3 August, 2018

量子暗号鍵配送
― 最近の研究開発状況

富田　章久

北海道大学大学院情報科学研究科

革新的研究開発推進プログラム ImPACT
Impulsing Paradigm Change through Disruptive Technologies Program

講演内容

1. はじめに
   - 量子暗号がなぜ必要か―超長期安全性
   - 量子暗号鍵配送（QKD)
   - QKDの始まり
2. QKDの今
   - 安全性
   - 実装
   - 装置開発の現況
3. QKDのこれから
   - 実装安全性
   - 大規模ネットワーク
4. おわりに

長期間秘匿性をどのように担保するか？

ゲノム情報（ヒトの寿命以上）

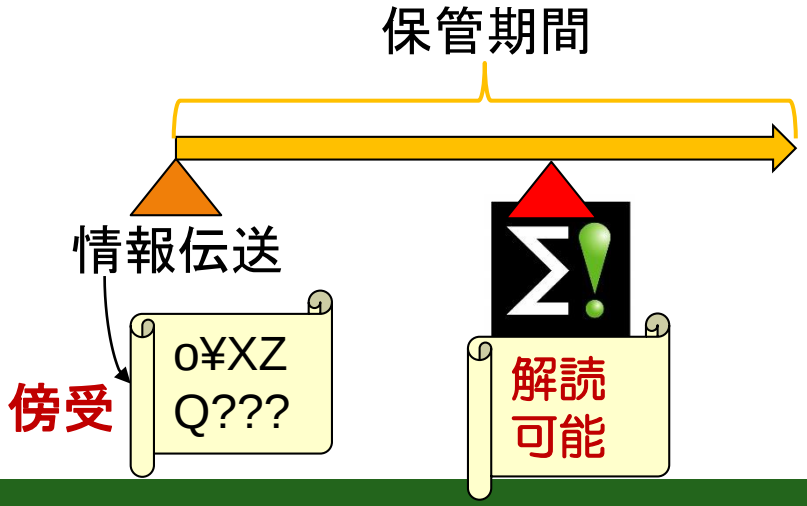
国家機密（特定機密 ≦ 60年）

(1) 現代暗号

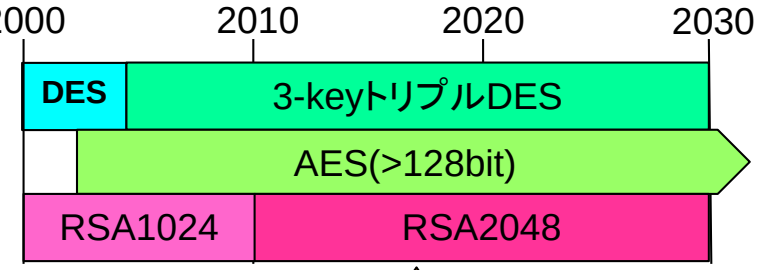
⇒ 計算量的安全

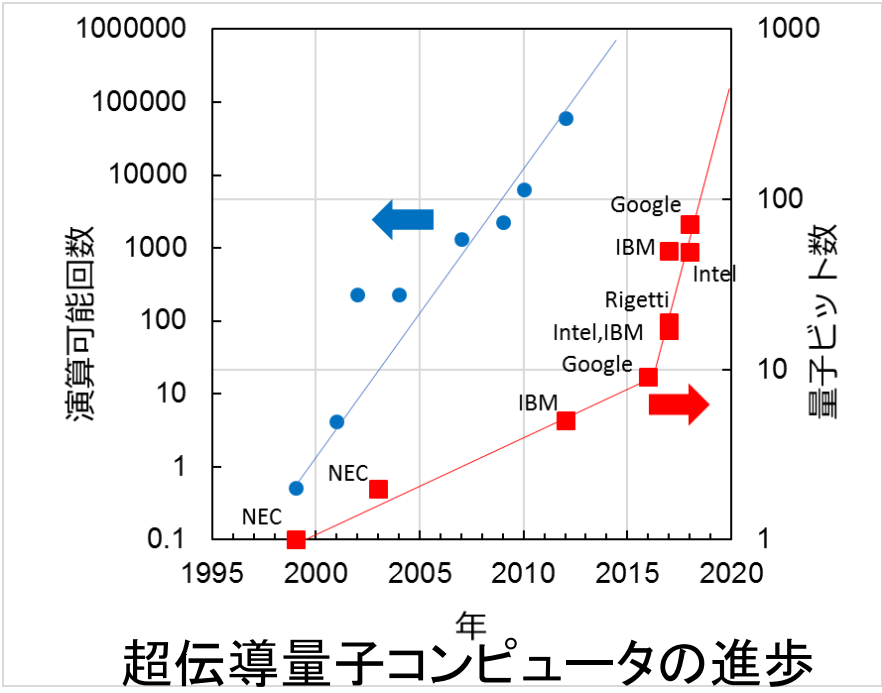
超長期間安全性の保証なし

– Store Now, Read Later



暗号の世代交代（米国標準技術研推奨）





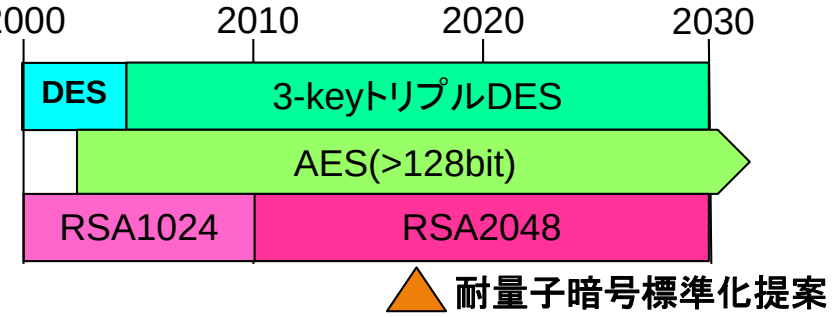
超伝導量子コンピュータの進歩

長期間秘匿性をどのように担保するか？

ゲノム情報（ヒトの寿命以上）

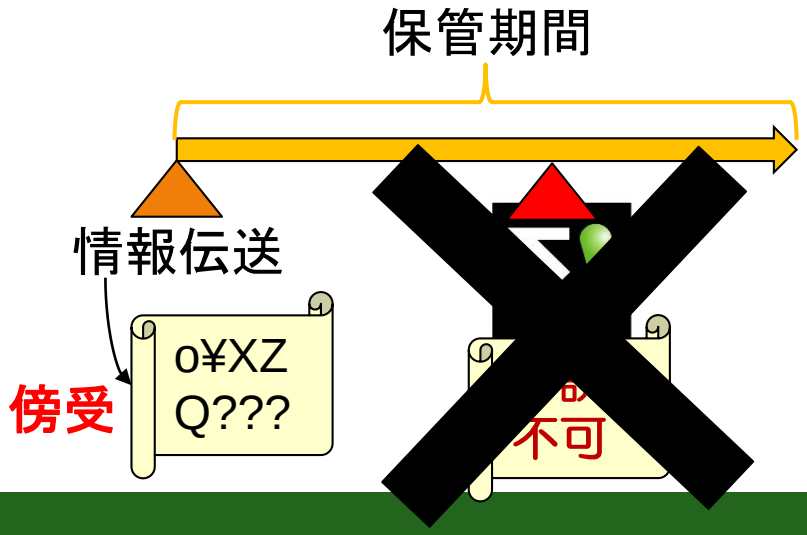
国家機密（特定機密 ≦ 60年）

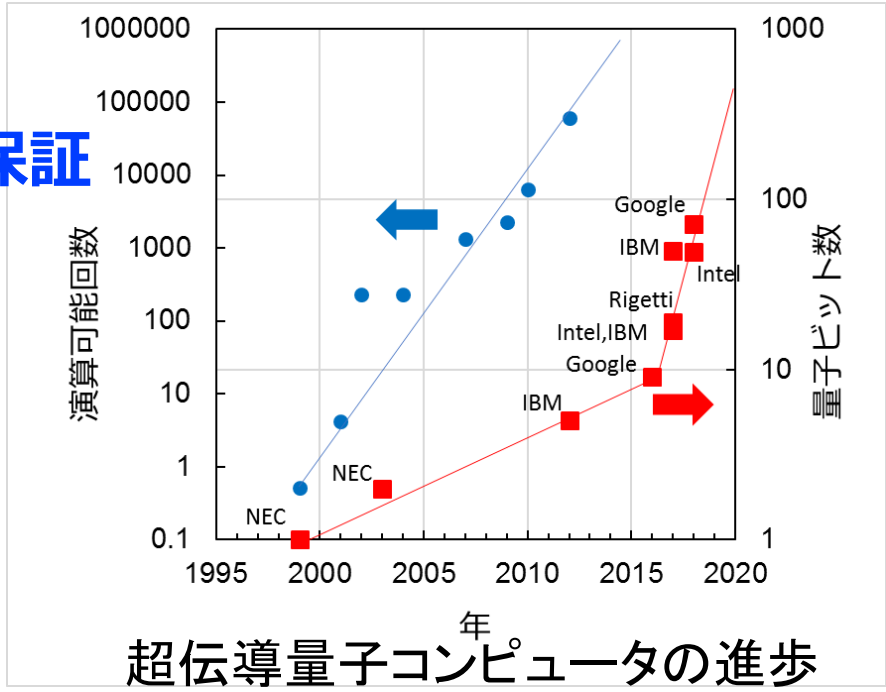
暗号の世代交代（米国標準技術研推奨）



(2) 情報理論的安全プロトコル

技術がいかに進歩しても安全性を保証

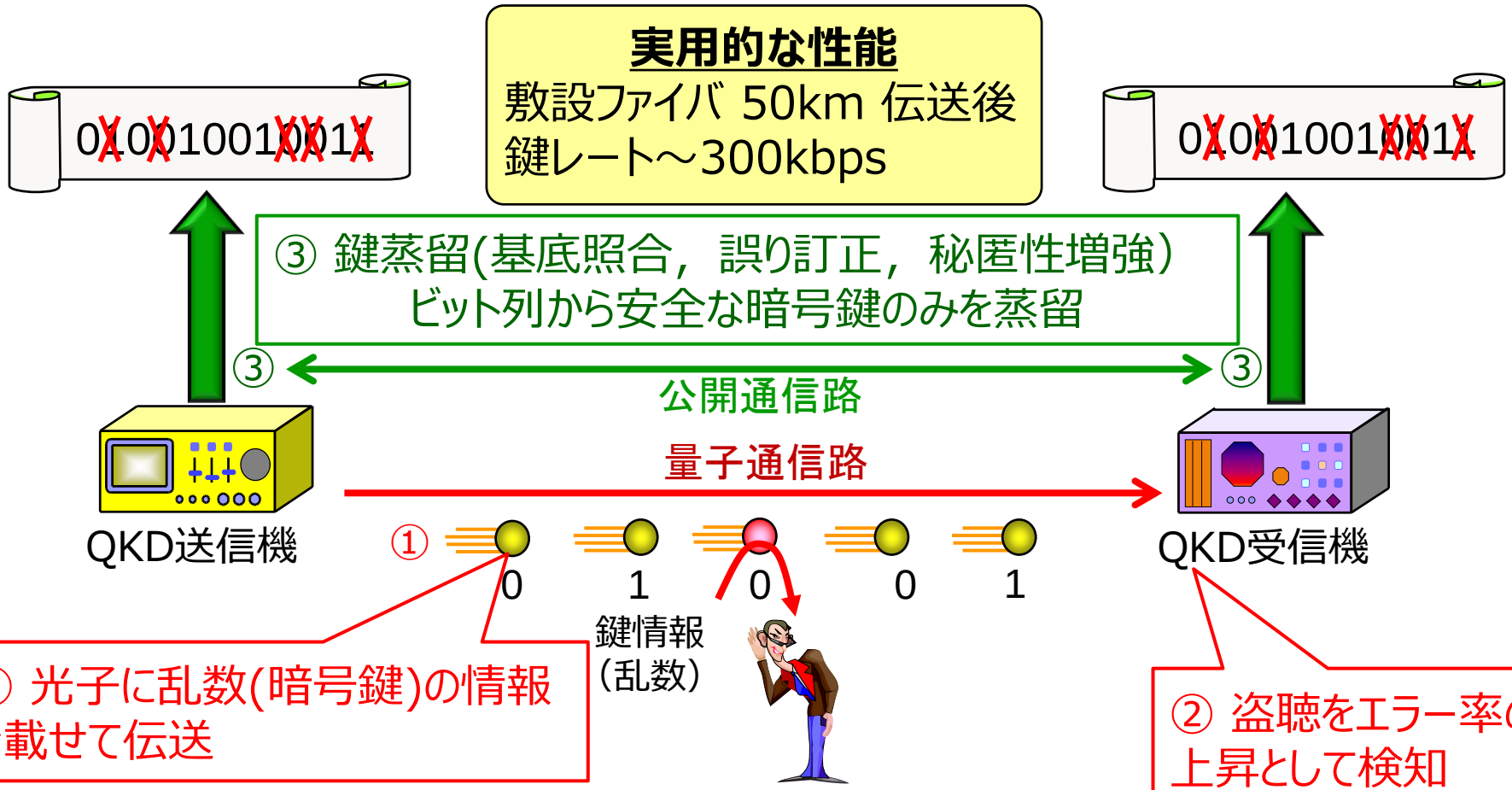




超伝導量子コンピュータの進歩

量子鍵配送：Quantum key distribution（QKD）

2地点間で情報理論的に安全な暗号鍵を共有



QKD 前史

1968　Wisner : Quantum Banknotes and Oblivious Transfer

- Conjugate Coding
- 70年ごろIEEE-ITに投稿. プレプリントは流布. 出版は1983年（SIGACT News)

QKDの始まり

1979 CharlieGillesに会う

1984 BB84 protocol(1)

- 量子メモリを使う

1992 初実験(2)

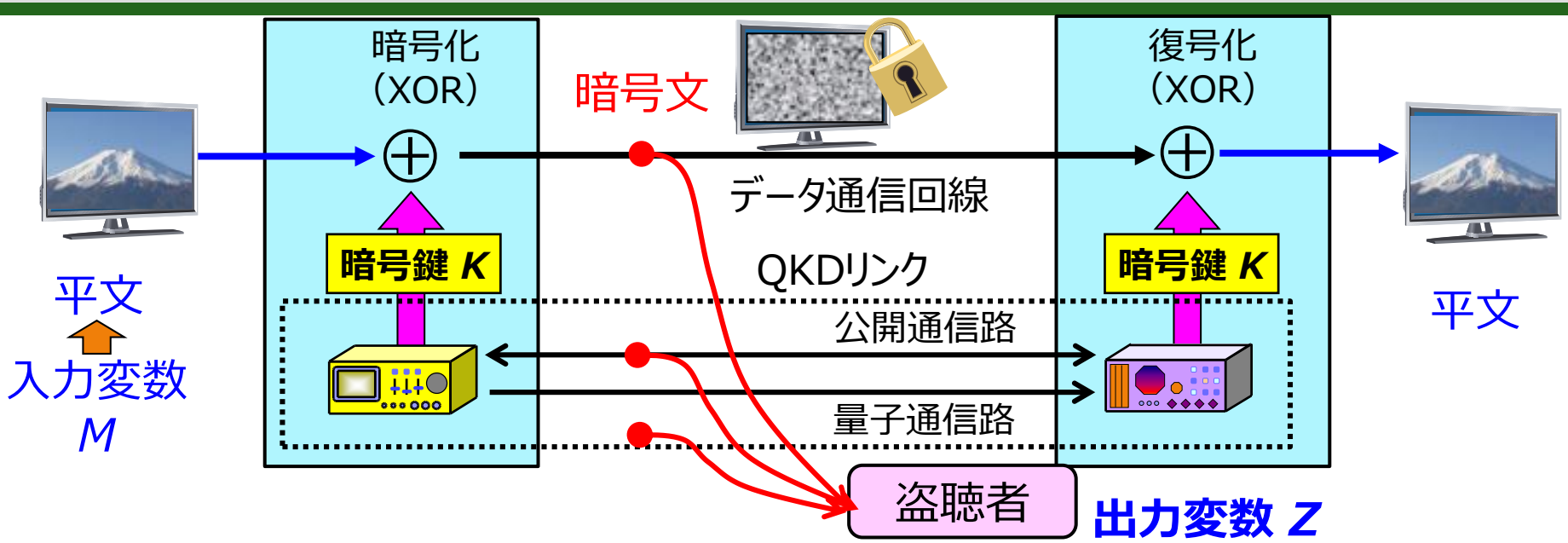
- 基底照合を導入

1998 無条件安全(3)

2000 Shore-Preskill

1. Bennett & Brassard, Proc. IEEE Int'l Conf. Comp., Sys., and Sig. Proc. (Bangalore, India, Dec. 1984).
2. Bennett,et al., J. Crypt., **5**, 3 (1992)
3. Mayers, J. ACM, **41**, 351 (2001)

情報理論的安全性（ε-安全性）



・暗号鍵Kと盗聴者の変数Zの統計的相関を任意の数ε以下に抑えることができる

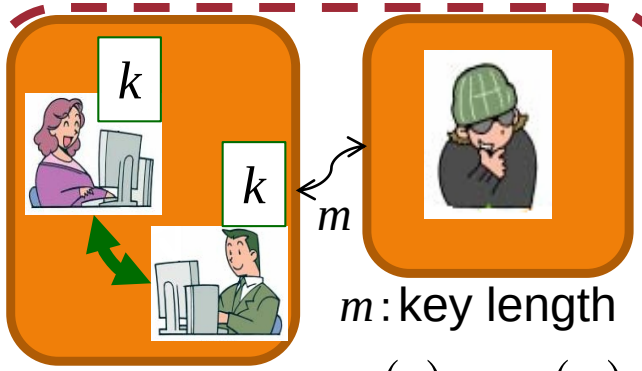
⇒情報漏洩の危険性を限りなくゼロにできる(**ε:セキュリティパラメータ⇒ ε -安全性)**

・通常、$\varepsilon = 10^{-11}$ ⇒ 情報漏洩の危険性は10^{11}回の鍵生成操作の中で1回以下

・数理暗号の汎用結合(UC)安全性に対応⇒公開鍵暗号では選択暗号文攻撃に対する強秘匿・頑健性(IND/NM-CCA2:Indistinguishable/Non-malleable-Chosen Cipher Attack2)

ε-安全性の定式化

Result of the ideal protocol



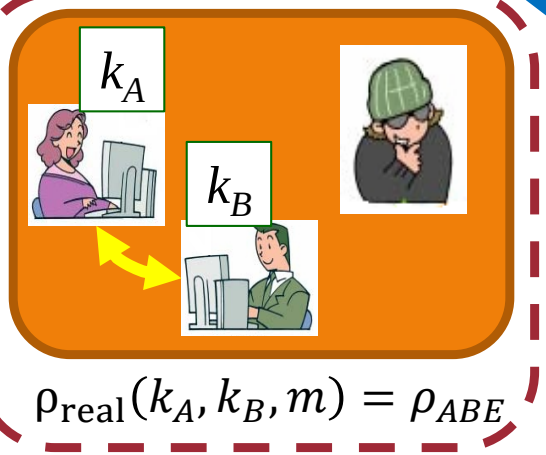
C_{ideal}

判別機械 → $G_M = \begin{cases} 1 : \textit{same} \\ 0 : \textit{different} \end{cases}$

(optimal measurement)

C_{real}

Result of a real protocol



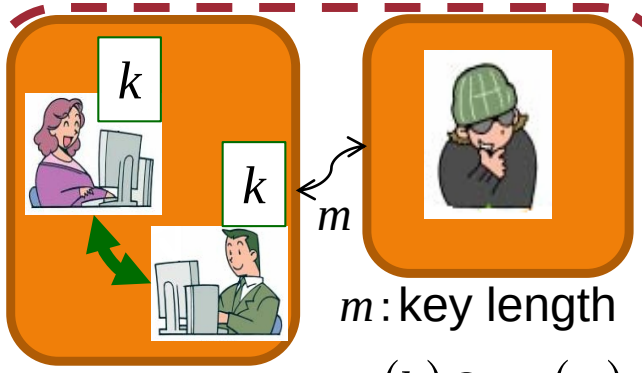
A protocol is ε-secure,
if $\forall \varepsilon > 0, \exists C_{\text{ideal}}$ s. t.

$$|P(G_M = 0|C_{\text{ideal}}) - P(G_M = 0|C_{\text{real}})| \leq \varepsilon$$

$$\frac{1}{2}\|\rho_{\text{ideal}} - \rho_{ABE}\| \leq \varepsilon$$

ε-安全性の定式化

Result of the ideal protocol



C_{ideal}

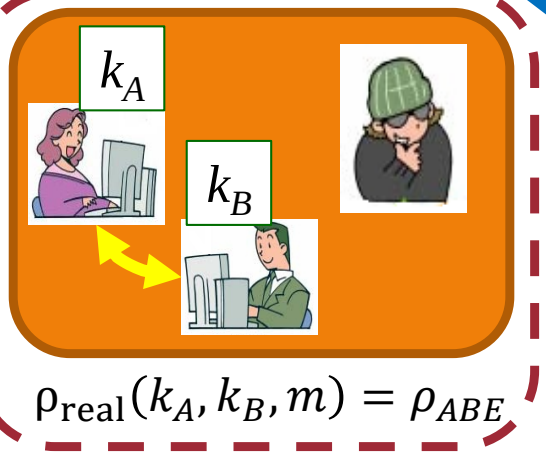
判別機械

$$G_M = \begin{cases} 1 : \textit{same} \\ 0 : \textit{different} \end{cases}$$

(optimal measurement)

C_{real}

Result of a real protocol



$$\frac{1}{2}\|\rho_{\text{ideal}} - \rho_{ABE}\| \leq \varepsilon$$

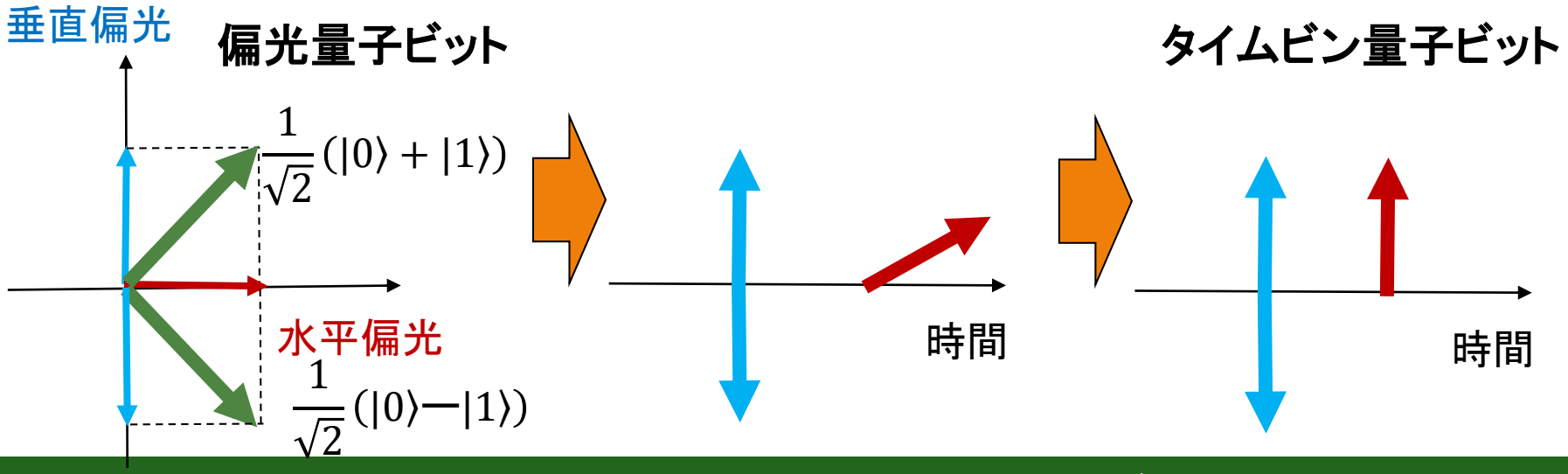
Alice－Bobの状態を**pure state**にしたい

量子誤り訂正（ビット誤り・位相誤り）

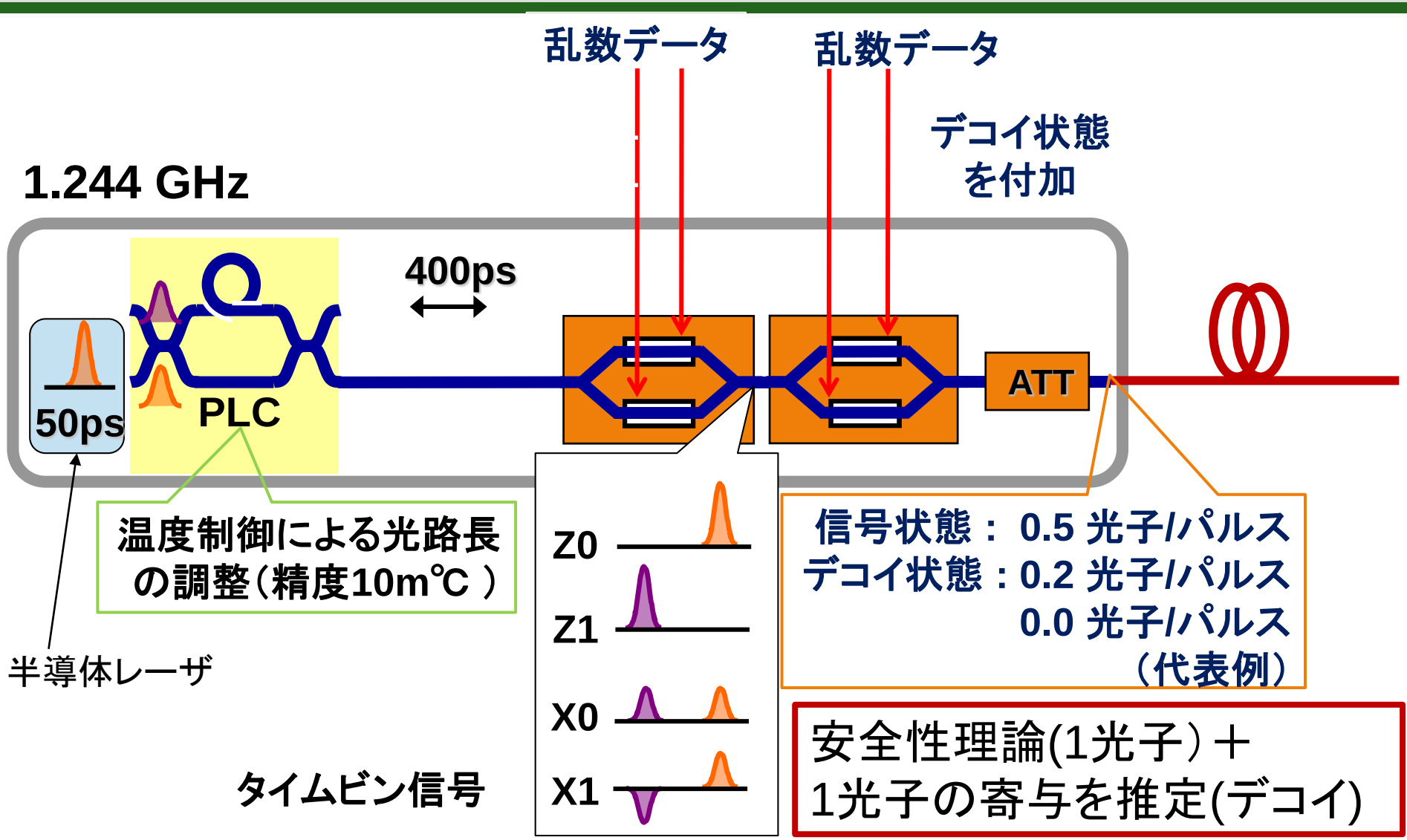
偏光から位相差(タイムビン量子ビット)

光ファイバを伝搬する偏光状態は不安定

青：垂直偏光
赤：水平偏光
緑：両偏光の和



エンコーダ（送信部）

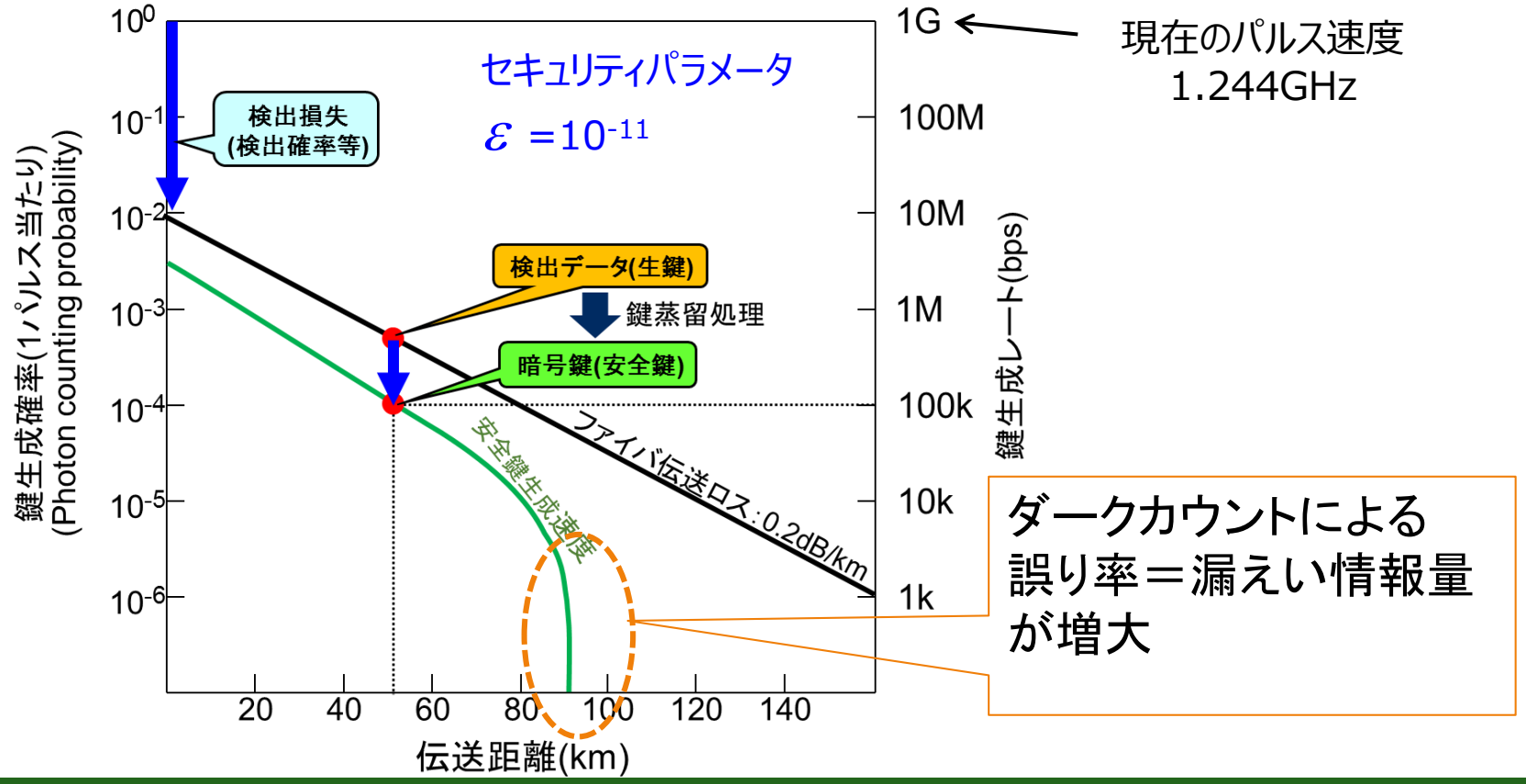

乱数データ
乱数データ
デコイ状態
を付加
1.244 GHz
400ps
50ps
PLC
ATT
温度制御による光路長
の調整（精度10m℃）
半導体レーザ
Z0
Z1
X0
X1
タイムビン信号
信号状態： 0.5 光子/パルス
デコイ状態：0.2 光子/パルス
0.0 光子/パルス
（代表例）
安全性理論(1光子）＋
1光子の寄与を推定(デコイ)

QKDの性能指標：安全性＋鍵生成レート

・安全性を向上（セキュリティパラメータεを小さく）させると鍵生成速度は下がる

・鍵生成速度＝(パルス速度) x (透過率) x [1 − (誤り訂正) − (秘匿性増強)]

ビット誤り　　位相誤り



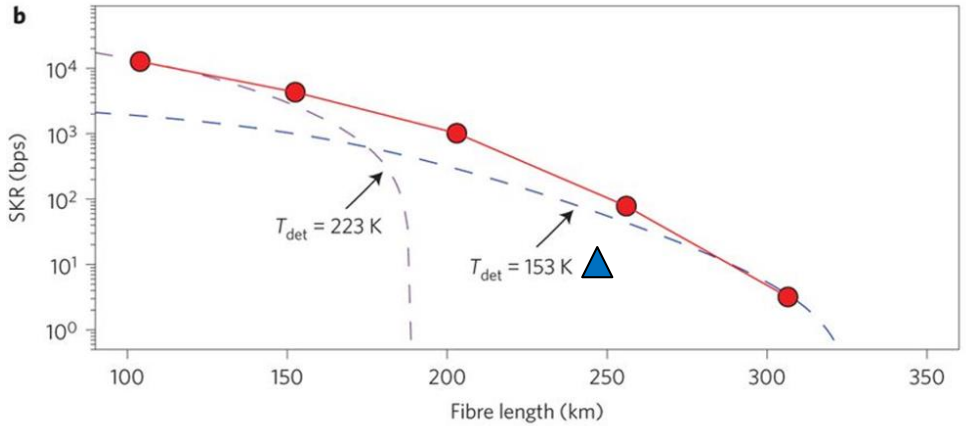
State-of-Arts experiments

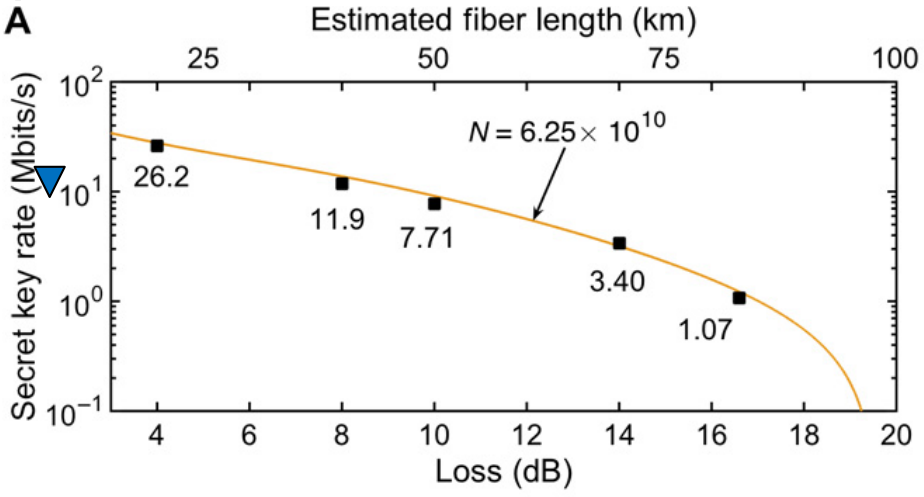
伝送距離

- ● COW(2015): 3.18bps after 307km (51.9 dB loss)
- ▲ Decoy BB84(2017) : 8.4bps after 240km (44.4dB loss)

鍵生成速度

- ■ Qudit (2017) : 26.2Mbps at 4dB loss
- ▼ Decoy BB84 (2017): 13.72Mbps at 2 dB loss





● Korzh, *et al*., *Nat. Photon.* **9**, 163 (2015)

■ Islam, *et al.,* Sci. Adv. **3**,(11) 1 (2017)

▲ Frölich, *et al*., Optica 4, 163 (2017)

▼ Yuan, et al., J. Lightwave Tech. **36**, 3427 (2017)

信頼性試験の状況（NEC）

・QKD実用化に向けた評価実験をサイバーセキュリティ・ファクトリーで開始　（2015年9月プレスリリース）

サイバーセキュリティ・ファクトリーに設置したQKD装置
左：送信機、右：受信機

サイバーセキュリティ・ファクトリー

研究開発の現状まとめ

量子暗号の製品化と利用状況

- ベンチャー企業が製品化(スイス id quantique, 中国 QuantumCtekなど) 大きな市場はできていない
- 性能は，鍵生成速度10kbps程度@20~30km

日本の状況

- 世界最速(300k~1Mbps@50㎞)装置をNECと東芝が開発
- ユーザ環境での信頼性試験実施中
- 実装安全性，信頼性を重視．製品化は未定

中国の状況

- 巨額の国家予算を投入，世界最大の量子暗号ネットワーク(北京ー上海間2000㎞）を構築
- 2017年6月，衛星から２つの地上局（距離1200km）への量子もつれ配信に成功．世界最高水準のレーザ捕捉追尾技術を保持

研究の方向

MORE QKD

- 性能(伝送距離，鍵レート)の向上
- 実装安全性の保証
- 高信頼性の保証

MORE THAN QKD

- ネットワーク化 (伝送制御，鍵管理，ユーザ管理，etc.)
- アプリケーション開発(古典的情報理論的安全な暗号技術との融合)

BEYOND QKD

- 量子中継
- QKD以外の量子暗号プロトコル
- 異なる原理に基づく鍵共有

実装安全性: *A Skeptical Customer?*

Show me Evidence!

Security certification process should include:

1. **definition** of protocol and devices
2. **clarification** of the assumptions of security theory
3. **extraction** of the device requirements from the theoretical assumptions
4. **characterization** of devices ~ methods and criteria
5. **improvement** on protocol, devices, system design & fabrication
6. **documentation** of the criteria, method and proof of fulfilment

安全性評価＝安全性理論の仮定検証

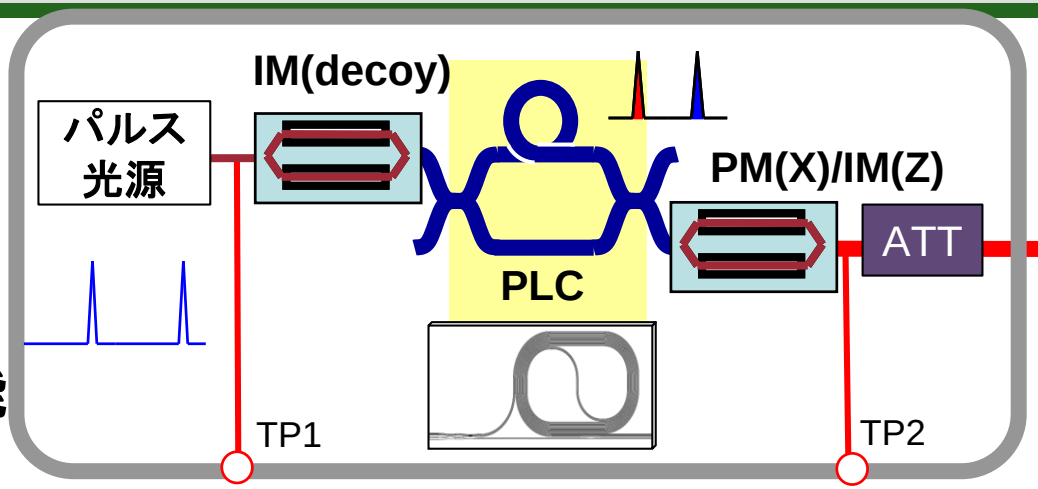
1. **プロトコルにおける設定値（秘密）が判別不可能**
   - ビット値，基底，デコイパルスの位置，テストビットの位置，(秘匿性増強における）ハッシュ関数の選択
2. **設定値を外部から観測・制御不可能**
   - サイドチャネルがない：量子チャネルからのみ情報を得る
3. **安全性理論における仮定が成立**
   - ✓ 一般的な仮定
     - ✓ 量子力学は正しい
     - ✓ 情報理論的に安全な古典通信路がある
   - ● 安全性理論に依存する仮定
     - パルスは独立 (パルス間の相関を持たない)
     - 光子数分布は既知
     - 光子検出効率は基底選択に無依存

送信機の仮定と光パルスの特性

設定値の判別不可能性

- パルス波形
- 波長スペクトラム
- 偏光
- 空間モード

が全ての状態で判別不能



BB84状態

X基底のパルスとZ基底のパルスが判別不能
（タイムビンの振幅比，位相差が正確）

パルスの独立性

位相相関 → 隣接パルス間の干渉性がない
強度相関

光子数分布が既知

ポアソン分布
平均光子数が正確（強度変動が小さい）

送信機の評価

パルス光源（実装：利得スイッチ半導体レーザ）

1. パルス毎の強度測定
   - 強度の安定性
   - パルス間強度相関
2. 隣接パルス間の干渉性測定

強度変調器

3. パルス毎の強度測定
   - 強度相関
   - サブプロトコルの提案 (Pattern Sifting, Alternate Key Distillation)
   - 安定性

BB84状態

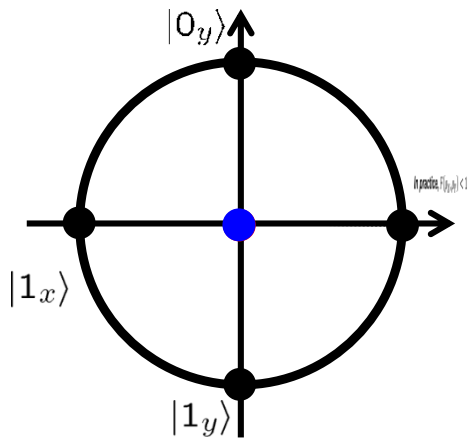
4. 状態トモグラフィ

4. 状態生成における信号劣化の影響

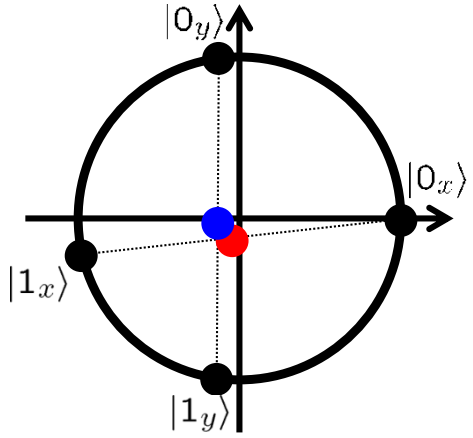
位相変調器への劣化信号印加

➡ 状態生成エラー（State Preparation Flaw）

Ideally, $F(\rho_X, \rho_Y) = 1$



In practice, $F(\rho_X, \rho_Y) < 1$



GLLP:

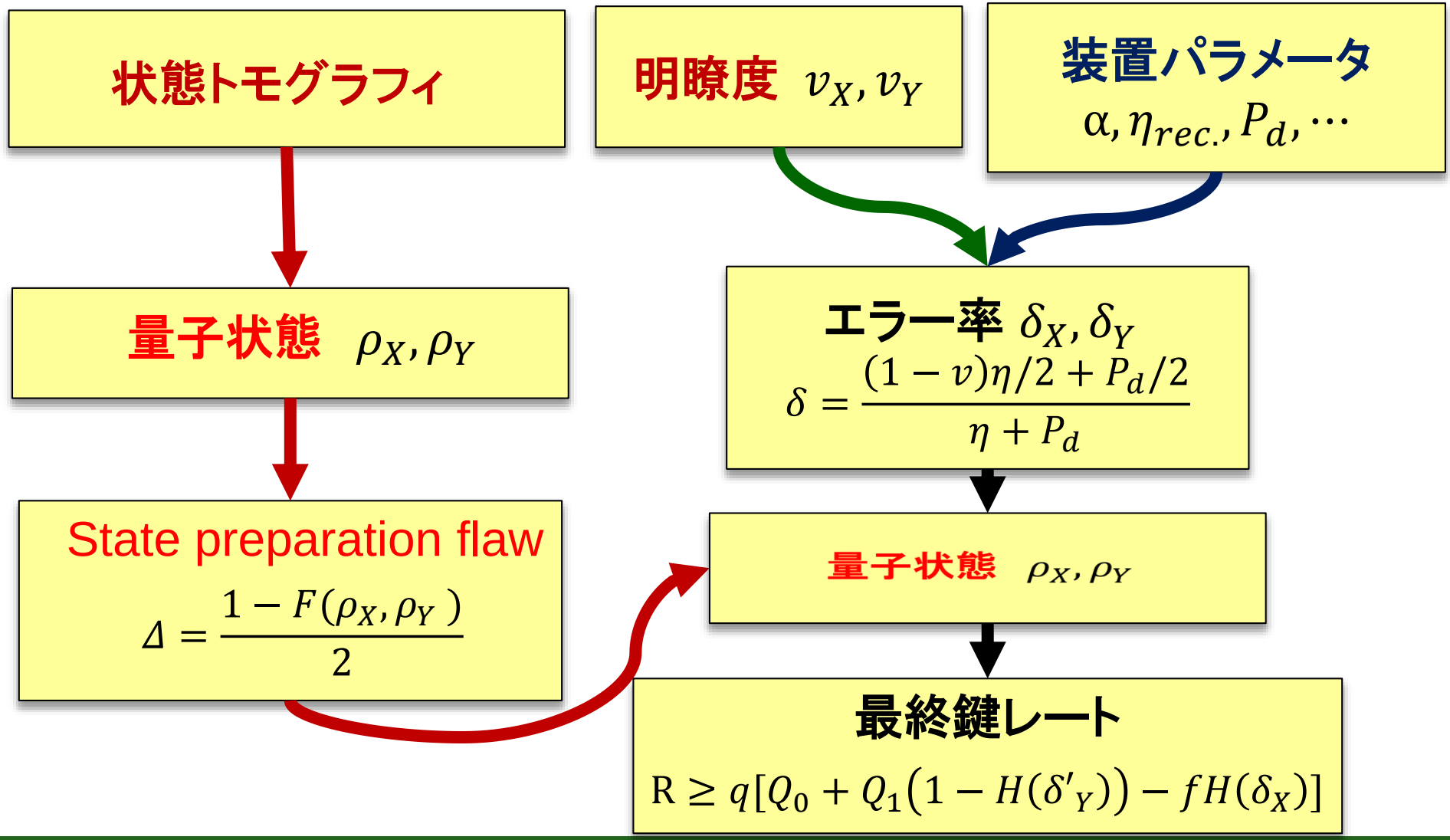
$$R \propto 1 - h(\delta_x) - h(\delta'_y)$$

$$\delta'_y \leq \delta_y + 4\Delta + 4\sqrt{\Delta\delta_y}$$

$$\Delta = \left[\left(1 - F\left(\rho_Y, \rho_X\right)\right)/2\right]/\eta_{\text{detection}}$$

D. Gottesman, H. K. Lo, N. Luetkenhaus, and J. Preskill,Quant. Inf. Comput. **5**, 325 (2004).
M. Koashi, arXiv:quant-ph/0505108.

状態生成エラーの評価と鍵レートの推定



状態トモグラフィ

2 次元の行列は Pauli 行列で展開できる:

$$\hat{\rho} = \frac{1}{2}\sum_{i=0}^{3} \frac{S_i}{S_0}\hat{\sigma}_i$$

展開係数（Stokes parameters）を下のように観測値から推定する

$$S_0 = 2n_0, S_1 = 2(n_1 - n_0), S_2 = 2(n_2 - n_0), S_3 = 2(n_3 - n_0)$$

where

$$n_0 = \frac{1}{2}(\langle 0|\rho_X|0\rangle + \langle 1|\rho_X|1\rangle) = \frac{1}{2}(I_{Z_0|X_0} + I_{Z_0|X_1} + I_{Z_1|X_0} + I_{Z_1|X_1})$$

$$n_1 = \langle 0|\rho_X|0\rangle = I_{Z_0|X_0} + I_{Z_0|X_1}$$

$$n_2 = \langle X_1|\rho_X|X_1\rangle = I_{X_0|X_1} + I_{X_1|X_1}$$

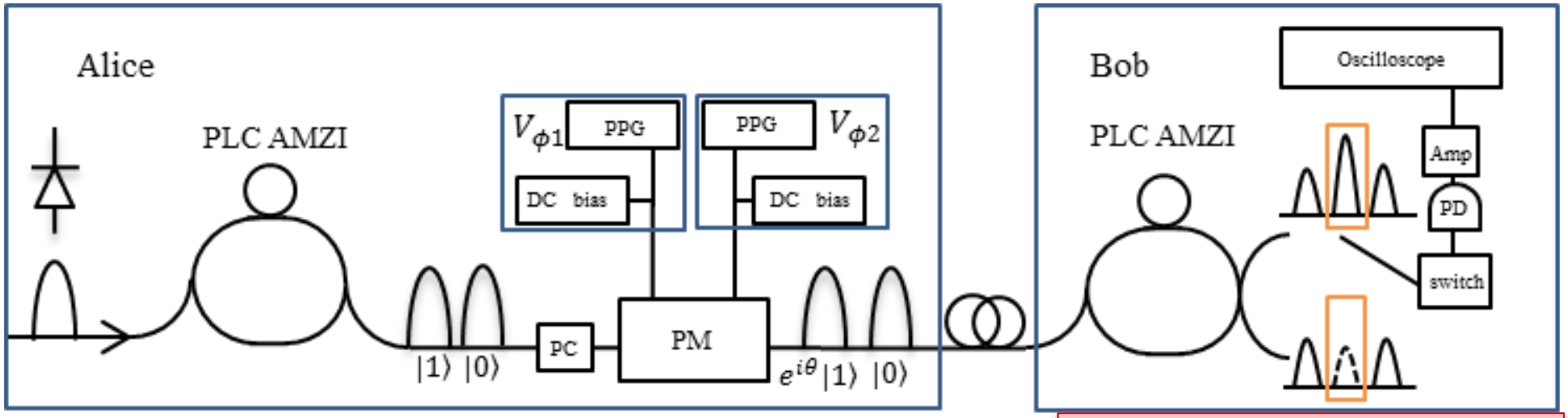
$$n_3 = \langle Y_1|\rho_X|Y_1\rangle = I_{X_0|Y_1} + I_{X_1|Y_1}$$

prepared state

Measurement basis and outcome

実験

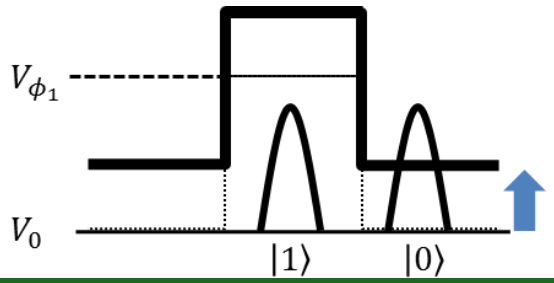
受信機は完全であると仮定



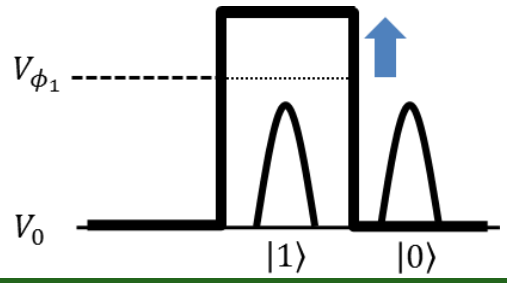
Center pulse reflects interference

Two patterns of voltage shift

Shift of bias (DC)



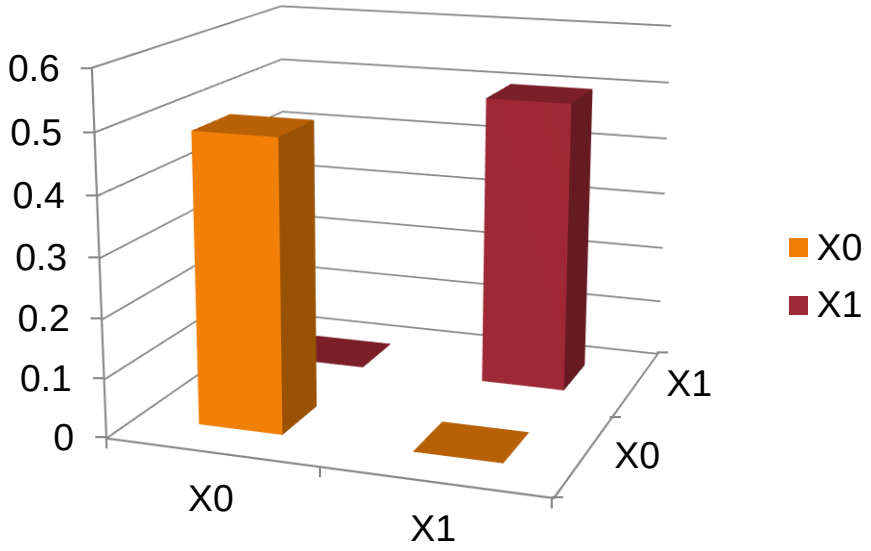
Change of modulation signal (AC)



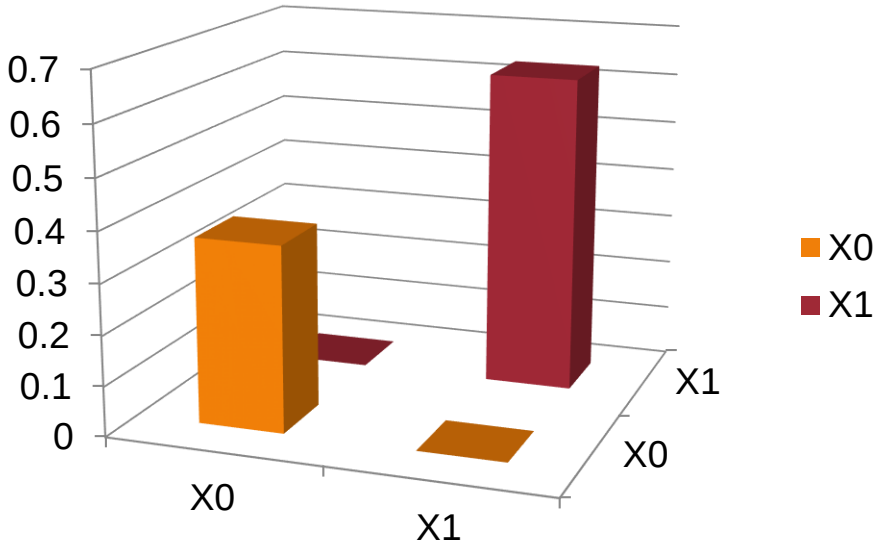
状態トモグラフィの測定結果 (DDM)

Density matrix ρ_X from DDM in AC case

No shift

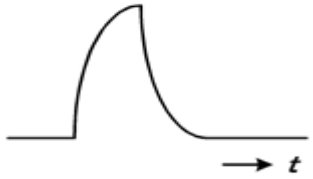


25% Amplitude shift



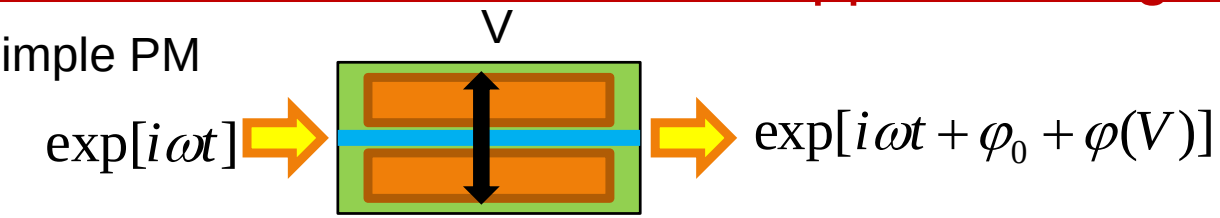
実装法の改善

high speed modulation ⇨ pulse shape distortion ⇨ altered signal voltage by timing ⇨ PM fluctuation

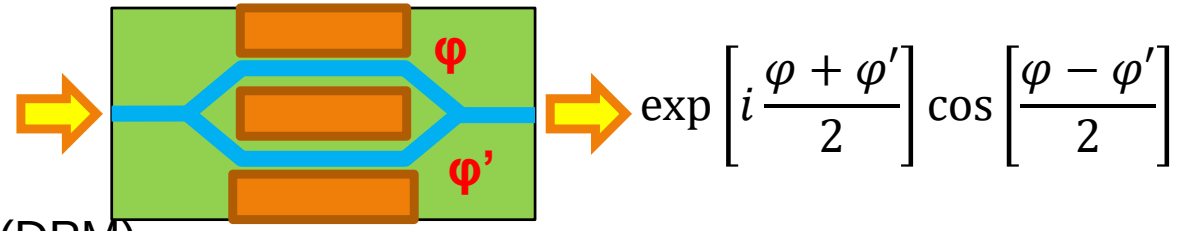


Phase modulation robust to applied voltage change

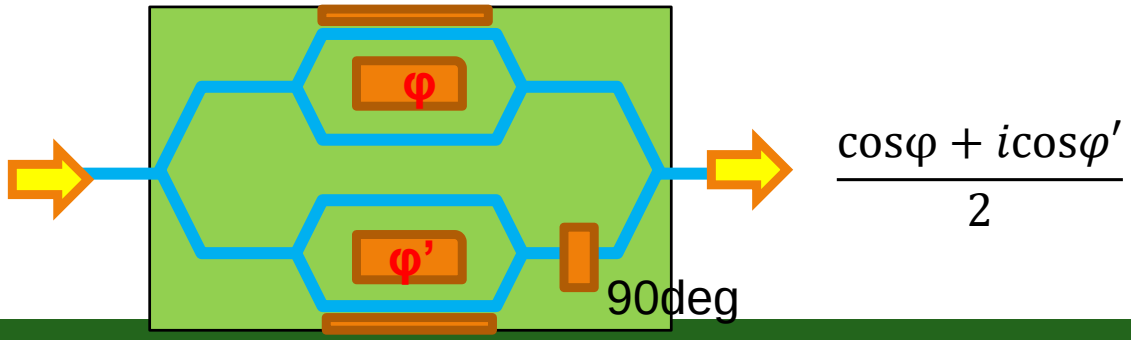
Simple PM

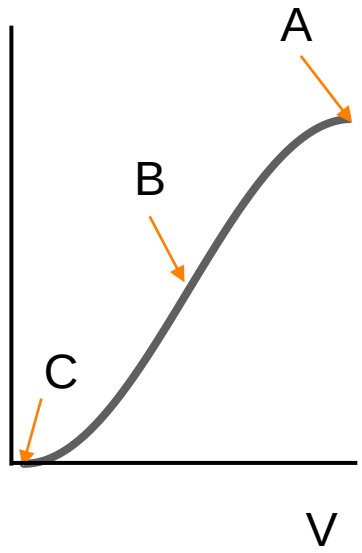


Mach-Zehnder (DDM)



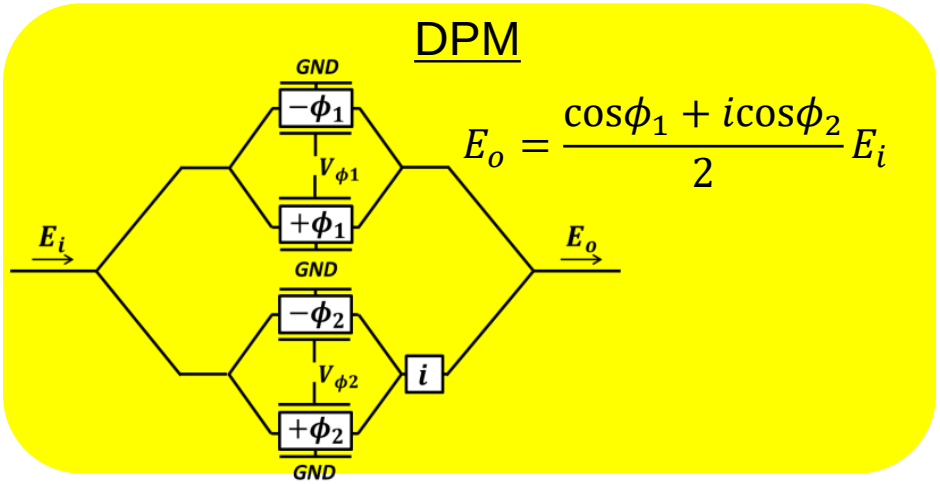
Nested (DPM)





DPMによる状態生成

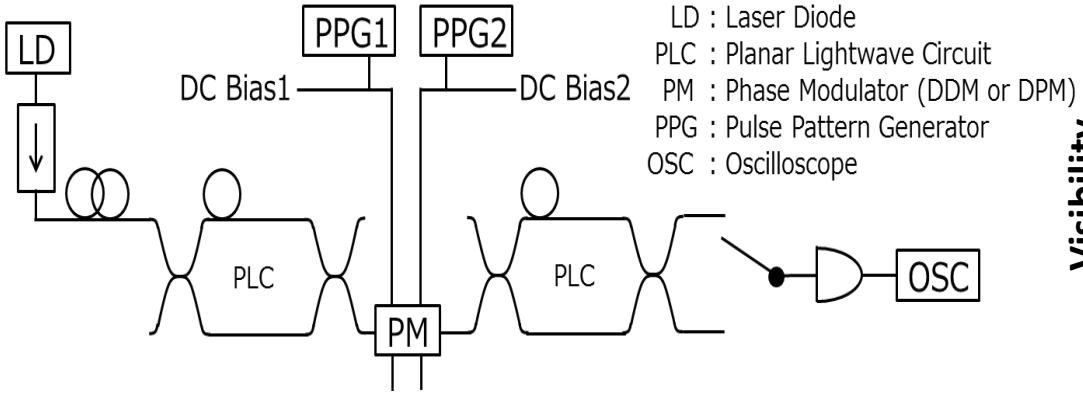
Phase modulation for BB84 states

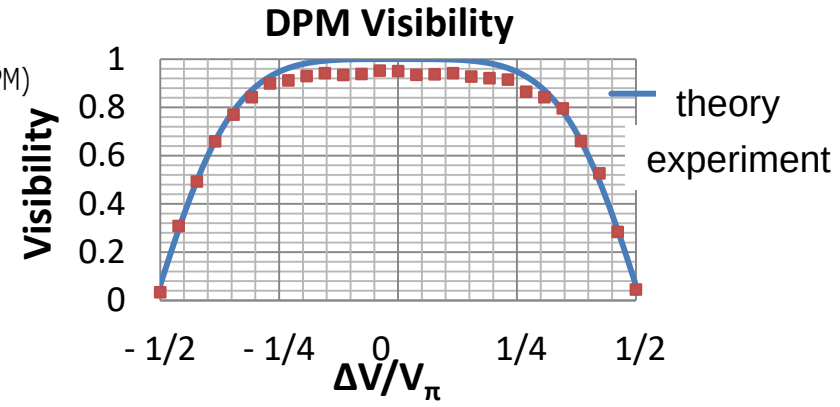


		X0	X1	Y0	Y1
$\|0\rangle$	ϕ_1	0			
	ϕ_2	0			
$\|1\rangle$	ϕ_1	0	π	π	0
	ϕ_2	0	π	0	π

For $\phi_i = 0 \; or \; \pi$,

$$\cos(\phi_i + \delta) = \cos\phi_i \left(1 - \frac{1}{2}\delta^2 + \cdots\right)$$

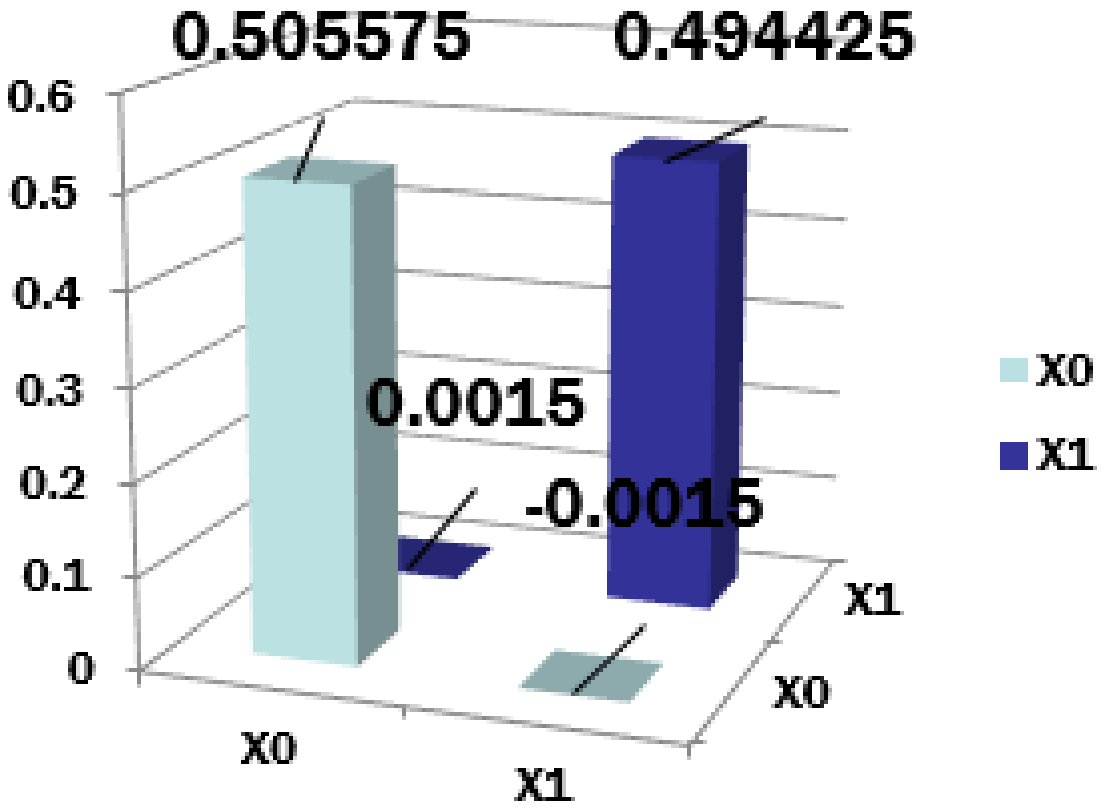




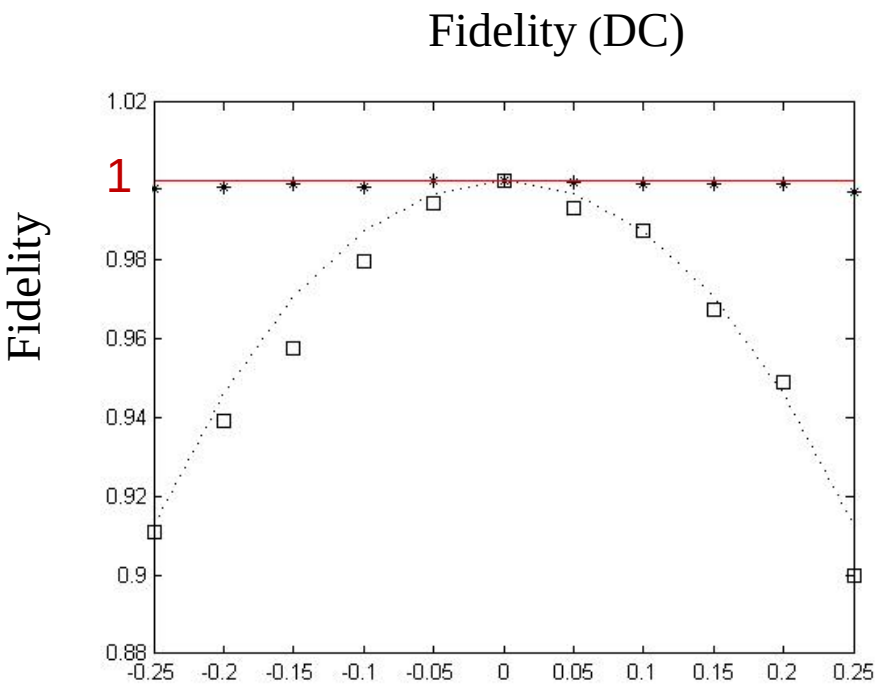
状態トモグラフィの測定結果 (DPM)

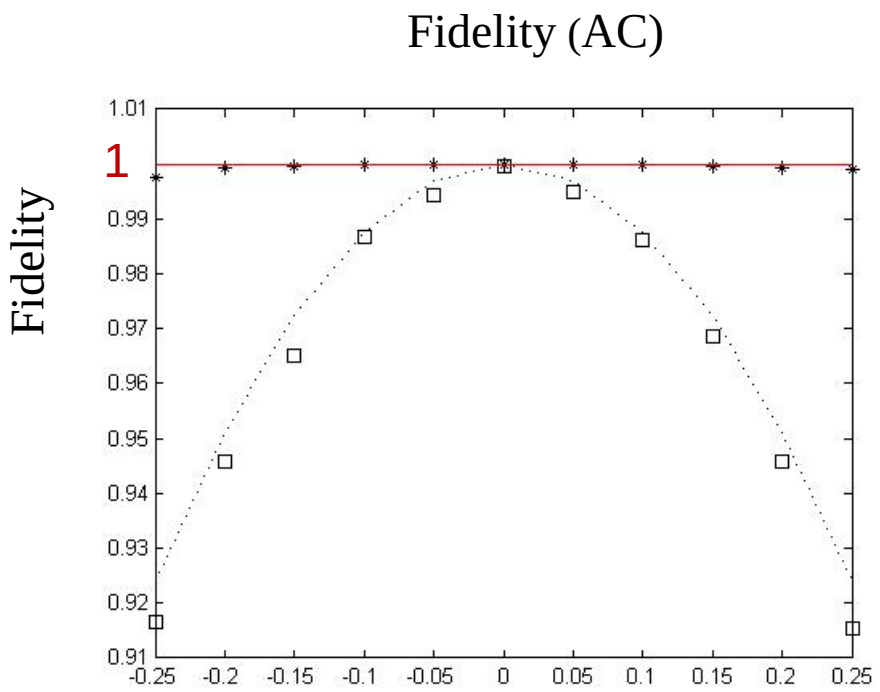
Density matrix ρ_X from DPM in AC case

25% Amplitude shift



基底間のFidelity $F(\rho_X, \rho_Y)$





◘ DDM Experiment

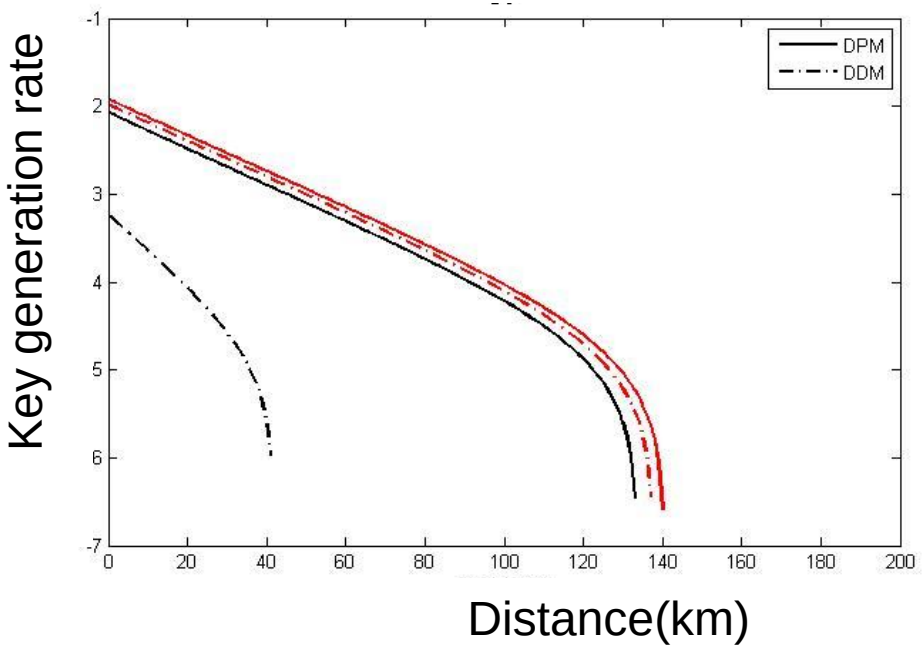
····· DDM Theory

✱ DPM Experiment

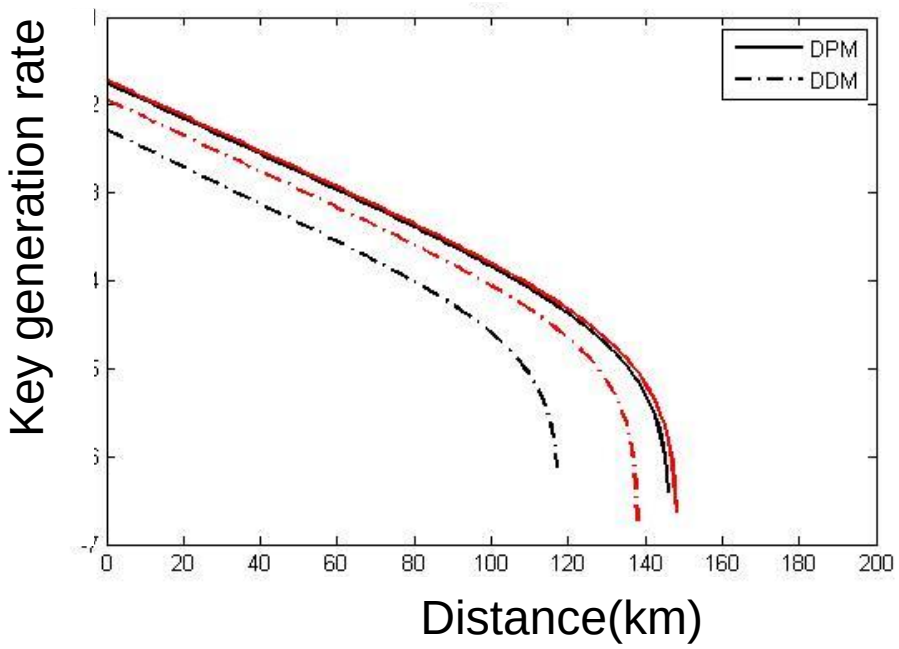
—— DPM Theory

最終鍵レート

Key generation rate by changing DC



Key generation rate by changing AC



DPM no shift

DDM no shift

DPM5% shift

DDM5% shift

State preparation flawの影響は適切な実装法で抑圧できる

ネットワーク化：海外動向

中国

新華社
金融通信に量子暗号
を実利用（2012年2月）

50ノード級の大規模量子暗号ネットワーク（合肥市）

世界最大の量子暗号ネットワークを構築
北京、済南、合肥、上海を結ぶ2000kmのバックボーン

Qiang Zhang氏 (USTC) のご好意による

衛星量子通信：中国(1/2)

量子科学技術衛星 Mozi（墨子）
を打ち上げ（2016年8月）

量子科学技術衛星 600kg

・2017年6月、1200km離れた2つの地上局に向けて衛星から量子もつれ配信を行う実験に世界で初めて成功 (J. Yin et al., Science, vol. 356, no. 6343, p. 1140, June 2017)

中国が世界最高精度のレーザ捕捉追尾技術を保持

衛星量子通信：中国(2/2)

・2017年7月、衛星-地上間でQKD実験公表
・鍵生成速度1.1 kbit/s
　セキュリティパラメータ 10^{-9}

・光源波長：848.6 nm
・パルス生成速度：100 MHz
・パルス幅：0.2 ns
・地上ビーム径10 m
（1200 km伝搬後）

・2017年7月、地上-衛星間での量子テレポーテーション実験公表

日本では企業が試作機開発、ユーザ環境で運用試験中

NEC
共通鍵暗号（AES）と量子暗号（QKD）を統合
⇒ネットワークスイッチ間を直結する専用回線
を秘匿化するQKD-AES統合システムを開発
⇒2015年夏から都内のサイバーセキュリティ
関連施設において長期運用試験を実施中

http://jpn.nec.com/press/201509/20150928_03.html

現在世界最高速

東芝
世界最高速、かつ小型の
量子暗号装置を開発
⇒2015年夏から仙台市において、
ゲノム解析データの暗号化通信
実験を実施中

http://www.toshiba.co.jp/about/press/2015_06/pr_j1801.htm

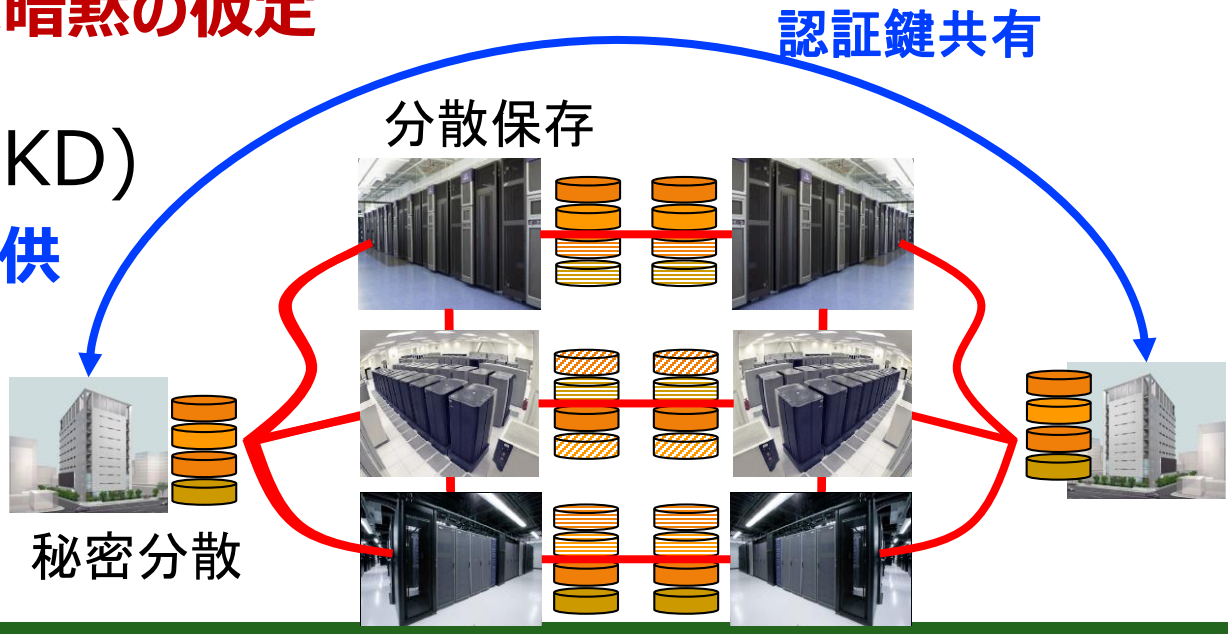
超長期安全な秘密保管ネットワーク(提案)

秘密分散

- 原データを無意味化された複数の断片（シェア）に分割（**情報理論的安全**）
- 一部のシェアが失われても原データを復元可能
- 秘匿性を保ったまま計算が可能
- **伝送路の秘匿性は暗黙の仮定**

量子暗号鍵配送（QKD）

- **安全な伝送路を提供**
- **認証鍵(~kbits)共有により離れた拠点間で情報伝送**



おわりに

QKD：　34歳（26歳？）.
ようやく独り立ち？

- エンジニアリング的な課題
- 基本的な課題：測定と操作，知りうる情報の限界