量子力学100周年研究会：量子基礎・量子情報のこれまでとこれから　2025/9/11

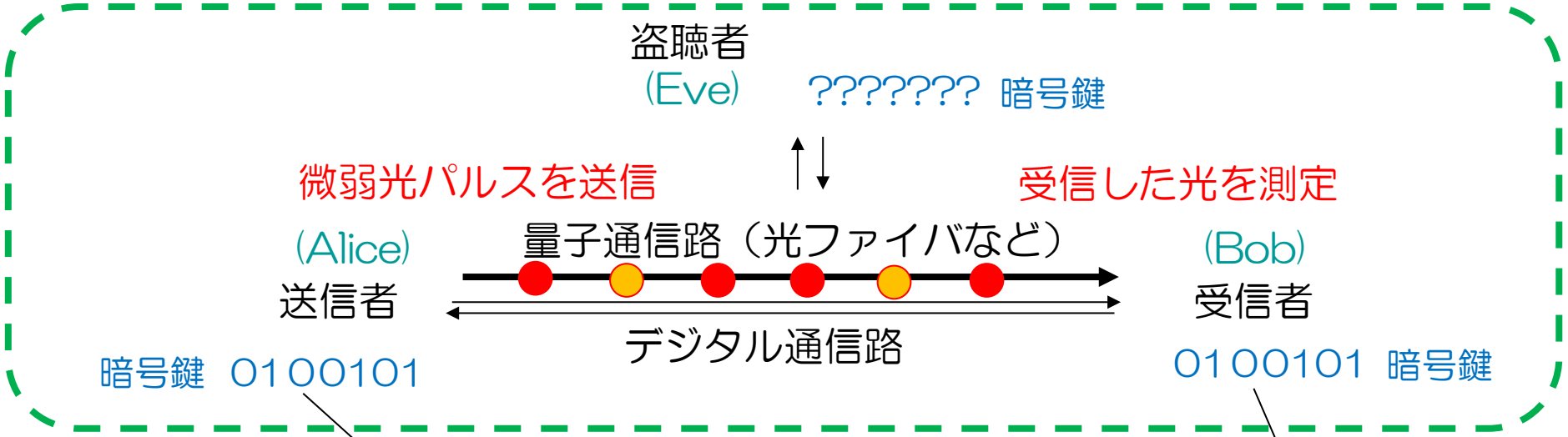
量子暗号のセキュリティ理論から見える量子力学

小芦　雅斗
東京大学 大学院工学系研究科

Promenade:　ＱＫＤの基礎
Movement 1: 量子情報基礎との意外な関り
Promenade:　ＱＫＤの原理
Movement 2: 量子鍵配送の原理の見直し
Promenade:　ＱＫＤの実際
Movement 3: アイデアのRepurposing
Promenade:　ＱＫＤの理論
Movement 4: セキュリテイ証明の２つのアプローチ
Postlude:　まとめと雑感

QKDの基礎

暗号鍵：
AliceとBobに共有されたランダムなビット列で、Eveはその内容を知らない。



量子鍵配送（QKD）
Quantum Key Distribution

Message:
「カード番号は
1202 4545 4343 5656
です。」

符号化

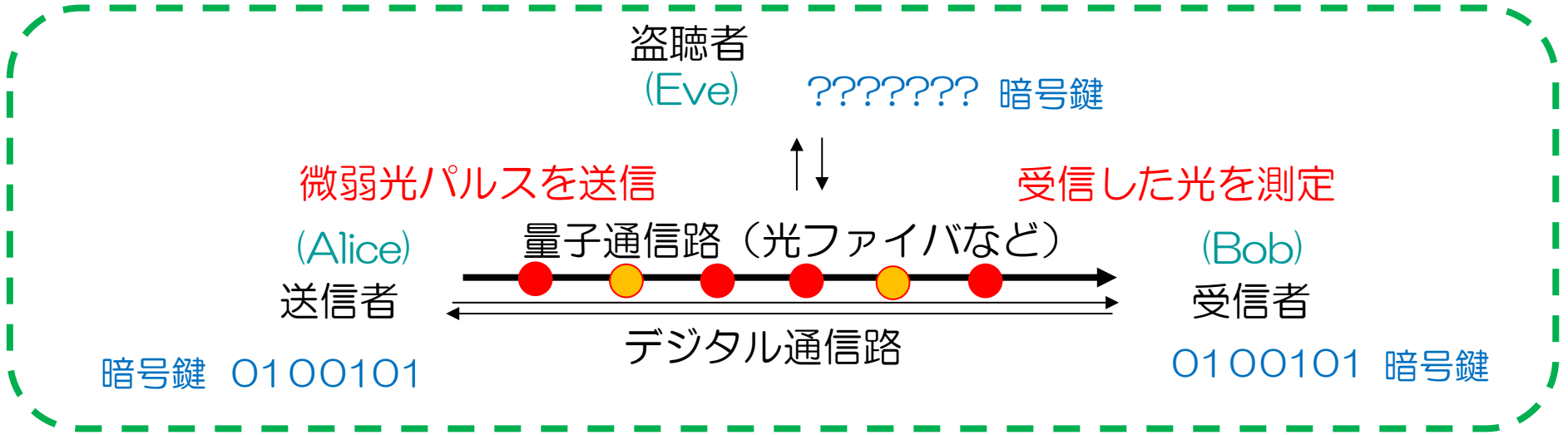
1011010

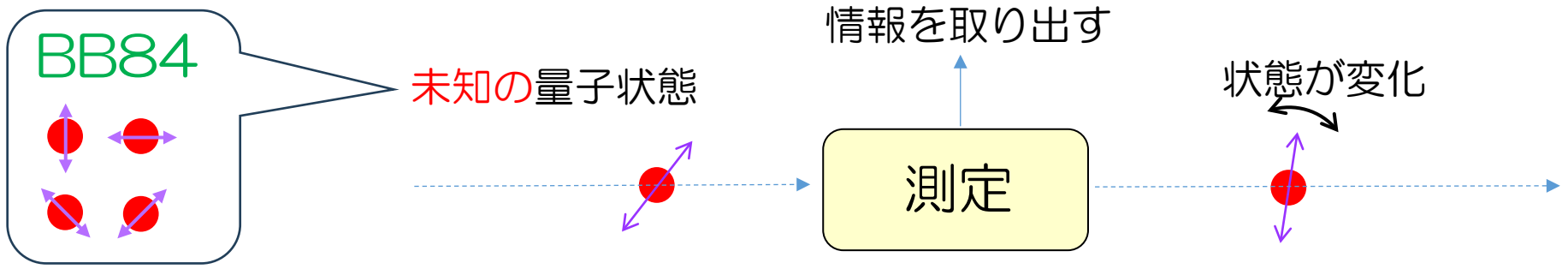
デジタル通信路

復号化

Message:
「カード番号は
1202 4545 4343 5656
です。」

QKDの基礎





最初に提案された方式
(Bennett-Brassard 1984)

「量子系から情報を取り出すと、状態が変化する」

量子測定の反作用
情報取得と擾乱のトレードオフ
ハイゼンベルクの不確定性関係

量子力学100周年研究会：量子基礎・量子情報のこれまでとこれから　2025/9/11

量子暗号のセキュリティ理論から見える量子力学

小芦　雅斗
東京大学 大学院工学系研究科

Promenade:　ＱＫＤの基礎
Movement 1: 量子情報基礎との意外な関り
Promenade:　ＱＫＤの原理
Movement 2: 量子鍵配送の原理の見直し
Promenade:　ＱＫＤの実際
Movement 3: アイデアのRepurposing
Promenade:　ＱＫＤの理論
Movement 4: セキュリテイ証明の２つのアプローチ
Postlude:　まとめと雑感

量子情報の大きさとは？

古典情報　　シャノンの情報源符号化定理

$\{p_i, i\}$　　ABCDBCDBCABCDBC….

確率　文字

$$H(\{p_i\}) \equiv -\sum_i p_i \log_2 p_i \quad \text{bits}$$　Shannon(1948)

この信号を保存するのに必要十分なメモリの大きさ

量子情報の場合は？　　ρ_3 ρ_1 ρ_5 ρ_2 ρ_3 ρ_4 …

$\{p_i, \rho_i\}$　　$\rho \equiv \sum_i p_i \rho_i$

量子状態

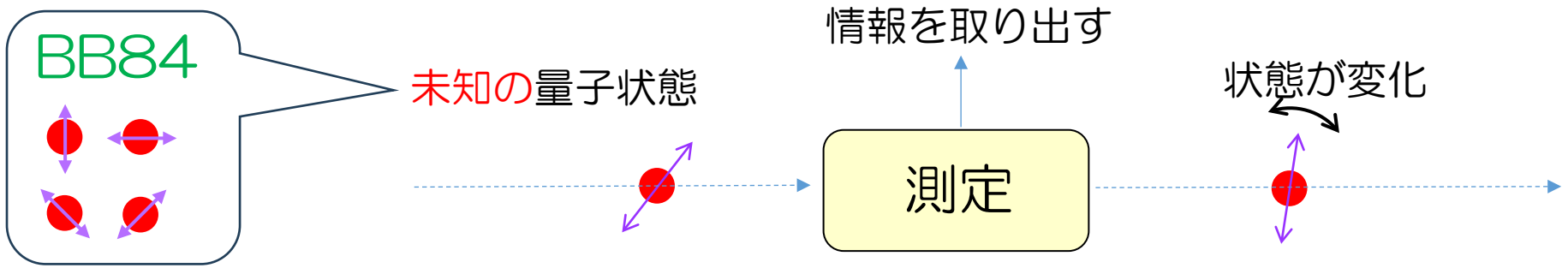
$$S(\rho) \equiv -\mathrm{Tr}[\rho \log_2 \rho] \quad \text{qubits}$$　Schumacher(1995)

この信号を保存するのに十分な量子メモリの大きさ

本当にそれだけ必要？

一見すると、量子暗号とは何の関係もない話に思えるのだが…

量子暗号に使える情報の収納場所は？



最初に提案された方式
(Bennett-Brassard 1984)

「量子系から情報を取り出すと、状態が変化する」

非直交2状態 Bennett (1992)

直交３状態 Goldenberg-Vaidman (1995)

直交２状態 Koashi-Imoto (1997)

$\{\rho_1, \rho_2, \rho_3, \dots\}$

一般の量子状態の組

取り出しても状態が変化しない情報

取り出したら状態が変化する情報

この区別をはっきりさせたい

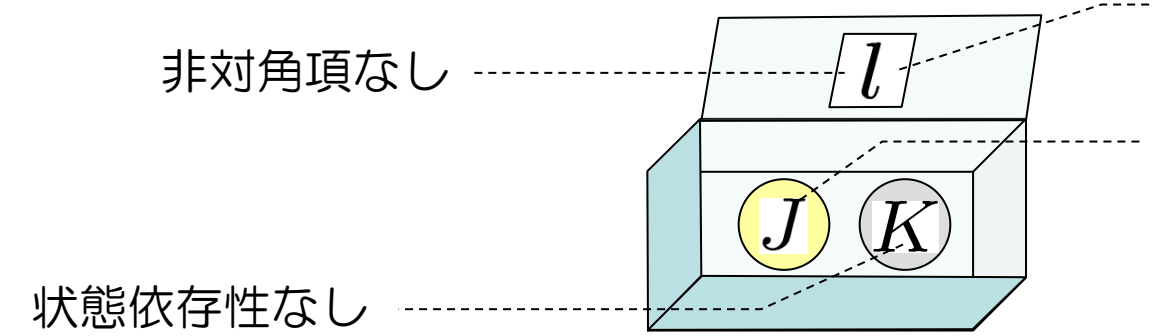
量子暗号に使える情報の収納場所は？

$\{\rho_1, \rho_2, \rho_3, \dots\}$

$\mathcal{H}$

これらの状態を変化させない操作は？

Koashi, Imoto, *Phys. Rev. A* **66**, 022318 (2002).



見るのは自由
書き換え不可

触ることができない

$$\mathcal{H} = \bigoplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

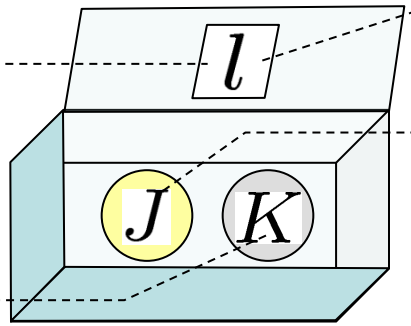
$$\rho_i = \bigoplus_l p^{(l,i)} \sigma_J^{(l,i)} \otimes \tau_K^{(l)}$$

量子情報源の最適圧縮率

$\{\rho_1, \rho_2, \rho_3, \dots\}$

これらの状態を変化させない操作は？

$\mathcal{H}$



非対角項なし

状態依存性なし

見るのは自由
書き換え不可

触ることができない

$$\mathcal{H} = \bigoplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

$$\rho_i = \bigoplus_l p^{(l,i)} \sigma_J^{(l,i)} \otimes \tau_K^{(l)}$$

情報源 $\{p_i, \rho_i\}$

$$\rho := \sum_i p_i \rho_i = \bigoplus_l p^{(l)} \sigma_J^{(l)} \otimes \tau_K^{(l)}$$

Koashi, Imoto, *Phys. Rev. A* **66**, 022318 (2002).

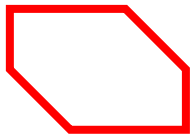
Koashi, Imoto, *Phys. Rev. Lett.* **87**, 017902 (2001).

$$S(\rho) = \underbrace{H(\{p^{(l)}\})}_{\text{必要な古典メモリ(bits)}} + \underbrace{\sum_l p^{(l)} S\left(\sigma_J^{(l)}\right)}_{\text{必要な量子メモリ(qubits)}} + \underbrace{\sum_l p^{(l)} S\left(\tau_K^{(l)}\right)}_{\text{保存の必要なし}}$$

量子暗号のセキュリティの研究の副産物として、この公式が発見された。

量子情報源の最適圧縮率

$\{\rho_1, \rho_2, \rho_3, \ldots\}$

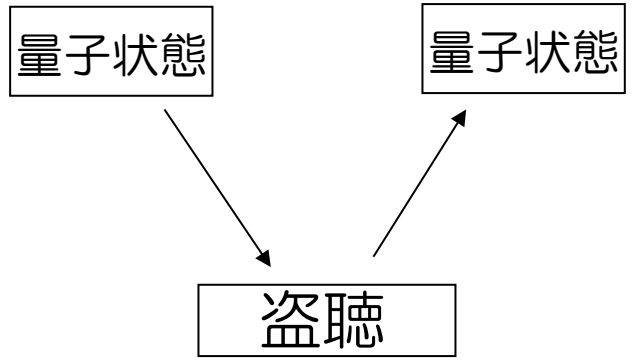


$\mathcal{H}$

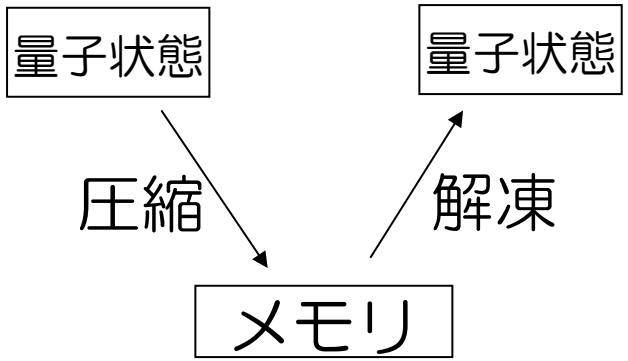
これらの状態を変化させない操作は？

$$\mathcal{H} = \bigoplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$$

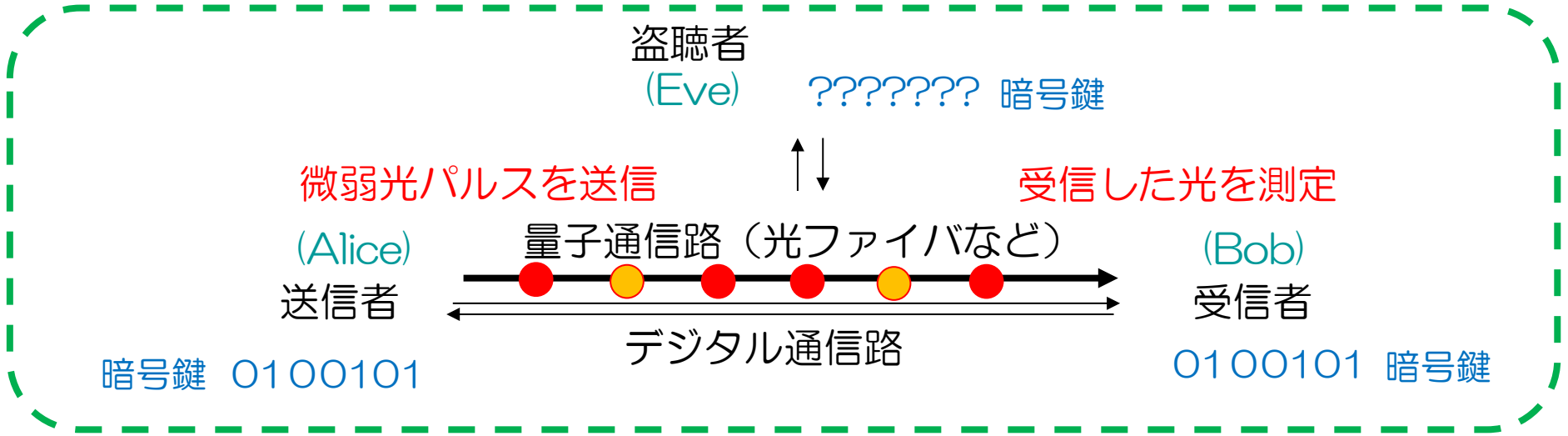
量子暗号に使える
状態の組み合わせを
一般的に理解したい



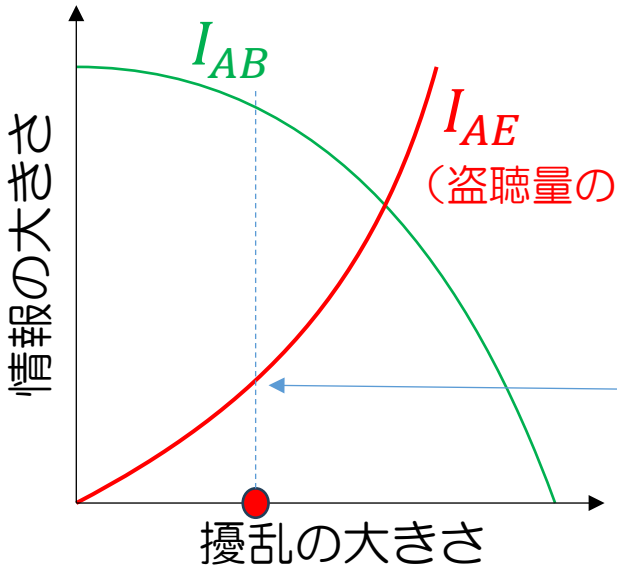
量子信号を保存するのに必要十分なメモリの大きさ



QKDの原理



「量子系から情報を取り出すと、状態が変化する」⇒ 状態の変化を調べれば、盗聴の程度がわかる



擾乱の大きさを推定
（ビットエラー率など）
盗聴量の上限 I_{AE} が定まる

通信したデータから、
シフト鍵を作り、エラー訂正
（長さI_{AB}の同じビット列を共有）

0100110001001　I_{AB} ビット

⇓ Privacy Amplification

暗号鍵 0100101　（$I_{AB} - I_{AE}$）ビット

量子力学100周年研究会：量子基礎・量子情報のこれまでとこれから　2025/9/11

量子暗号のセキュリティ理論から見える量子力学

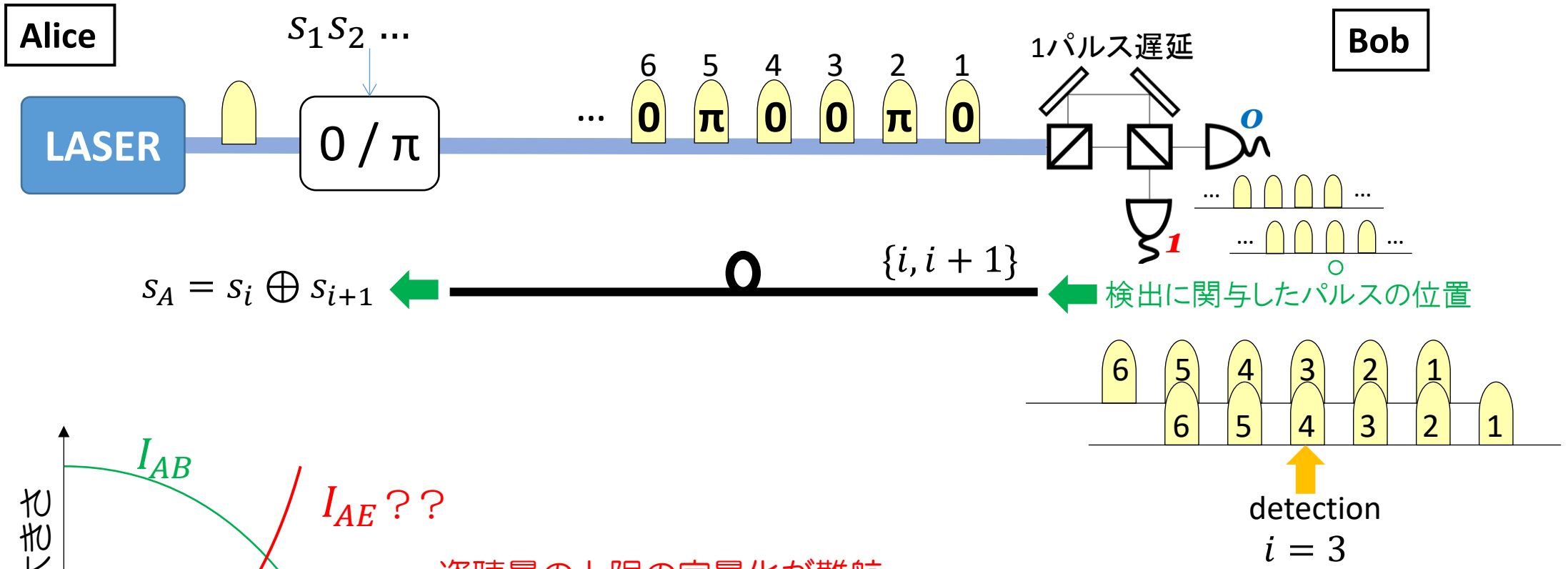
小芦　雅斗
東京大学 大学院工学系研究科

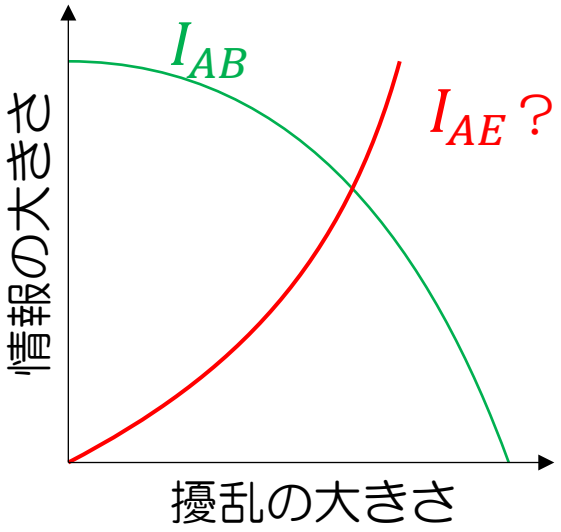
Promenade:　ＱＫＤの基礎
Movement 1: 量子情報基礎との意外な関り
Promenade:　ＱＫＤの原理
Movement 2: 量子鍵配送の原理の見直し
Promenade:　ＱＫＤの実際
Movement 3: アイデアのRepurposing
Promenade:　ＱＫＤの理論
Movement 4: セキュリテイ証明の２つのアプローチ
Postlude:　まとめと雑感

Differential Phase-Shift (DPS) QKD

DPS-QKD：シンプルな変調で長距離通信に期待

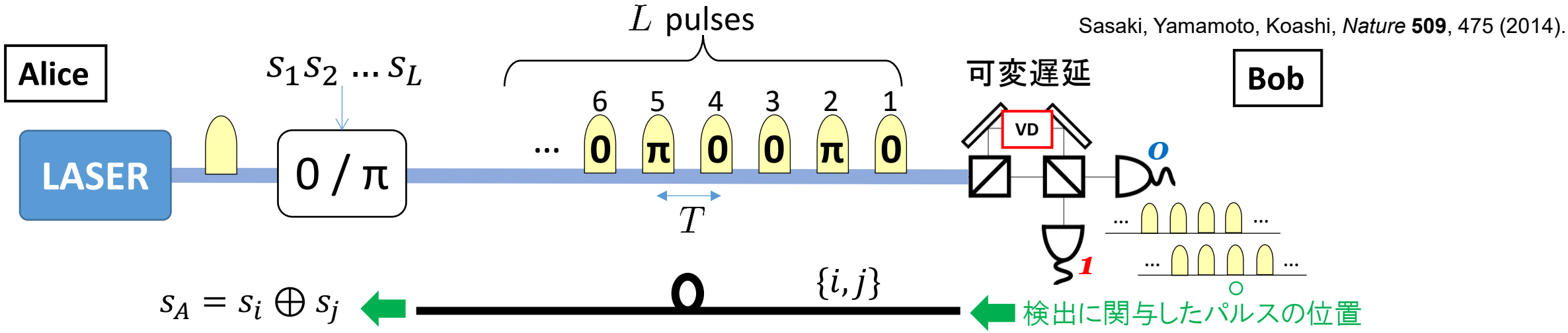
Inoue, Waks, Yamamoto, *Phys. Rev.* A **68**, 022317 (2003).





盗聴量の上限の定量化が難航

Round-Robin DPS QKD



Sasaki, Yamamoto, Koashi, *Nature* **509**, 475 (2014).

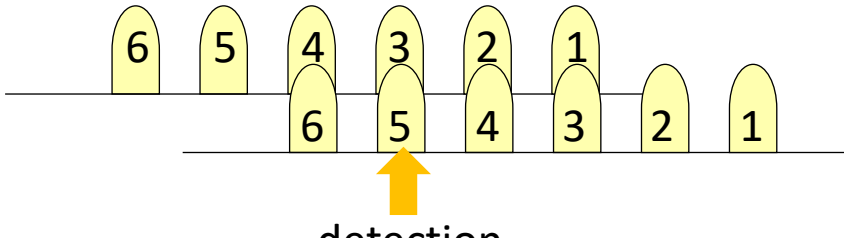
VD $(L-1)$種類の遅延を等確率に選ぶ

$\tau_D = T$

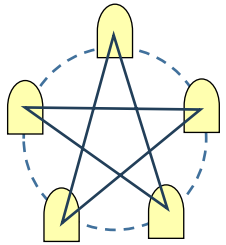
$\tau_D = 2T$

$\tau_D = 3T$

$\tau_D = (L-1)T$

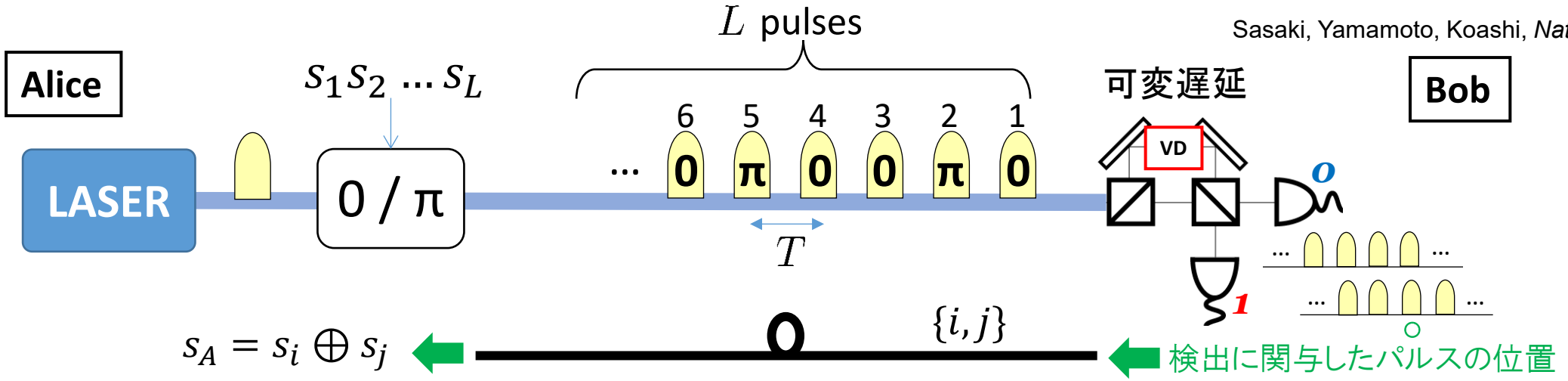


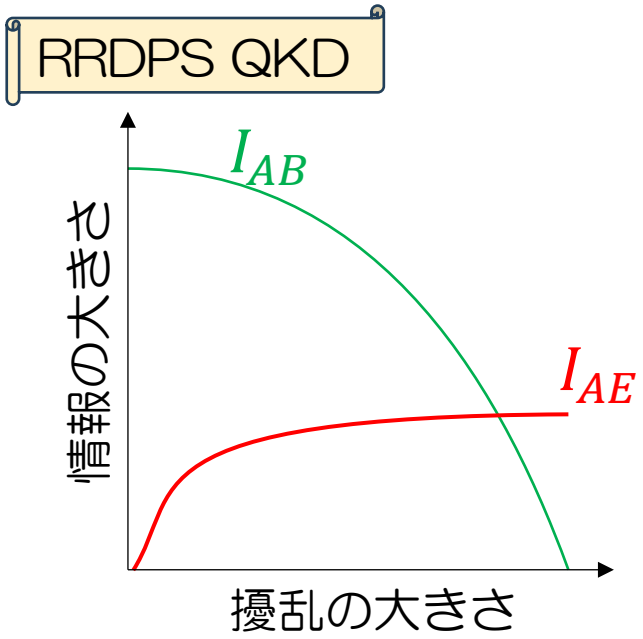
$\{i,j\} = \{3,5\}$

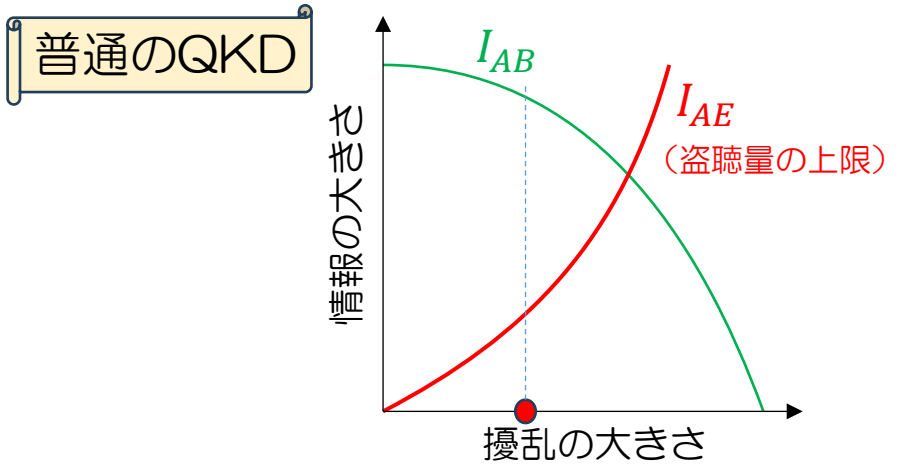


「総当たり」：高い対称性

Round-Robin DPS QKD



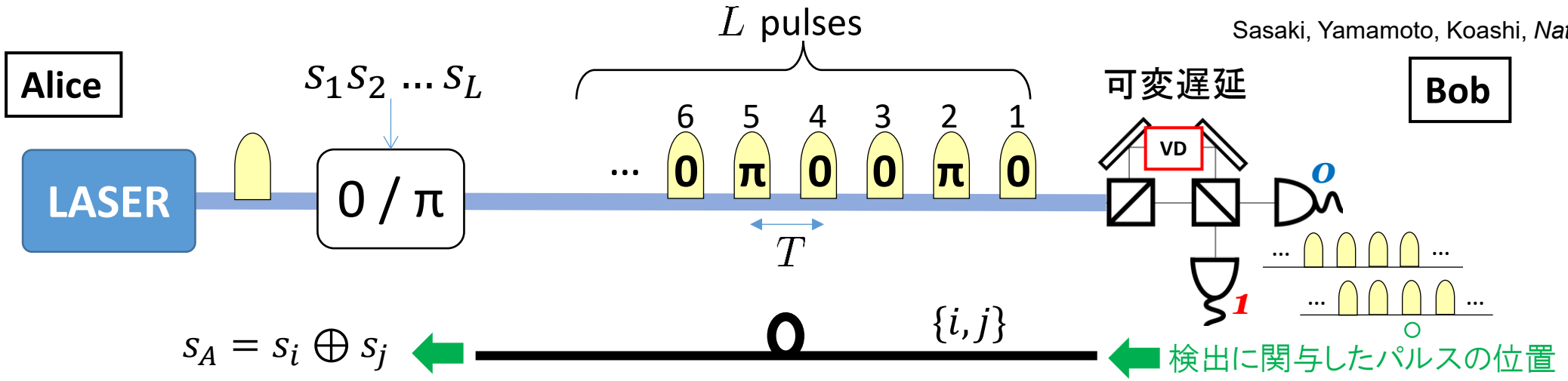




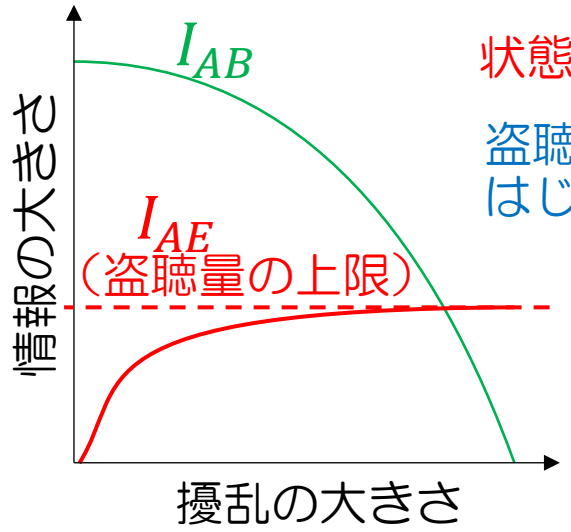
「量子系から情報を取り出すと、状態が変化する」

状態の変化を調べれば、盗聴の程度がわかる

Round-Robin DPS QKD



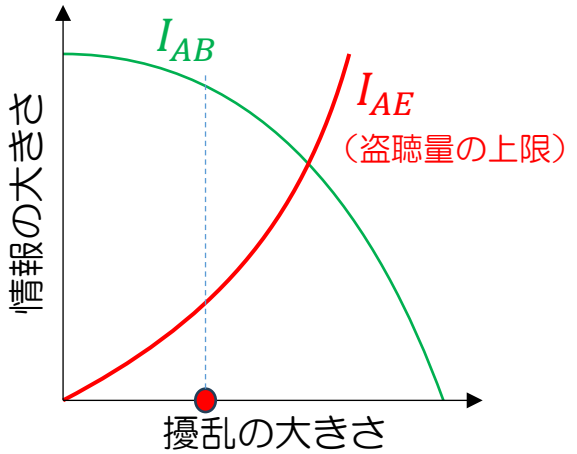
RRDPS QKD



状態の変化は無視しても良い

盗聴量の上限が小さいことが
はじめからわかっている。

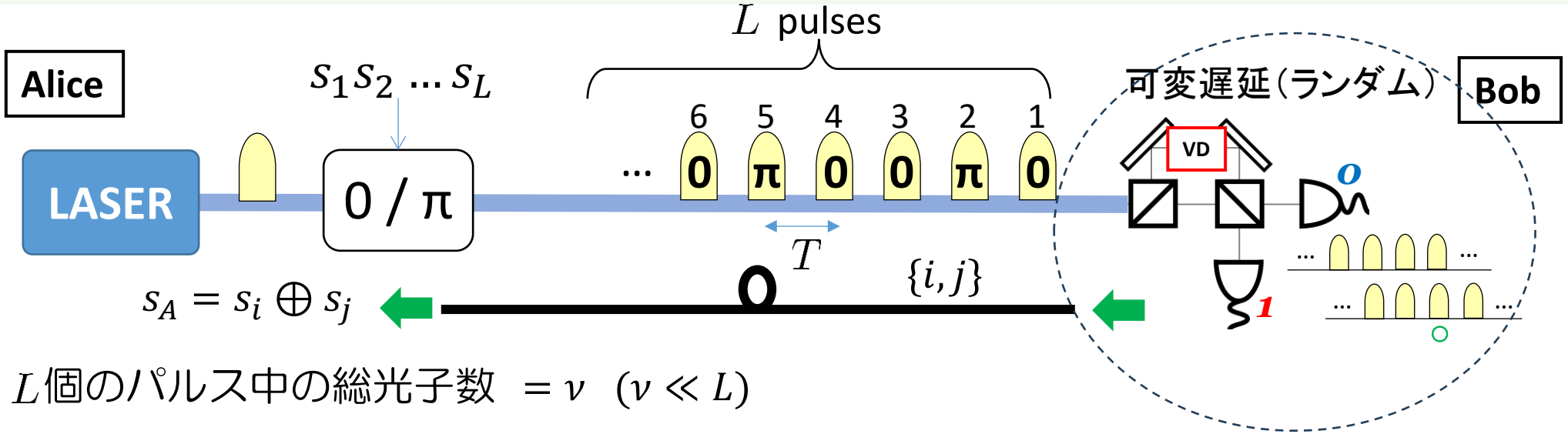
普通のQKD



「量子系から情報を取り出すと、状態が変化する」

状態の変化を調べれば、盗聴の程度がわかる

RRDPS QKDの原理

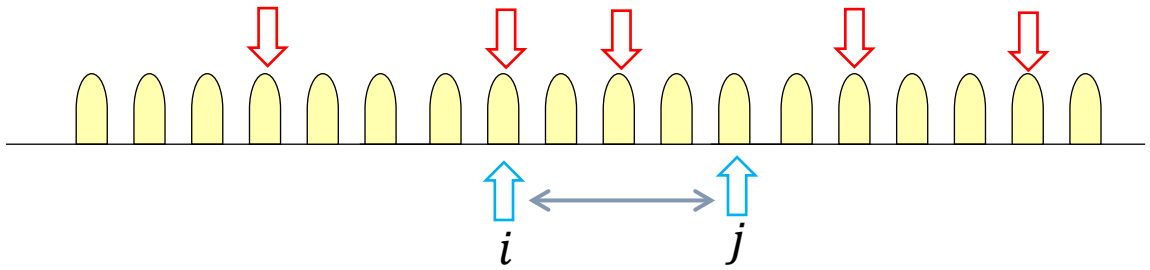


L個のパルス中の総光子数 $= \nu$ $(\nu \ll L)$

Bobは、間隔をランダムに選んでから測定する。

全パルスに1個程度光子がいれば、高い確率で（どこかのペアの）位相差がわかる。

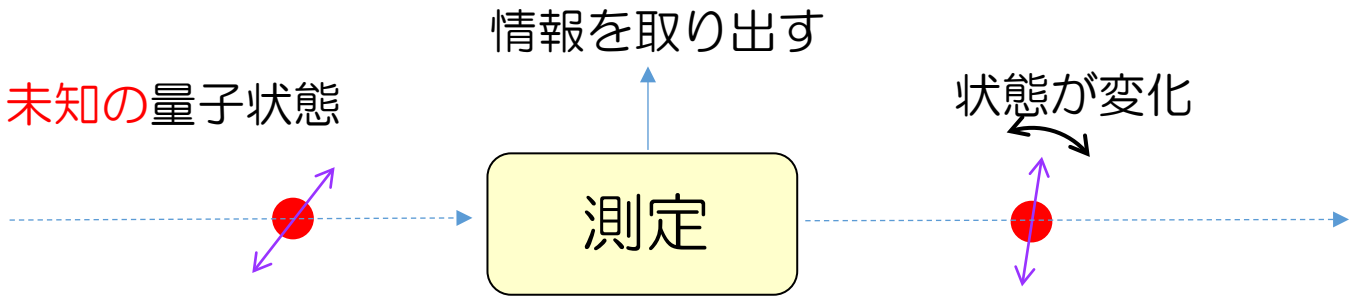
Eveが位相を知っている場所（全体の~ ν/L程度）



間隔はBobがランダムにきめる。

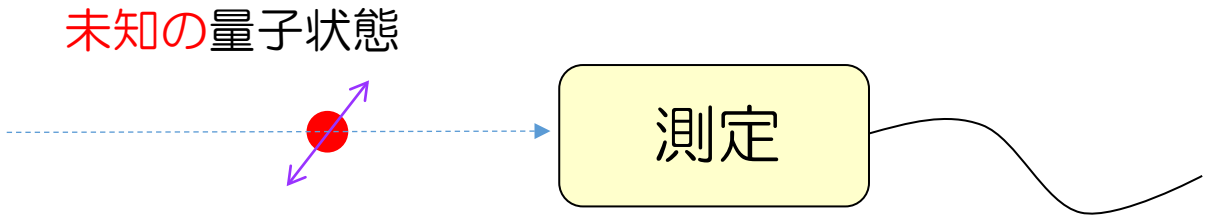
Eveに位相差がわかる確率は~ ν/L程度

RRDPS QKDの原理



通常のQKD

「量子系から情報を取り出すと、状態が変化する」



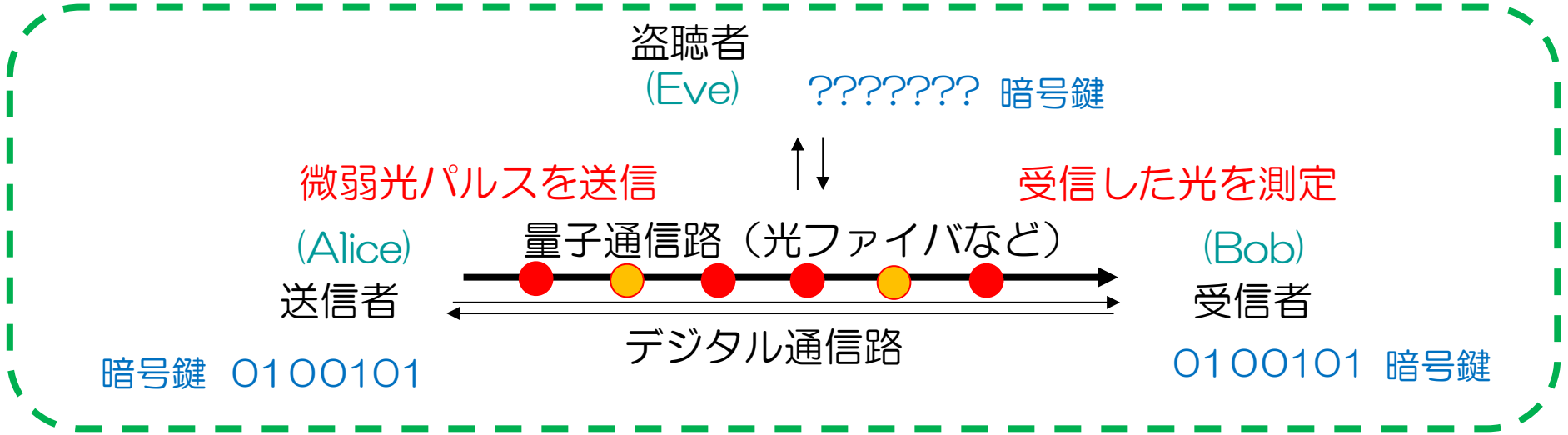
「量子系の中身を測定ですべて知ることはできない」

RRDPS　QKD

コヒーレントレーザーパルス列
可変遅延干渉計

量子力学には、もっと直接的に情報を隠す場所があった

QKDの実際



n_{fin}ビットまで短縮すれば、暗号鍵は安全である。

このような主張は、通信時間が無限大の極限（漸近極限）でしか意味がない。

実際のQKD装置のセキュリティで意味があるのは

n_{fin}ビットまで短縮すれば、暗号鍵はϵ-secureである。

n_{fin}の値は通信時間やϵの値にも依存する

通信したデータから、
シフト鍵を作り、エラー訂正
（同じビット列を共有）

01011001001　n_{rec}ビット

⇩ Privacy Amplification

暗号鍵 0100101　n_{fin}ビット

QKDの実際

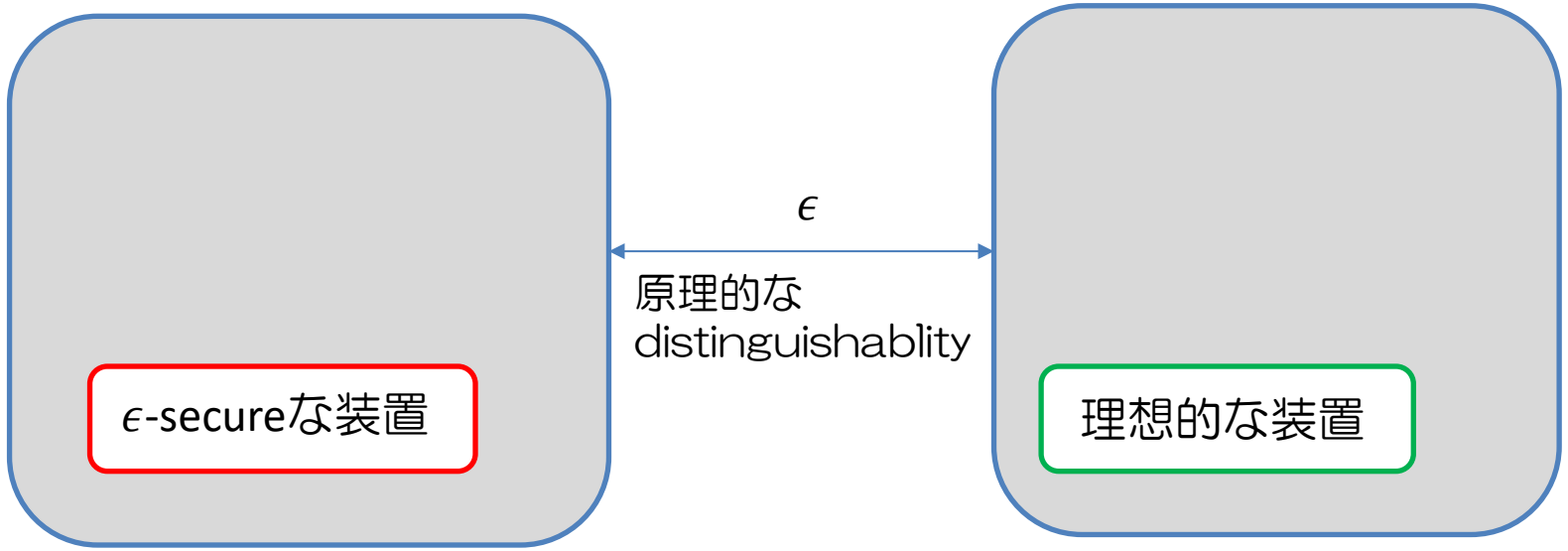
暗号鍵はϵ-secureである。

$$\frac{1}{2}\left\|\rho_{\mathrm{ABE}}^{\mathrm{ideal}}-\rho_{\mathrm{ABE}}^{\mathrm{actual}}\right\|_1 \leq \epsilon$$

ϵの値が明確な意味を持つ

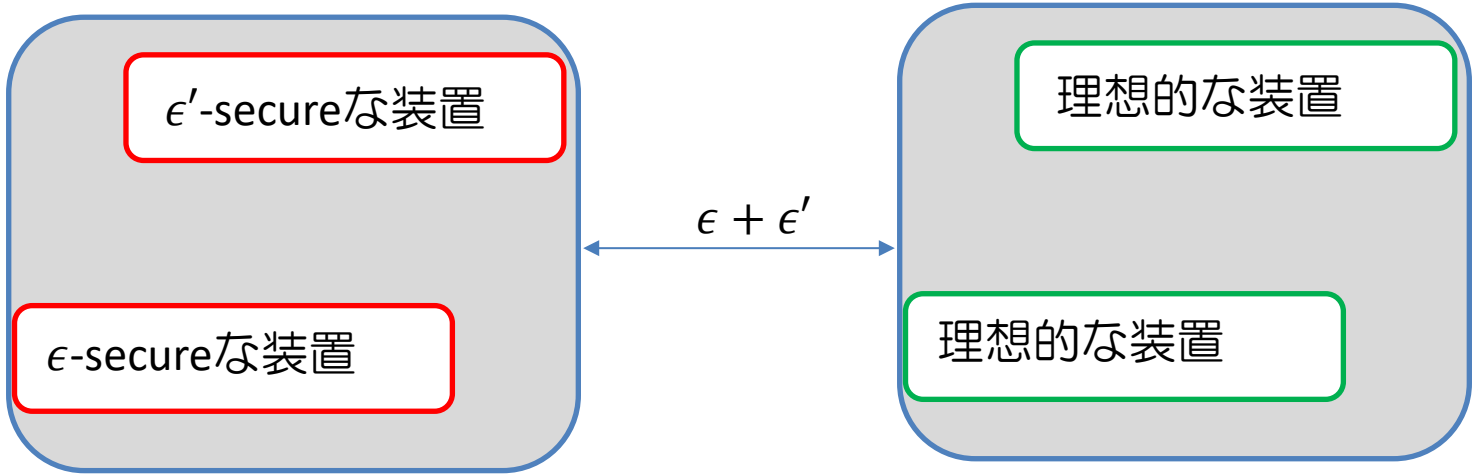
$$|\mathrm{Prob}(event|\ \mathrm{actual}\ )-\mathrm{Prob}(event|\ \mathrm{ideal}\ )| \leq \epsilon$$

$event$: 暗号装置を使って防ごうとしている悪い出来事

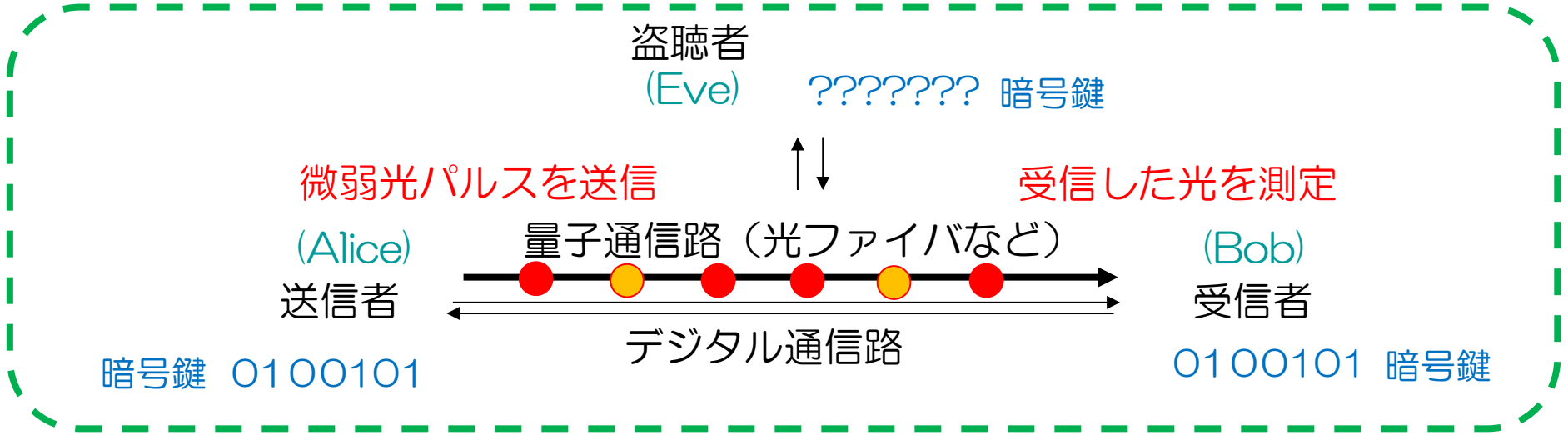


$\epsilon = 10^{-10}$の解釈：
「完璧な暗号装置を使えば防げたはずの出来事が、この暗号装置を使ったことが原因で起きた」と見なせるような事態は、100億分の１の確率でしか起きない。

汎用的結合可能性を持つ
(Universal Composability)



QKDの実際



QKDの有限長セキュリティの証明：

n_{fin}ビットまで短縮すれば、暗号鍵はϵ-secureである。

これが成り立つように、通信データの値とϵの値とから、なるべく大きいn_{fin}を定める手続きを導く。

・盗聴者の攻撃はiidとは限らない（コヒーレント攻撃）

・ホモダイン検出器を用いるCV-QKDは、測定値が連続値で、関与するHilbert空間の次元が無限大なので、有限長の解析が難しい

通信したデータから、
シフト鍵を作り、エラー訂正
（同じビット列を共有）

0101100 1001　n_{rec}ビット

↓ Privacy Amplification

暗号鍵 0100101　n_{fin}ビット

量子力学100周年研究会：量子基礎・量子情報のこれまでとこれから　2025/9/11

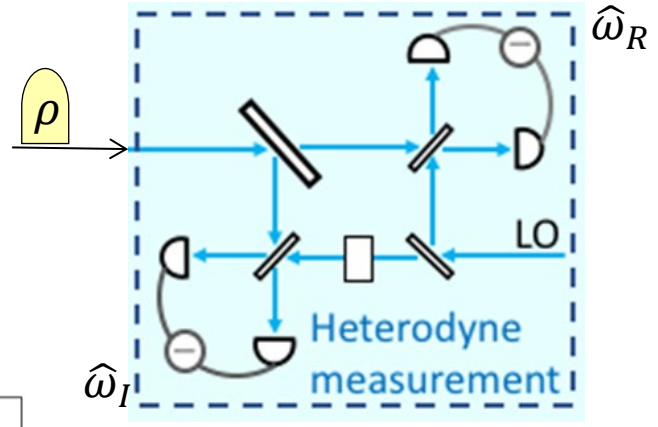
量子暗号のセキュリティ理論から見える量子力学

小芦　雅斗
東京大学 大学院工学系研究科

Promenade:　ＱＫＤの基礎
Movement 1: 量子情報基礎との意外な関り
Promenade:　ＱＫＤの原理
Movement 2: 量子鍵配送の原理の見直し
Promenade:　ＱＫＤの実際
Movement 3: アイデアのRepurposing
Promenade:　ＱＫＤの理論
Movement 4: セキュリテイ証明の２つのアプローチ
Postlude:　まとめと雑感

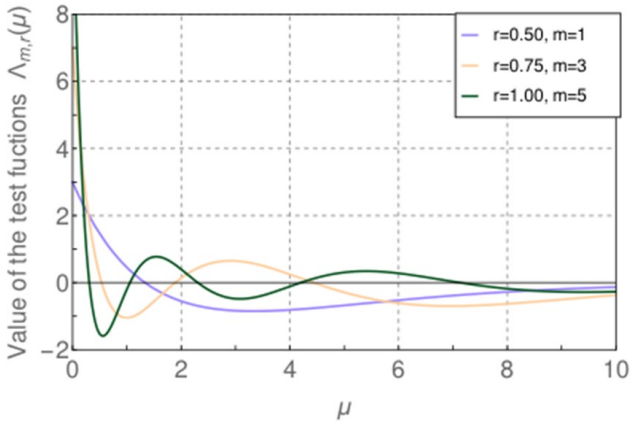
アイデアのRepurposing：その1

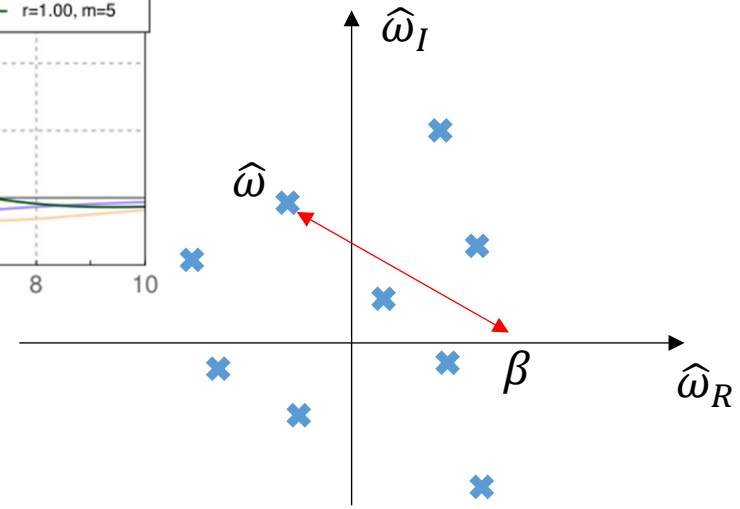
量子計算の計算資源となるような非古典的な光の状態
（multi-mode squeezed states）
がちゃんと作れているかを、簡単に使える道具（ホモダイン/ヘテロダイン検出器）で厳密に検証したい



iidが保証されている場合： Aolita, Gogolin, Kliesch, *et al.*, *Nat Commun* **6**, 8498 (2015).

これをnon-iidに拡張したい





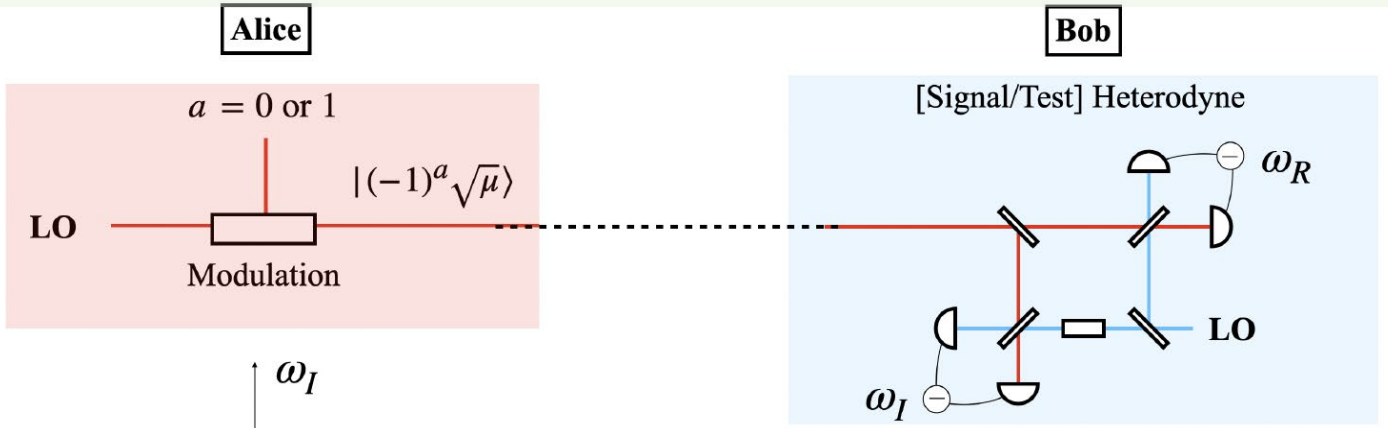
試行錯誤の末、
「ヘテロダイン検出の測定値から、コヒーレント状態とのFidelityの下限の推定量（有界、連続）を構成する手法」
までは出来た。

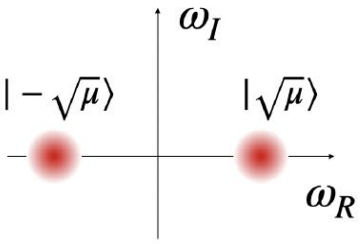
コヒーレント状態では量子計算にならないので、
残念ながらお蔵入り。

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\hat{\omega}-\beta|^2)] \leq \langle\beta|\rho|\beta\rangle$$

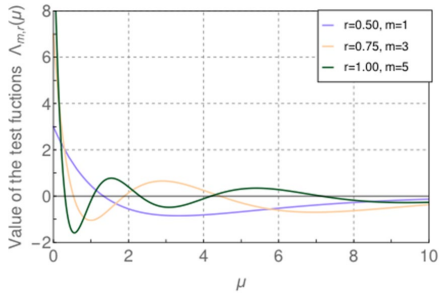
アイデアのRepurposing：その1

CV-QKDにおける状態変化の検知は、コヒーレント状態からどれだけずれているかを推定できれば良い



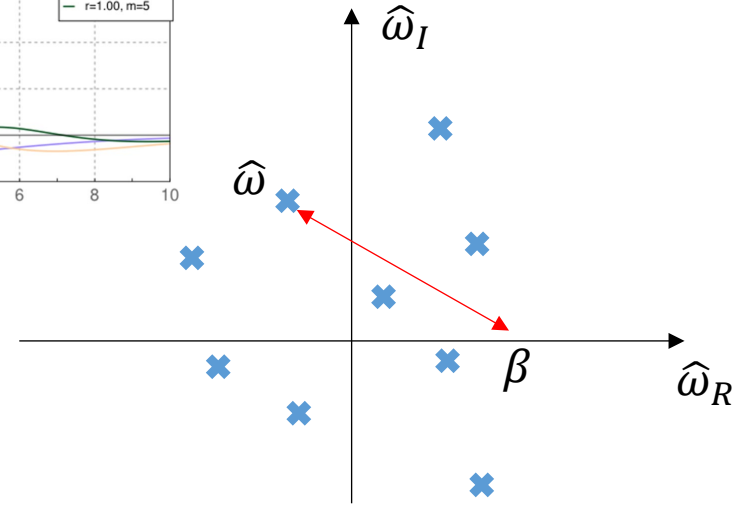


「ヘテロダイン検出の測定値から、コヒーレント状態とのFidelityの下限の推定量（有界、連続）を構成する手法」



デジタル信号処理でCV-QKDの有限長のセキュリティを初めてちゃんと証明できた。

Matsuura, Maeda, Sasaki, Koashi, *Nat. Commun.* **12**, 252 (2021).



量子計算の研究で出てきたアイデア（しかもお蔵入り）が、量子暗号の重要な課題の解決につながった。

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\hat{\omega}-\beta|^2)] \leq \langle\beta|\rho|\beta\rangle$$

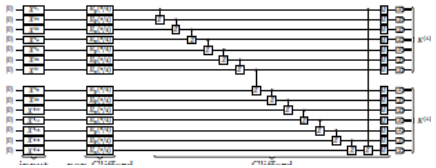
アイデアのRepurposing：その2

- 誤り耐性量子計算（FTQC）のオーバーヘッド

問題のサイズM

論理量子ビット数
$W(M) = O(\mathrm{poly}(M))$

計算したい回路

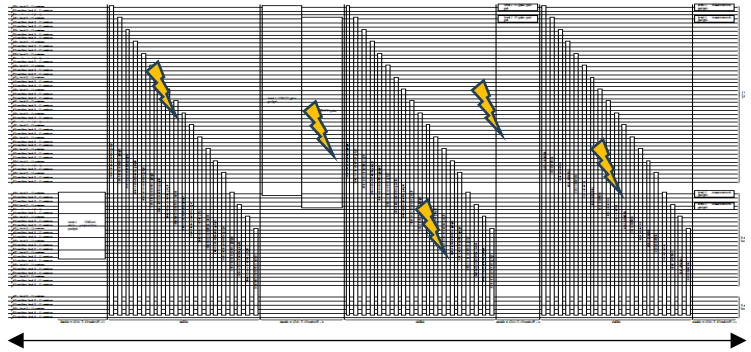


$D(M) = O(\mathrm{poly}(M))$
論理ステップ数

コンパイル

物理量子ビット数
$W(M) \times$???
空間オーバーヘッド
（符号、補助量子ビット）

実際の誤り耐性計算機の回路



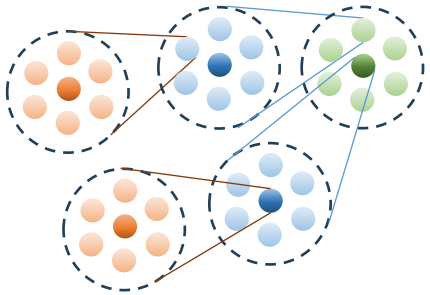
物理ステップ数
$D(M) \times$??? 時間オーバーヘッド
（エラー訂正、論理ゲート演算、魔法状態生成）

アイデアのRepurposing：その2

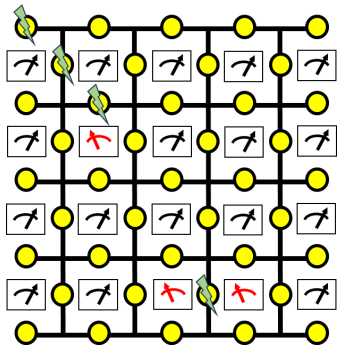
- 誤り耐性量子計算（FTQC)のオーバーヘッド）

Conventional FTQC schemes

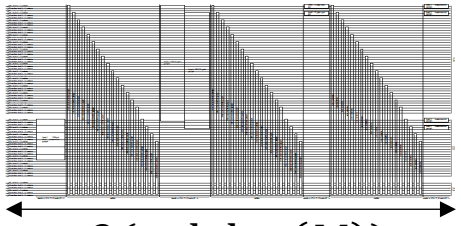
Steane符号の連接



表面符号



空間オーバーヘッド
$O(\mathrm{polylog}(M))$

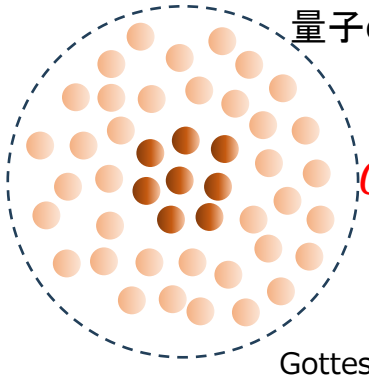


時間オーバーヘッド $O(\mathrm{polylog}(M))$

Recent FTQC schemes

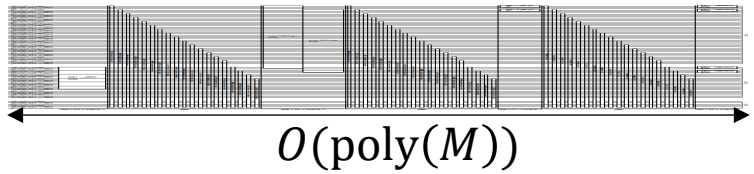
LDPC符号

量子expander符号



空間オーバーヘッドが定数

$O(1)$

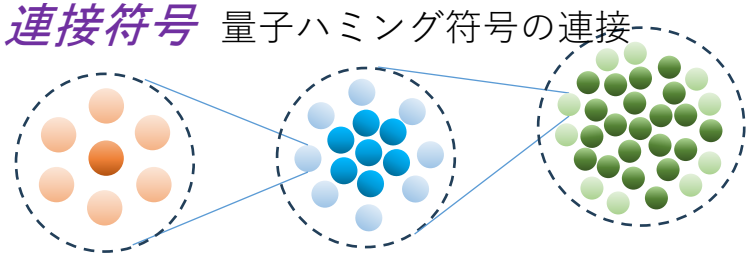


$O(\mathrm{poly}(M))$

時間オーバーヘッドは悪化

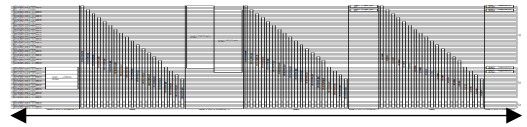
Gottesman, *Quantum Inf. Comput*. **14**, 1338 (2014).
Kovalev, Pryadko, *Phys. Rev.* A **87**, 020304 (2013).
Fawzi, Grospellier, Leverrier, *Commun. ACM* **64**, 106 (2020) [FOCS 2018].

連接符号 量子ハミング符号の連接



空間オーバーヘッドが定数

$O(1)$



$\exp O(\log^2(\log M))$

時間オーバーヘッドは悪化

Yamasaki and Koashi, *Nat. Phys.* **20**, 247 (2024).

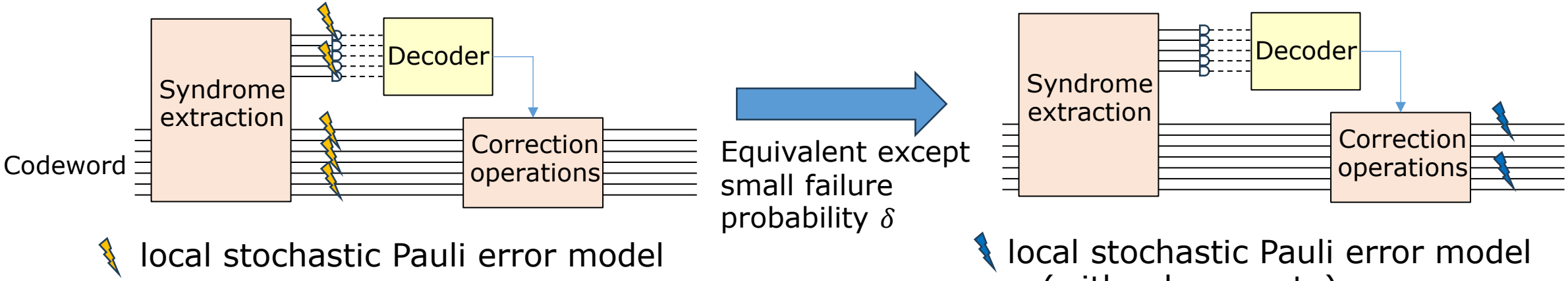
この時間空間トレードオフは本質的なものか？
（LDPC符号FTQCの時間オーバーヘッドはもっと短縮できそう）

アイデアのRepurposing：その2

- LDPC符号のエラー訂正

Property of single-shot decoding algorism:

Fawzi, Grospellier, Leverrier, *Commun. ACM* **64**, 106 (2020) [FOCS 2018].
Grospellier, *Thesis* (2019).



local stochastic Pauli error model

local stochastic Pauli error model (with a lower rate)

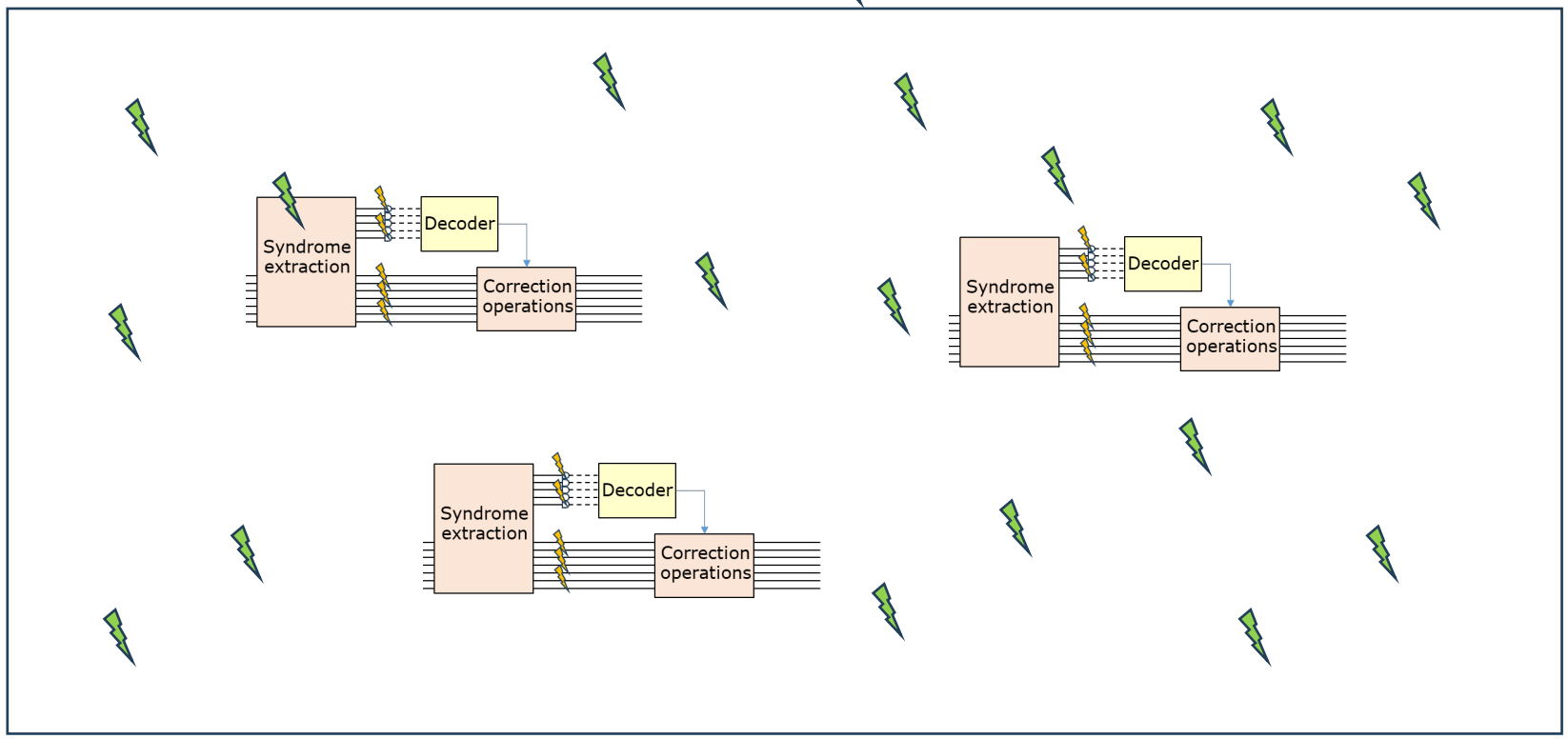
- FTQCにおけるLDPC符号のエラー訂正は、単に成功、失敗ではなく、エラーの数が減るという定量的な性能が重要
- シンドロームから訂正操作を決めるdecoderの中身は複雑だが、標準的なエラーモデルでの訂正性能が定理として与えられている。

ところが…

アイデアのRepurposing：その2

Full FTQC circuit

local stochastic Pauli error model



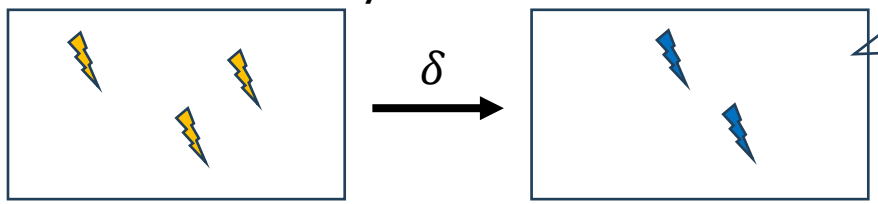
- FTQC回路全体の計算失敗確率が小さいことを解析的に証明したい。（しきい値定理など）
- ところが、エラー訂正の定理を組み合わせても全体の性能が評価できない困難に遭遇
  （部分回路は、全体回路と同一の誤りのモデルには従わない、という性質が原因）

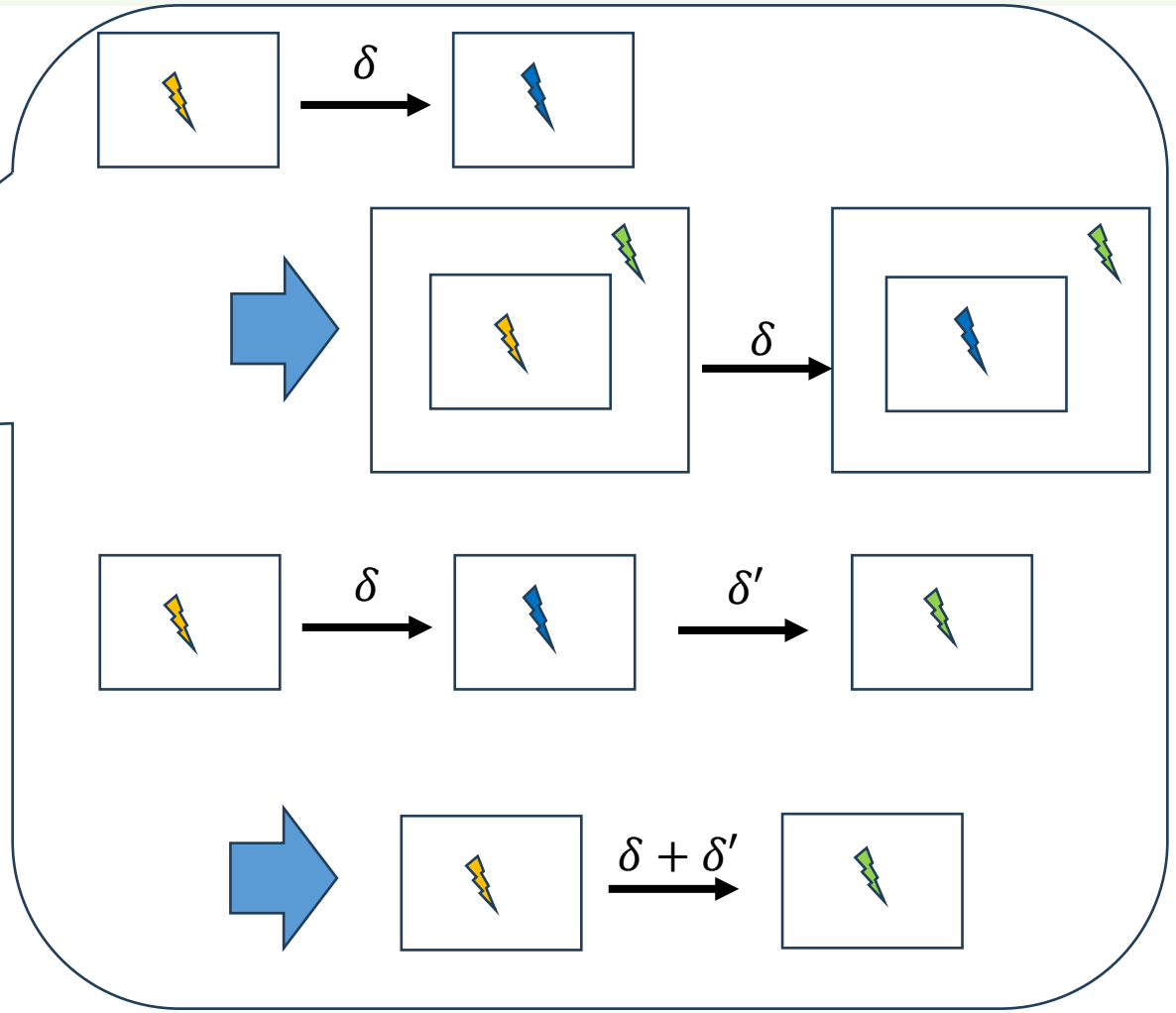
アイデアのRepurposing：その2

- 部分回路のComposableな還元ルール

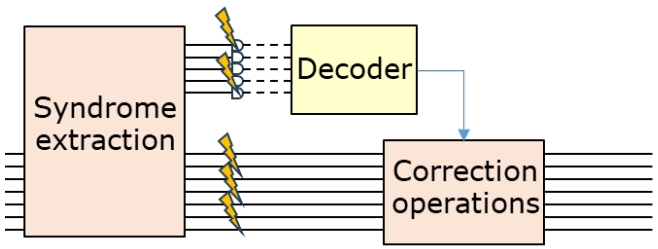
QKDのϵ-securityの考え方を借りて来る

Def: δ-reducibility

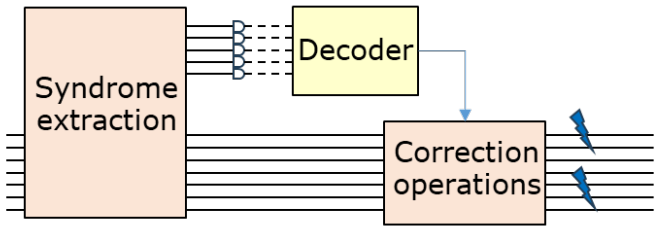




既知の定理を微修正
すれば満たす

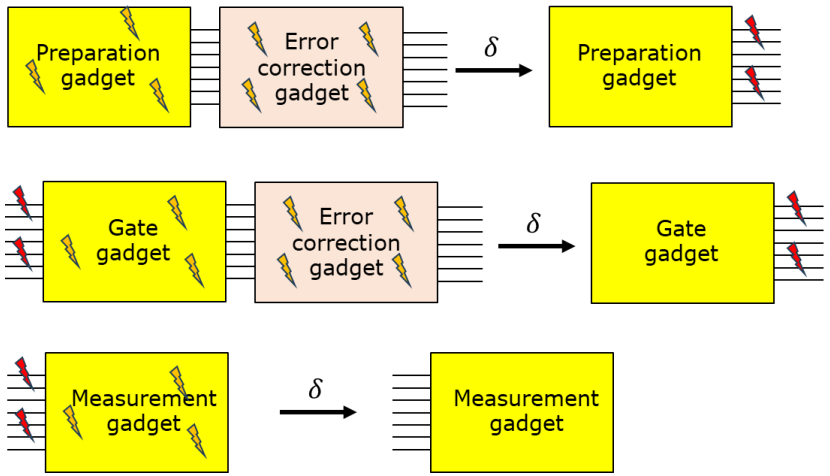


Equivalent except small failure probability δ

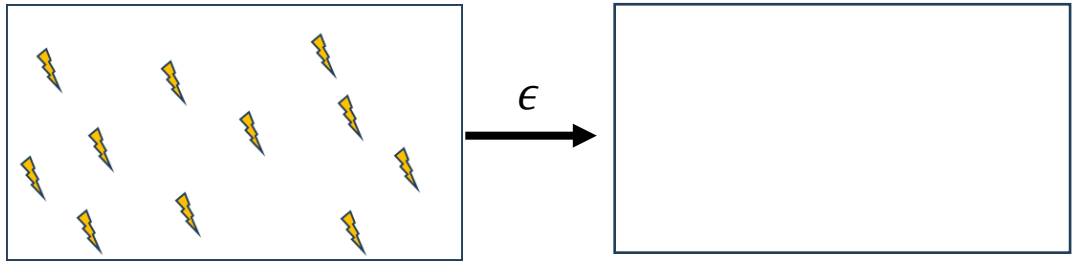


アイデアのRepurposing：その2

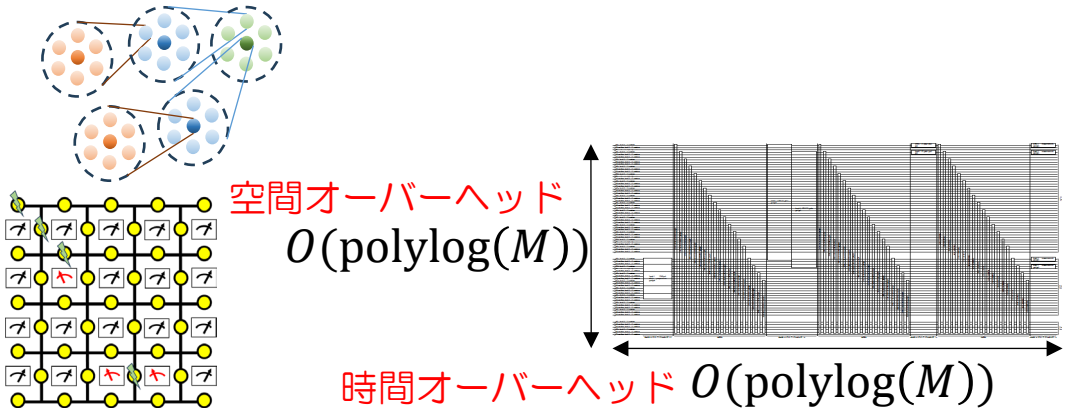
FTQC回路に登場する部分回路について
δ-reducibilityが成立するように設計すれば



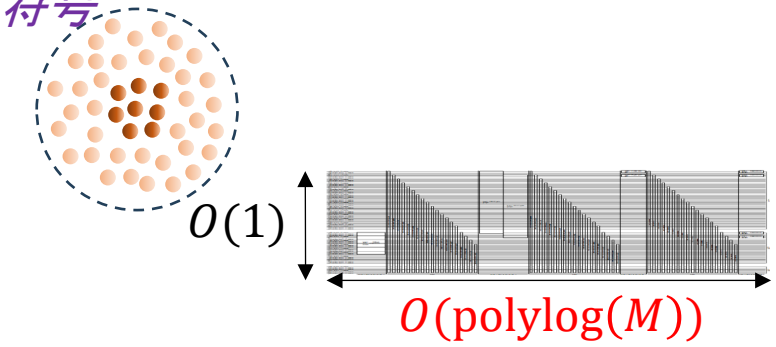
FTQC回路全体の計算失敗確率は自明



$\epsilon = \delta \times$(部分回路の数)



LDPC符号

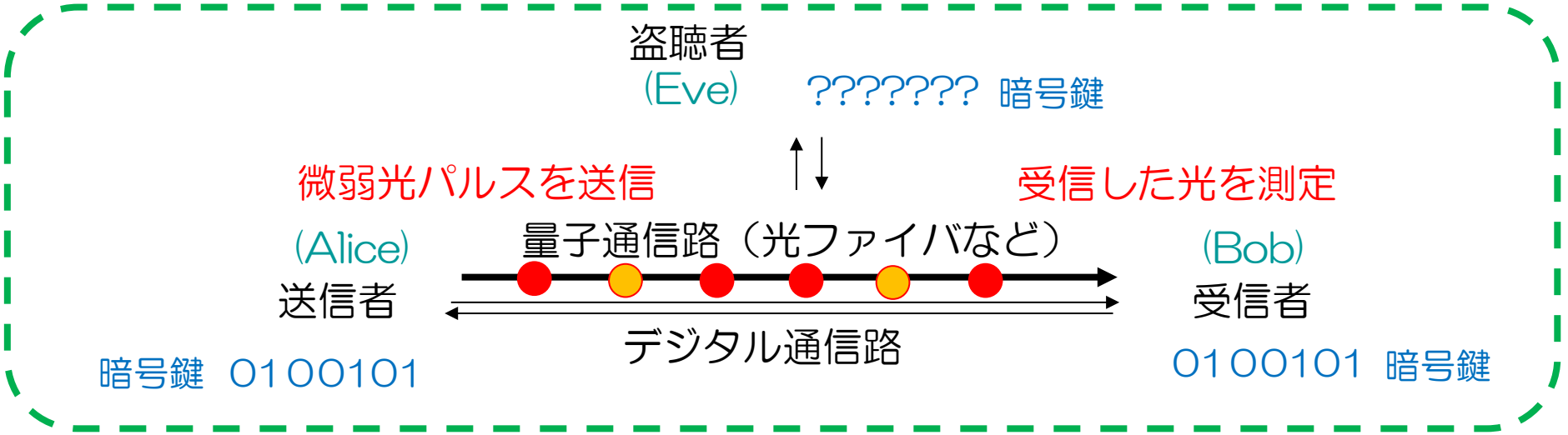


時間空間トレードオフを解消

Tamiya, Koashi, Yamasaki, arXiv:2411.03683.

量子暗号の標準的なアイデアが、量子計算の重要な課題の解決に（密かに）一役買った。

QKDの理論



QKDの有限長セキュリティの証明：

n_{fin}ビットまで短縮すれば、暗号鍵はϵ-secureである。

これが成り立つように、通信データの値とϵの値とから、なるべく大きいn_{fin}を定める手続きを導く。

具体的にはどうやって証明するのか？

通信したデータから、
シフト鍵を作り、エラー訂正
（同じビット列を共有）

01011001001　n_{rec}ビット

↓ Privacy Amplification

暗号鍵 0100101　n_{fin}ビット

QKDの理論

n_{fin}ビットまで短縮すれば、暗号鍵はϵ-secureである。

$$\frac{1}{2}\left\|\rho_{\mathrm{ABE}}^{\mathrm{ideal}}-\rho_{\mathrm{ABE}}^{\mathrm{actual}}\right\|_1 \leq \epsilon$$

理想的な暗号鍵の性質

- Secret　鍵の情報が漏洩していない
- Uniformly distributed　鍵の値の分布が一様
- Identical　送受信者の鍵が一致

Secrecy (for Alice)

$$\frac{1}{2}\left\|\rho_{\mathrm{AE}}^{\mathrm{ideal}}-\rho_{\mathrm{AE}}^{\mathrm{actual}}\right\|_1 \leq \epsilon' \quad (\epsilon'\text{-secret})$$

Correctness

$$\mathrm{Prob}(z \neq z') \leq \epsilon'' \quad (\epsilon''\text{-correct})$$

こちらがセキュリティ証明の本丸

Aliceの暗号鍵が一様分布で漏洩がないことを証明する。Bobは忘れてよい。

With $\epsilon = \epsilon' + \epsilon''$

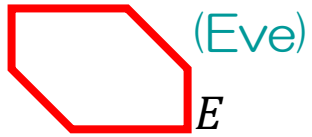
$$\frac{1}{2}\left\|\rho_{\mathrm{ABE}}^{\mathrm{ideal}}-\rho_{\mathrm{ABE}}^{\mathrm{actual}}\right\|_1 \leq \epsilon \quad (\epsilon\text{-secure})$$

QKDの理論

n_{fin}ビットまで短縮すれば、暗号鍵はϵ-secretである。

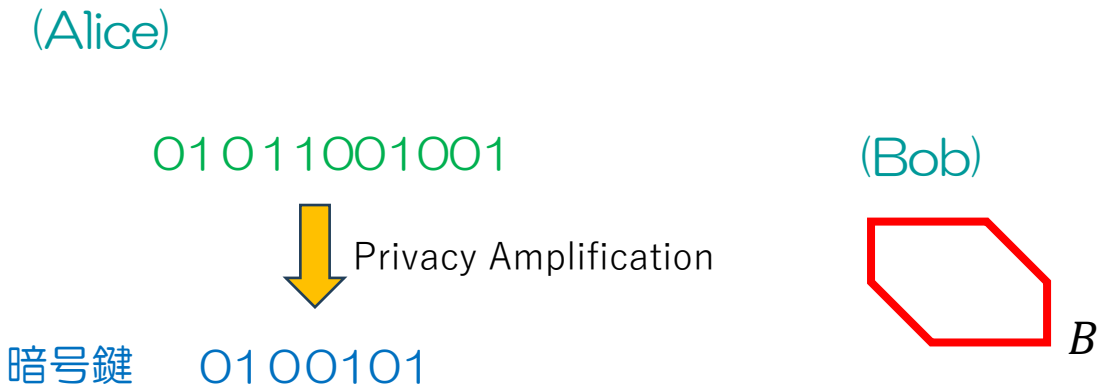
$$\frac{1}{2}\left\|\rho_{\mathrm{AE}}^{\mathrm{ideal}}-\rho_{\mathrm{AE}}^{\mathrm{actual}}\right\|_1 \leq \epsilon$$

QKDの有限長セキュリティ証明の２つのアプローチ



Leftover hashing lemma: Renner (2005)

AliceとEveの相関に着目し、Privacy Amplification で相関が切れることを直接証明する



Phase-error correction: Mayers (1996) Lo-Chau (1999) Shor-Preskill (2000) Koashi (2009)

AliceとBobの相関に着目し、 Aliceの暗号鍵と相補的な物理量とBobが完全な相関を持てることを示す

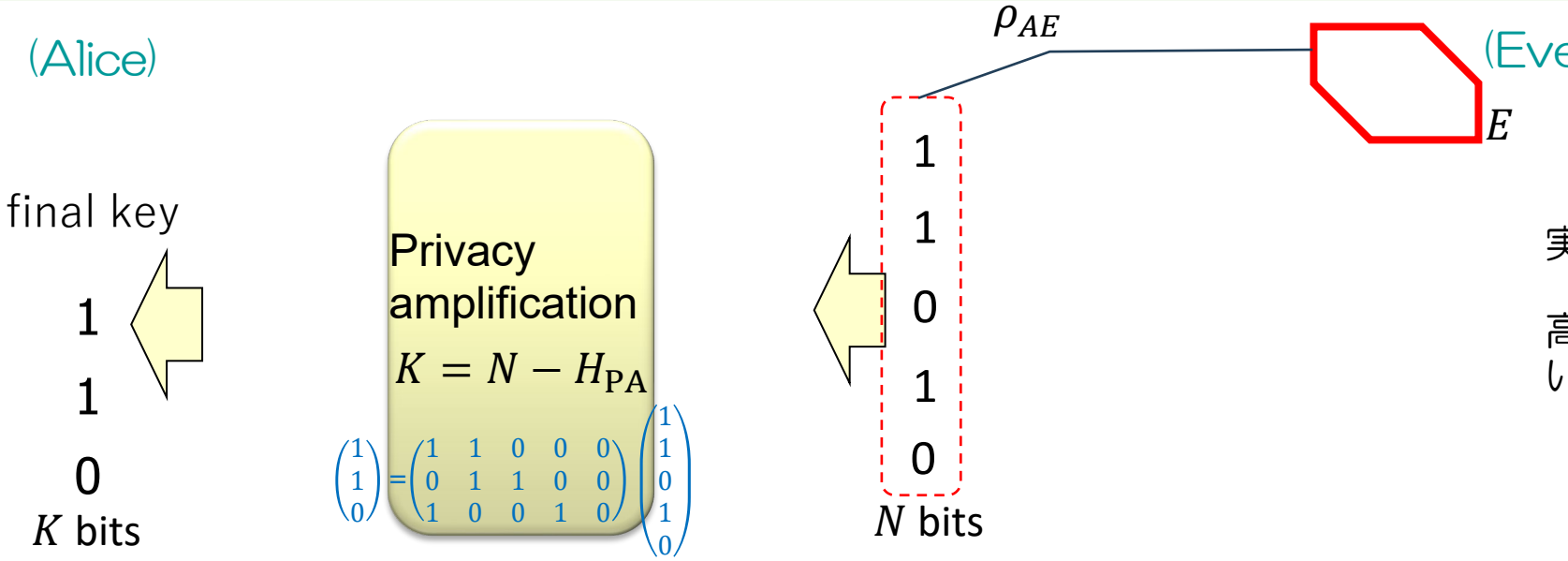
量子力学100周年研究会：量子基礎・量子情報のこれまでとこれから　2025/9/11

量子暗号のセキュリティ理論から見える量子力学

小芦　雅斗
東京大学 大学院工学系研究科

Promenade:　ＱＫＤの基礎
Movement 1: 量子情報基礎との意外な関り
Promenade:　ＱＫＤの原理
Movement 2: 量子鍵配送の原理の見直し
Promenade:　ＱＫＤの実際
Movement 3: アイデアのRepurposing
Promenade:　ＱＫＤの理論
Movement 4: セキュリテイ証明の２つのアプローチ
Postlude:　まとめと雑感

セキュリティ証明の２つのアプローチ

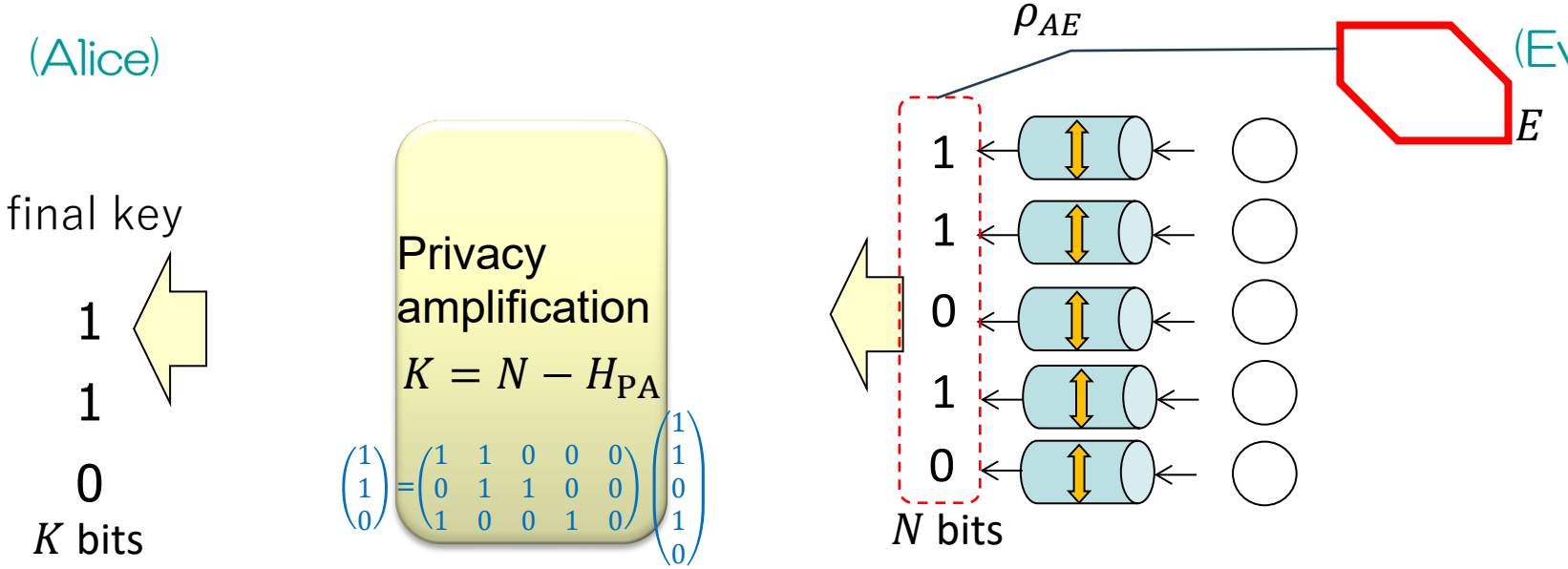


N体の状態ρ_{AE}の
Smooth conditional min entropy
$H_{\min}^{\epsilon}(A|E)_{\rho}$　（の下限）を計算する。

実際に起こる状態変化を追跡している。

高い鍵レートが約束された量が定義されているが、計算が大変。

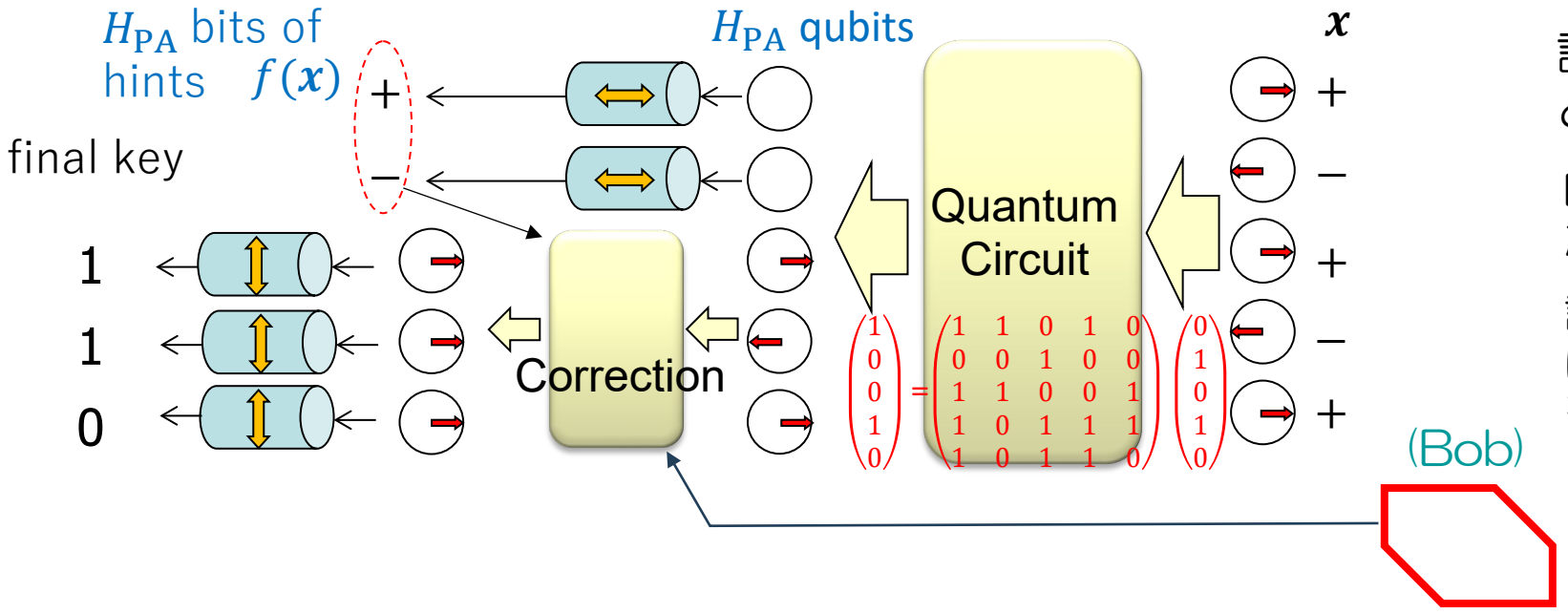
セキュリティ証明の２つのアプローチ



N体の状態ρ_{AE}の
Smooth conditional min entropy
$H_{\min}^{\epsilon}(A|E)_{\rho}$　（の下限）を計算する。

実際に起こる状態変化を追跡している。

高い鍵レートが約束された量が定義されているが、計算が大変。



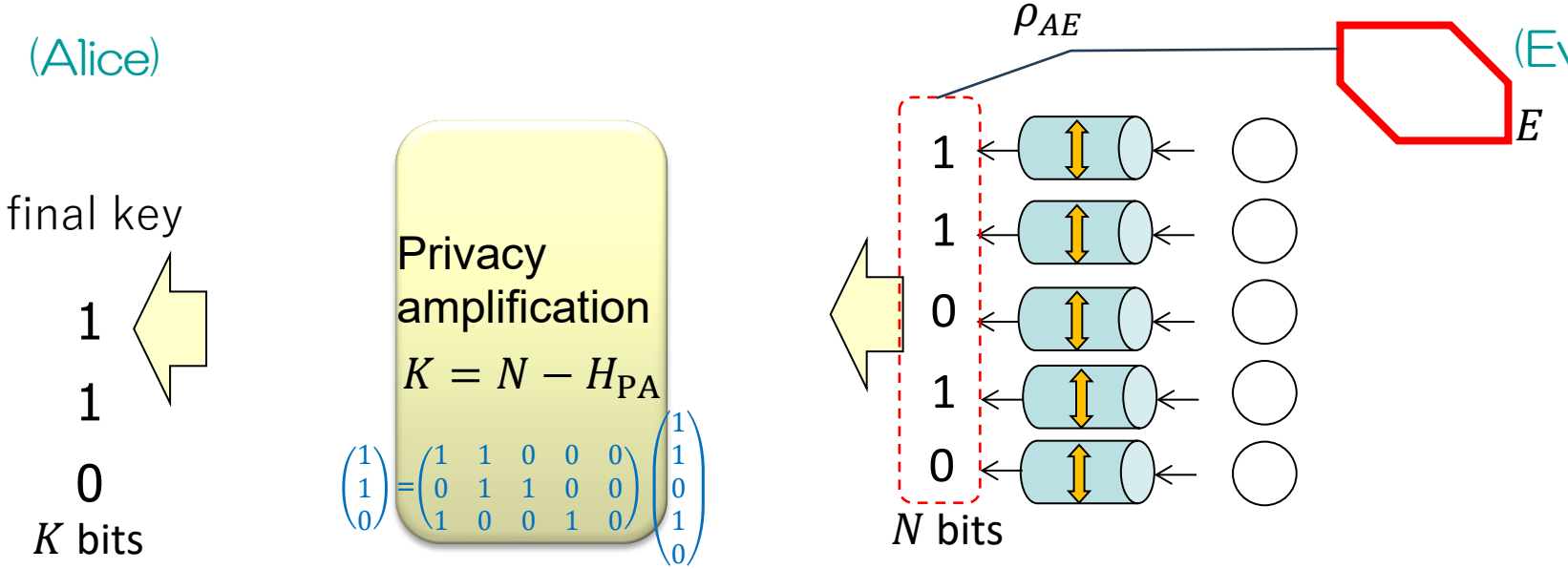
訂正操作後の量子ビットと‘+++++’状態とのFidelity（の下限）を計算する。

Bobが、実際の操作を放棄して訂正に注力した仮想的な場合の状態変化を追跡

訂正操作をひとつ思いついてしまえば計算は簡単だが、高い鍵レートになる訂正操作を思いつけるとは限らない

　漸近極限の鍵レートもOptimalにならない

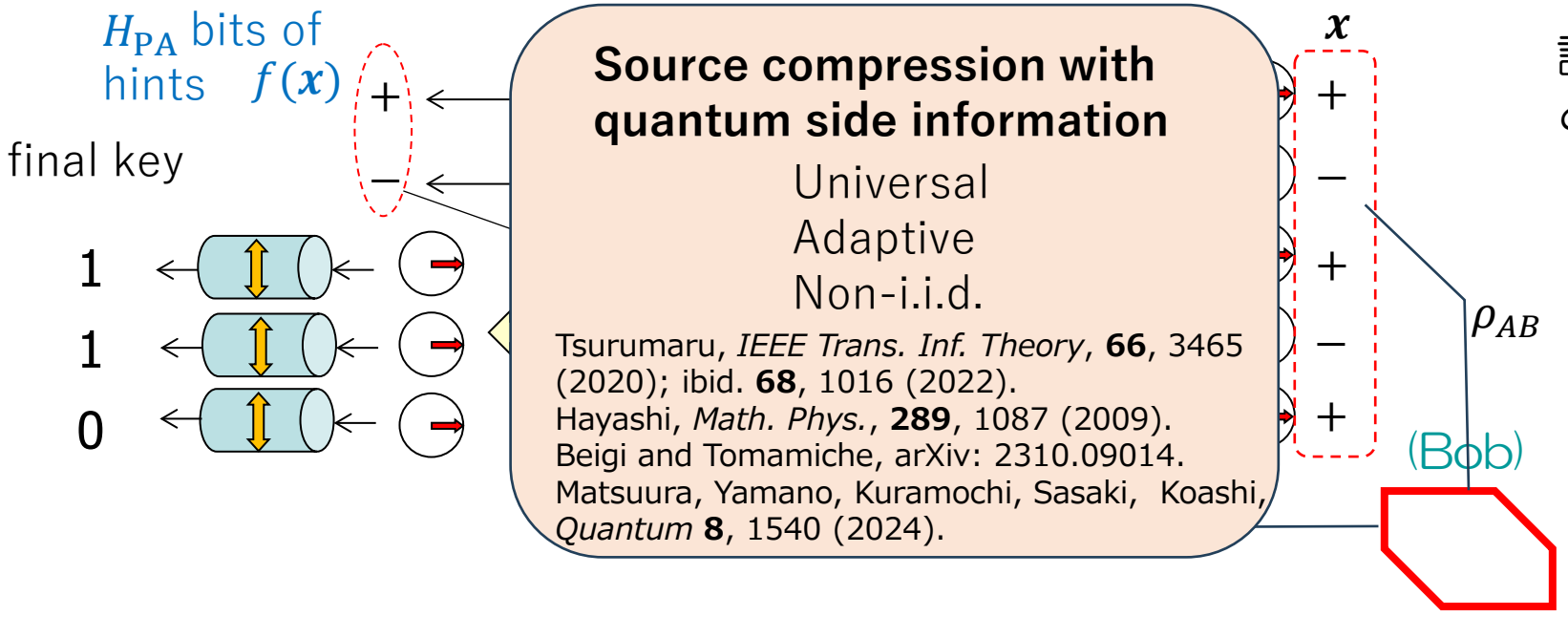
セキュリティ証明の２つのアプローチ



N体の状態ρ_{AE}の
Smooth conditional min entropy
$H_{\min}^{\epsilon}(A|E)_{\rho}$　（の下限）を計算する。

実際に起こる状態変化を追跡している。

高い鍵レートが約束された量が定義されているが、計算が大変。



訂正操作後の量子ビットと‘+++++’状態とのFidelity（の下限）を計算する。

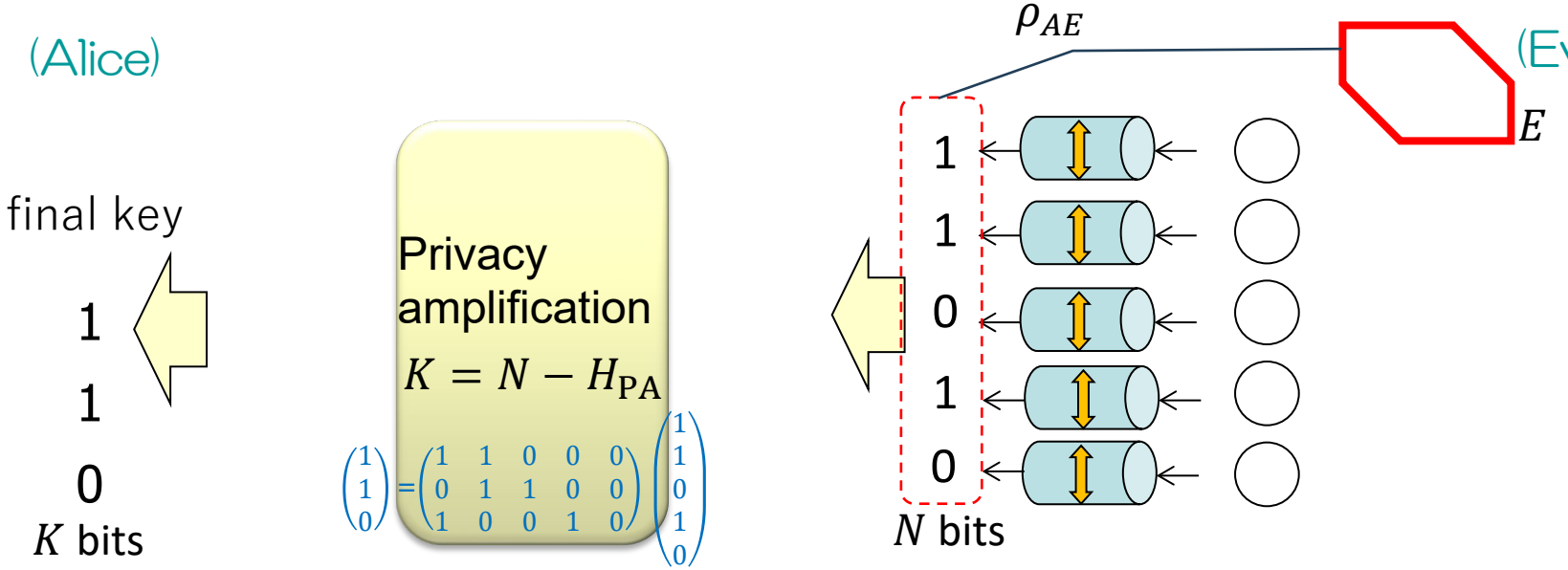
計算量は増えるが、良い訂正操作を系統的に見つける手法

漸近極限の鍵レートがOptimalになる

１体のConditional Renyi entropy
$H_{1-\alpha}^{\uparrow}(A|B)_{\rho}$

Matsuura, Yamano, Kuramochi, Sasaki, Koashi, arXiv:2504.07356.

セキュリティ証明の２つのアプローチ



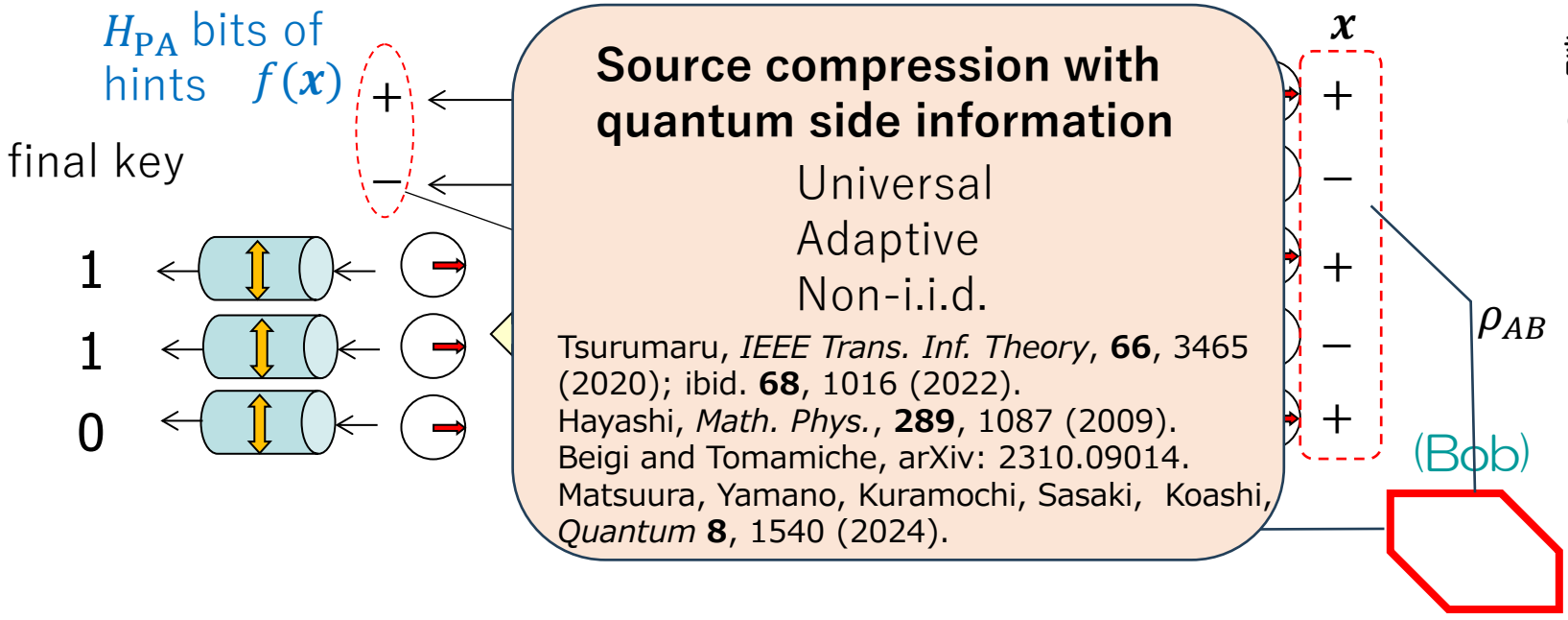
N体の状態ρ_{AE}の
Smooth conditional min entropy
$H_{\min}^{\epsilon}(A|E)_{\rho}$　（の下限）を計算する。

実際に起こる状態変化を追跡している。

高い鍵レートが約束された量が定義されているが、計算が大変。

１体のConditional Renyi entropy
$\tilde{H}_{\alpha}^{\downarrow}(A|E)_{\rho}$

Kamin, Burniston, Tan, arXiv:2504.12248.



訂正操作後の量子ビットと‘+++++’状態とのFidelity（の下限）を計算する。

計算量は増えるが、良い訂正操作を系統的に見つける手法

漸近極限の鍵レートがOptimalになる

１体のConditional Renyi entropy
$H_{1-\alpha}^{\uparrow}(A|B)_{\rho}$

Matsuura, Yamano, Kuramochi, Sasaki, Koashi, arXiv:2504.07356.

まとめと雑感

- QKDの原理の基礎理論が、量子情報の定量化の未解決問題を偶々解決することになった。

- 量子暗号の長距離化を目指した研究が、偶々、全く別原理のQKDが存在することの発見につながった。

- 量子計算の研究で生まれたアイデアが、偶々、 QKDの重要な課題の解決につながった。量子暗号の標準的なアイデアが、偶々、量子計算の重要な課題解決の障害を取り除いた。

- QKDのセキュリティ理論の全く異なる2つのアプローチが、偶々、同じタイミングで同じエントロピー関数に行き着いた。

偶然か否か、については諸説あると思うが、少なくとも言えるのは、
量子力学が底が浅ければこんなことは一切起きなかったはず

量子力学 vs 人類の知恵　は、100年経ったこれからも、
絶妙なバランスで楽しませてくれそう。