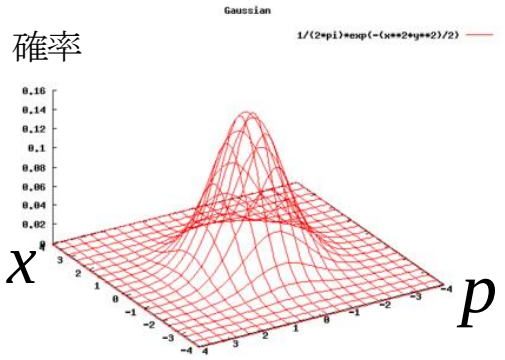
連続変数QKD
Continuous-Variable QKD

- ホモダイン検出器
  - ✓ 室温で動作
- コヒーレント状態を用いる
- 特殊なデバイスがいらない

今回使用

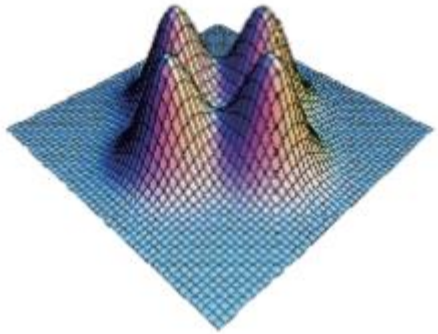
CVQKDの変調プロトコル

- ガウス変調プロトコル
  Aliceがコヒーレント光の
  直交位相振幅を複素平面上で
  ガウス分布するように変えて送信



今回はCVQKDの
ガウス変調プロトコル
を用いる

- 離散変調プロトコル
  Aliceが有限通り（例えば4通り）に
  位相を変えて送信



卒業研究はこちら

コヒーレント状態と直交位相振幅

生成演算子　$\hat{a}^\dagger$

消滅演算子　$\hat{a}$

$$\Rightarrow \quad \left[\hat{a}, \hat{a}^\dagger\right] = 1$$

消滅演算子 $\hat{a}$ の固有状態をコヒーレント状態と定義

$$\hat{a}\left|\alpha\right\rangle = \alpha\left|\alpha\right\rangle \qquad \alpha \in \mathbb{C}$$

直交位相振幅演算子 $\hat{x}$, $\hat{p}$ を次のように定義

$$\begin{cases} \hat{x} = \dfrac{\hat{a} + \hat{a}^\dagger}{2} \\ \hat{p} = \dfrac{\hat{a} - \hat{a}^\dagger}{2i} \end{cases}$$

コヒーレント状態なら

$$\Delta x = \Delta p = \frac{1}{2}$$

交換関係

$$\left[\hat{x}, \hat{p}\right] = \frac{i}{2}$$

不確定性関係

$$\Delta x \Delta p \geq \frac{1}{4}$$

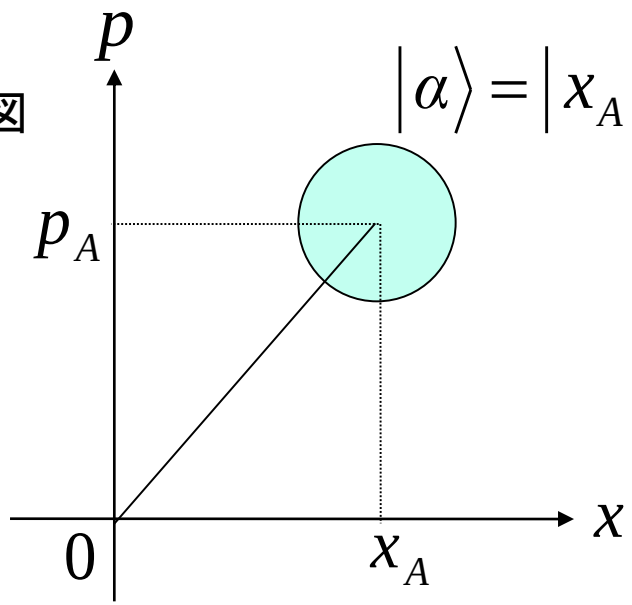
$$(\Delta x)^2 = \left\langle \hat{x}^2 \right\rangle - \left\langle \hat{x} \right\rangle^2$$

$$(\Delta p)^2 = \left\langle \hat{p}^2 \right\rangle - \left\langle \hat{p} \right\rangle^2$$

ガウス変調プロトコル−Alice

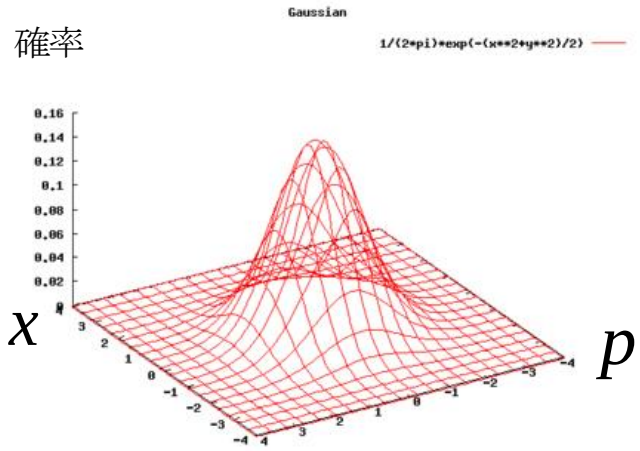
＜Aliceの送信状態＞

位相平面の図



$$|\alpha\rangle = |x_A + ip_A\rangle$$

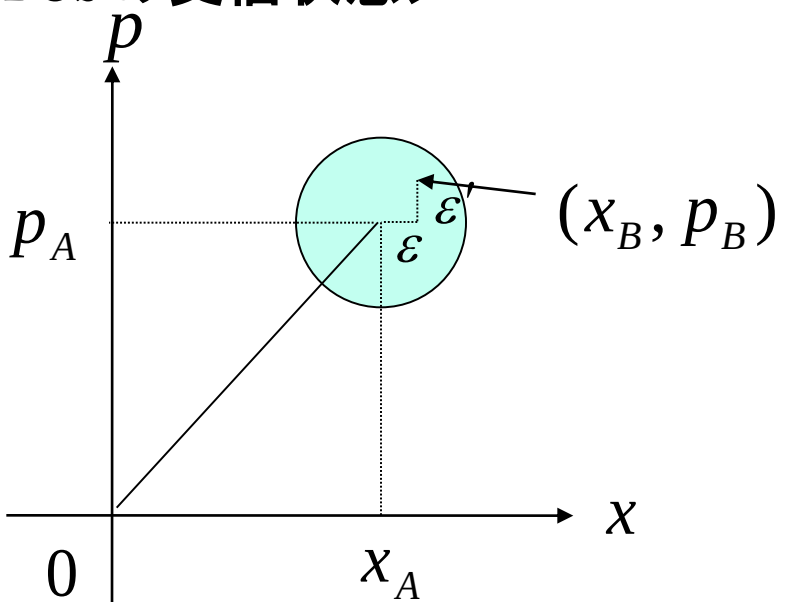
確率



- 直交位相振幅 x_A, p_A をそれぞれガウス分布から選択
- パルスレーザーの位相・振幅を変調
- コヒーレント状態|α >の光をBobへ送信

ガウス変調プロトコル–Bob

＜Bobの受信状態＞



＜送信状態＞

(x_A, p_A)

Bobの測定

x or p

基底確認

(x_A, x_B) or (p_A, p_B)

$$\begin{cases} x_B = x_A + \varepsilon \\ p_B = p_A + \varepsilon' \end{cases}$$

相関のある実数データを共有

↓

誤り訂正および秘匿性増強により秘密鍵を共有

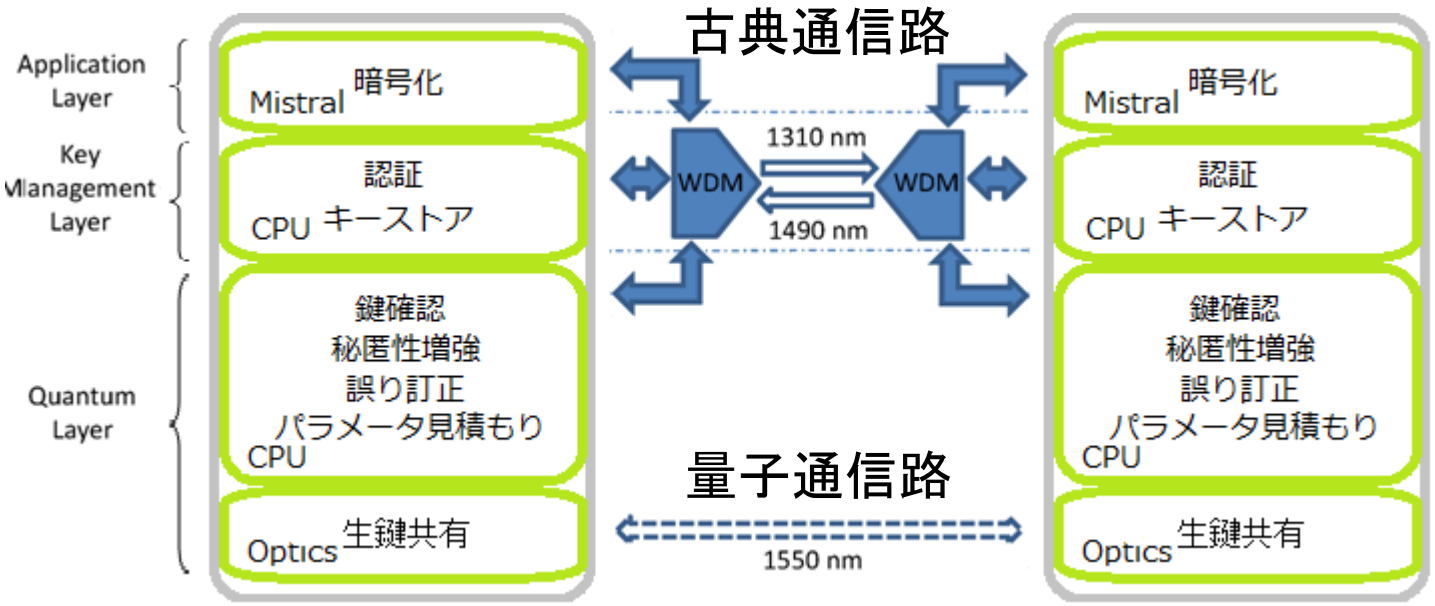
Project SEQURE
(Symmetric Encryption with QUantum key REnewal)

- SeQureNetによりフィールドテストが行われた
- 目的：QKDを用いて安全な通信システムの開発
- 期間：2010年7月末日から2011年2月の初めまでの6ヵ月間
- パレゾー・マシー（仏）間
- ファイバー長17.7km
- 透過率34.5%

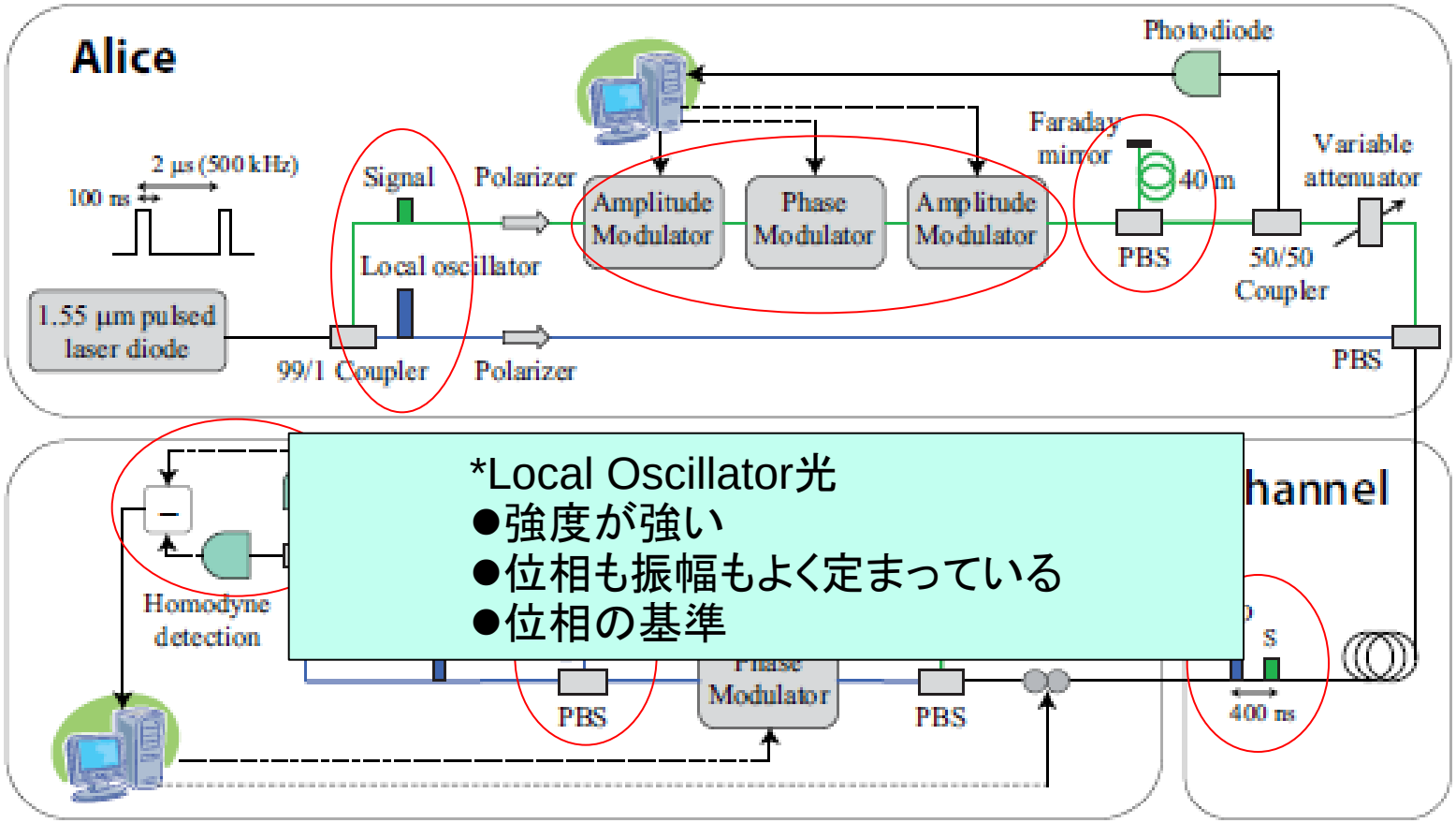
CVQKDで
最初の
長期間フィールド
テスト！

階層化構造 (Layered Architecture)

- 秘密鍵の生成・管理に階層化構造を用いる
- それぞれの階層ごとに別の処理を実施



実験装置



*Local Oscillator光
- 強度が強い
- 位相も振幅もよく定まっている
- 位相の基準

ホモダイン検出

入射光について

Signal光の消滅演算子 $\hat{a}$

LO光の消滅演算子 $\hat{b}$

出射光について

PD1側の消滅演算子 $\hat{a}_1$

PD2側の消滅演算子 $\hat{a}_2$

また$\hat{a}_1$, $\hat{a}_2$は次式を満たす

$$\hat{a}_1 = \frac{1}{\sqrt{2}}(-\hat{a} + i\hat{b})$$

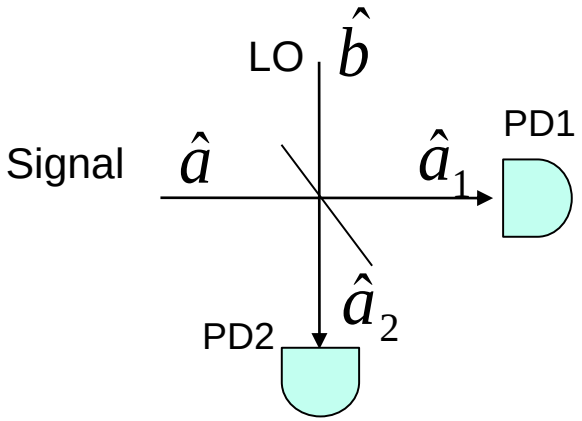
$$\hat{a}_2 = \frac{1}{\sqrt{2}}(\hat{a} + i\hat{b})$$

次にPD1とPD2に入射する

光子数演算子を$\hat{n}_1$, $\hat{n}_2$を考えると

$$\hat{n}_1 = \hat{a}_1^\dagger \hat{a}_1 = \frac{1}{2}\left(\hat{a}^\dagger\hat{a} + \hat{b}^\dagger\hat{b} - \hat{a}^\dagger\hat{b} - \hat{b}^\dagger\hat{a}\right)$$

$$\hat{n}_2 = \hat{a}_2^\dagger \hat{a}_2 = \frac{1}{2}\left(\hat{a}^\dagger\hat{a} + \hat{b}^\dagger\hat{b} + \hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right)$$



ホモダイン検出

ホモダイン検出は $\hat{n}_1$, $\hat{n}_2$ の差 $\hat{n}_{12}$ を見る

$$\hat{n}_{12} = \hat{n}_1 - \hat{n}_2 = i\left(\hat{a}^\dagger \hat{b} - \hat{b}^\dagger \hat{a}\right)$$

ここでLOは強度が強く安定なので $b \to |\beta| e^{i\theta}$ と置き換えて、

$$\begin{cases} \hat{a} = \hat{x} + i\hat{p} \\ \hat{a}^\dagger = \hat{x} - i\hat{p} \end{cases}$$

を代入して計算すれば

$$\hat{n}_{12} = 2|\beta|(\hat{x}\cos\theta + \hat{p}\sin\theta)$$

ただし $|\beta|^2$ はLO光の平均光子数、

θ はSignal光とLO光の相対位相

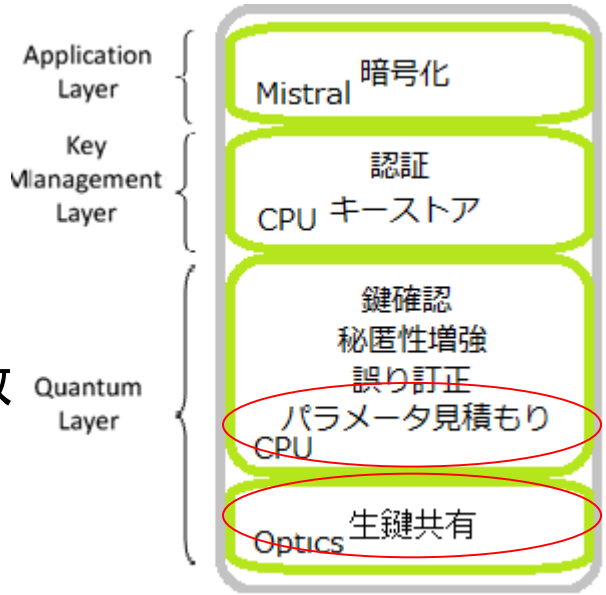
Quantum layer

- 生鍵共有ステップ
  QKDを行いAliceとBobで鍵を共有する
- パラメーター見積もりステップ
  過剰雑音ξ などのパラメーターを測定・見積もる

$$\xi = \frac{(\Delta x_{obs})^2}{(\Delta x)^2} - 1$$

$(\Delta x_{obs})^2$: 観測した分散

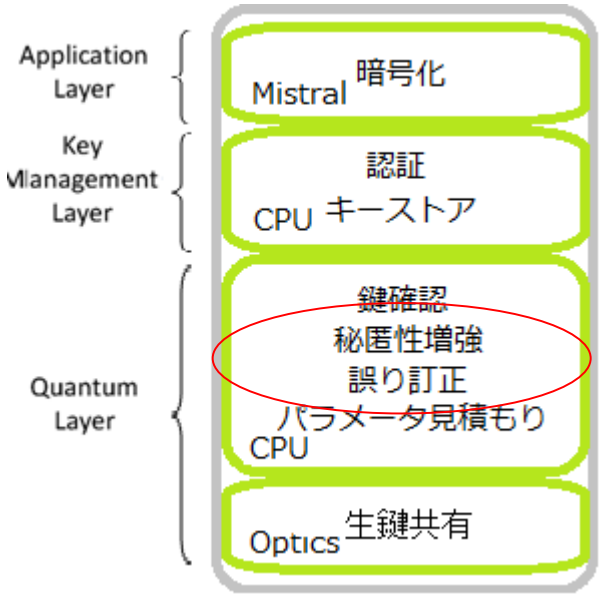
$(\Delta x)^2$: コヒーレント状態の分散



Quantum layer - 鍵蒸留

- 誤り訂正ステップ
  AliceとBobで誤りのないbitを共有
- 秘匿性増強ステップ
  Eveに漏れたであろうデータを破棄

- こうして得られた鍵を秘密鍵と呼ぶ
- 1秒あたりに得られる秘密鍵のbit数を秘密鍵生成率という



秘密鍵生成率とは

秘密鍵生成率の式

$r \propto I_{AB} - I_E$

I_{AB} ：AliceとBobが共有した情報の量

I_E ：Eveが盗聴によって得た情報の量

$I_{AB} > I_E$ の時に鍵を作ることができる

Eveの情報の量が増えると
鍵生成率が下がる

Eveの攻撃

Eveが得られる情報の量

盗聴者Eveが攻撃するとは・・

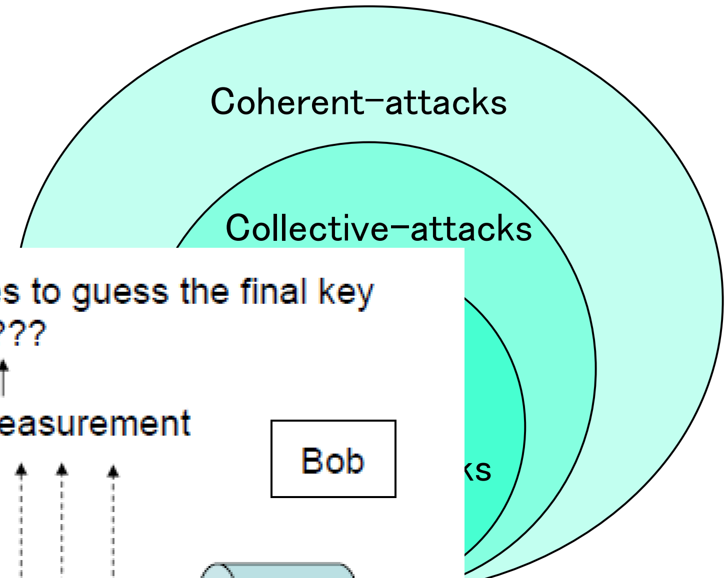
1.光パルスと自身の装置を相互作用

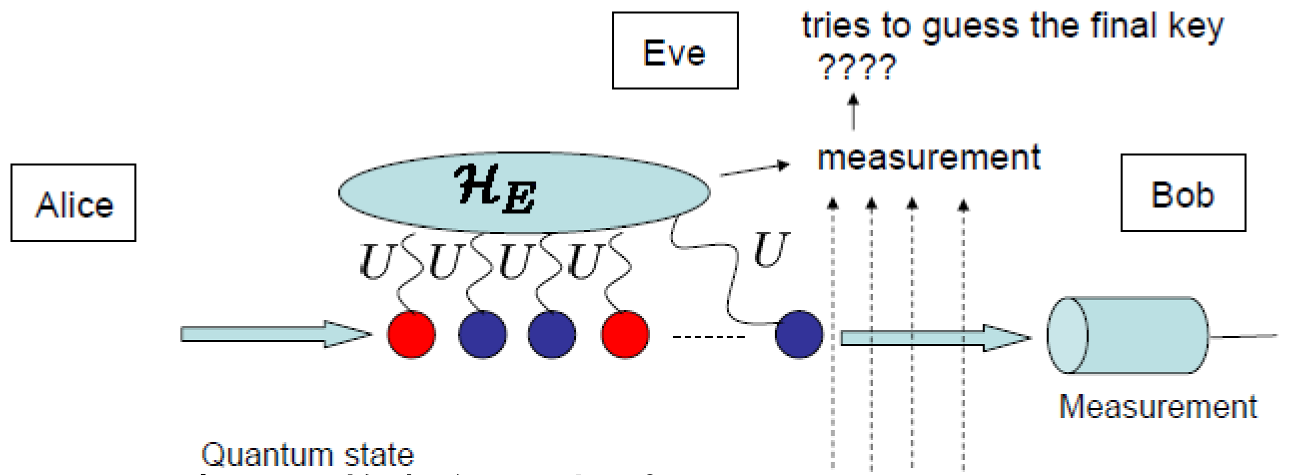
2.相互作用させた自身の系を測定

◆ Coherent-attacks
- ✓ 相互作用：一括
- ✓ 測定：　一括

◆ Collective-attacks
- ✓ 相互作用：個別

Eveの攻撃範囲の図





少ない

※一括とは複数個の光パルス

www.../QIMKEK1/Koashi.pdf

まとめて相互作用・測定することをいう

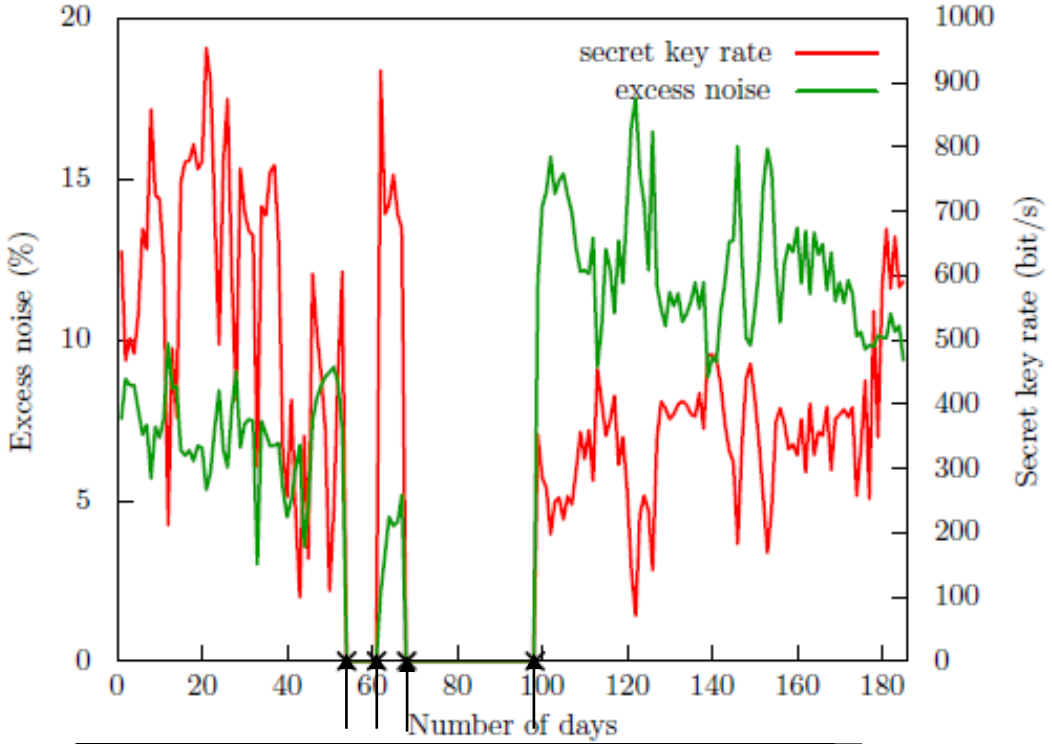
実験結果−秘密鍵生成率

100日以前

- Collective−attacksに対する鍵生成率 約600bit/s

100日以後

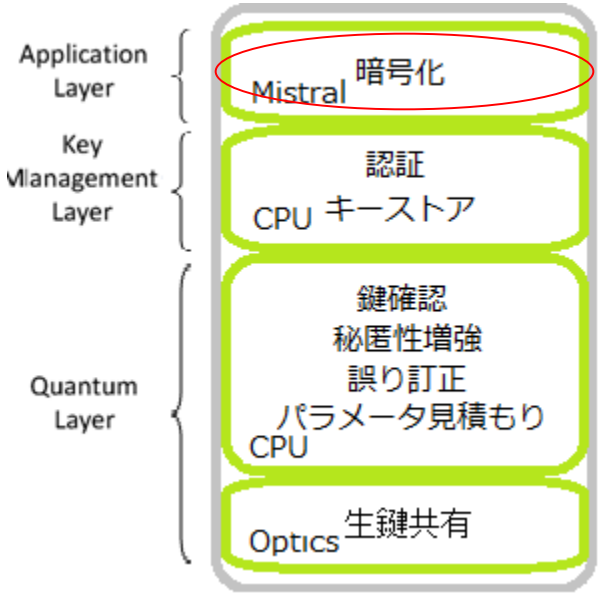
- Collective−attacksに対する鍵生成率 0bit/s
- Individual−attacksに対する鍵生成率 約400bit/s



Alice側PCのマザーボードの交換

Application layer

- 暗号化ステップ
  共有した鍵を用いて平文を暗号に変える
  Thales社の実製品(Mistral)を想定している



Application layer

- 1Gbit/s程度の速度で安全にデータを送りたい
- しかし
  最新のフィールドテストですら鍵生成率は1Mbit/s未満
- そこで現実的
  バー

データセンターのバックアップ等のため

*バーナム暗号

送信したいデータと同じ長さの秘密鍵

使った秘密鍵はその都度破棄

完全にランダムな秘密鍵を用いれば理論上安全

AES(Advanced Encryption Standard) 暗号

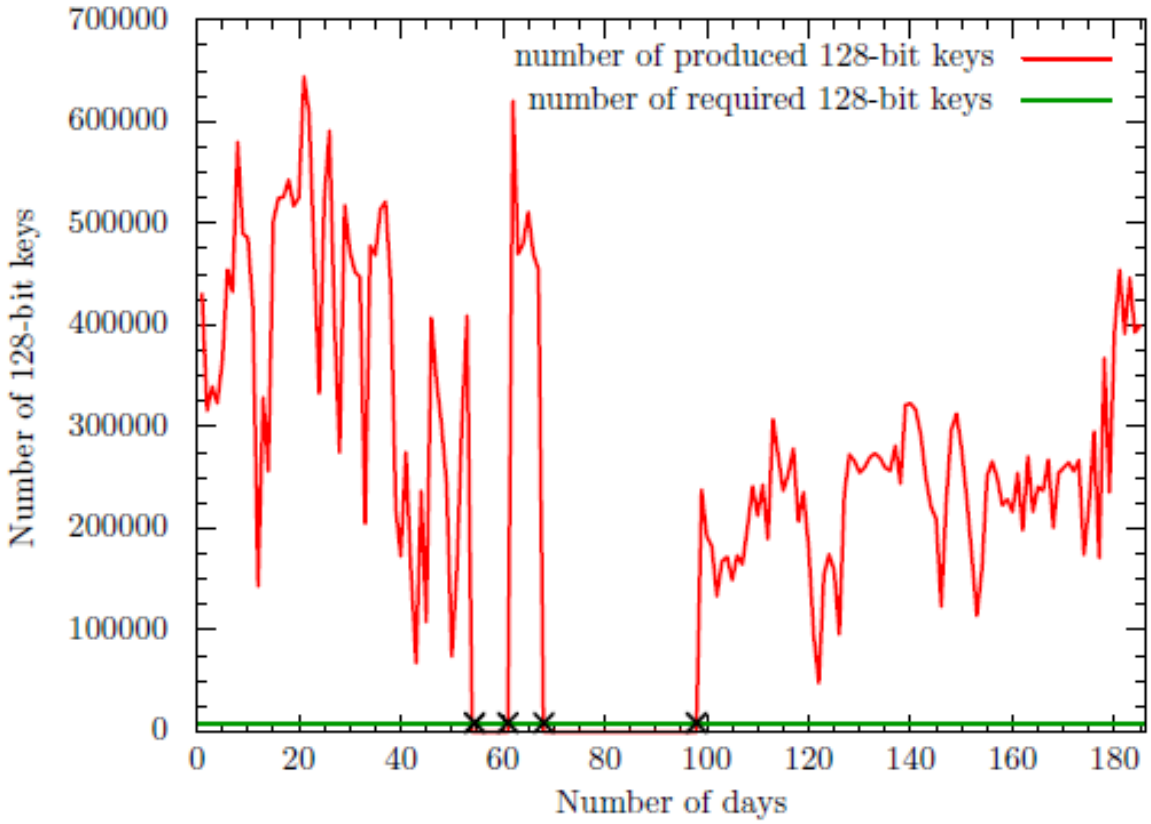
- 安全で速度の速い共通鍵暗号として
  2000年にNISTが選定
- ブロック暗号方式
- ✓ 平文を128bitのブロックに分ける
- ✓ 分けたブロックに対し秘密鍵を当てていく
- ✓ この操作を何度も繰り返す

計算量的安全性

対策:10秒ごとに秘密鍵を変えることにより安全性を高める

実験結果-1日あたりの128-bit key数

- 1日あたり8640個(10秒で1個)の128-bit keyが必要
- 実験中ほぼこの閾値は超えていたといえる



8640個の鍵

まとめ

- 2010年7月末日から2011年2月の初めまで6ヶ月間実験
- ファイバー長17.7km・透過率35.5%
- CVQKDのガウス変調プロトコルを用いた

その結果、以下のような結論が得られた

- 過剰雑音が多い場所では鍵生成率が小さくなる
- 100日以前はcollective-attacksに対し鍵生成率約600bit/s
- 100日以後はIndividual-attacksに対し鍵生成率約400bit/s
- 温度管理が出来ていない環境でも
  AES暗号に必要な鍵は十分作成できた

今後について

- 実装距離・速度共に向上を目指す

ご清聴有難うございました