量子暗号プロトコルの形式的検証のための Applied Pi-Calculus

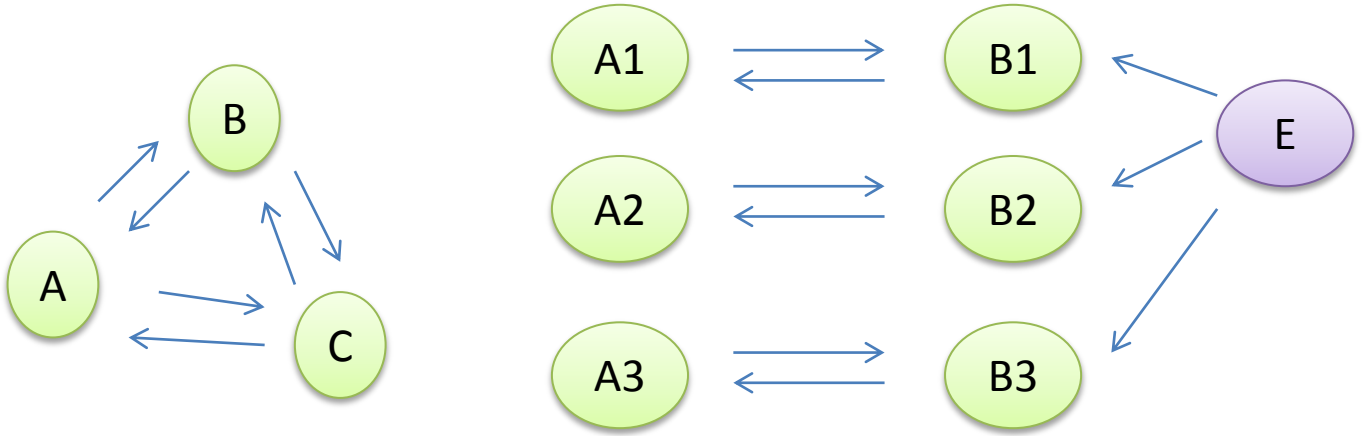
久保田 貴大　　角谷 良彦
東京大学大学院情報理工学系研究科

量子暗号プロトコル

- 量子計算・量子通信を用いて,
  古典暗号より強い安全性を目指している
  - 鍵配送 [BB’84, B’92, …]
  - 紛失通信 [M’96, BBC’92, …]
  - コミットメント [S’99, …]
  - 秘密分散 [HBB’98, …]

研究の動機

- さまざまな種類のプロトコルがある
  - 今後も提案されるかもしれない



- 仕様記述と安全性検証ができるような形式体系が必要

研究の概要

- 量子 Applied Pi-Calculus の提案
  - 確率 Applied Pi-Calculus [GPT'07] を拡張した
    - 量子変数への代入
    - 量子測定の反応関係
    - 観測同値
  - 観測同値を用いて,
    BB84 の安全性証明 [SP'00] を形式的に検証した

Outline

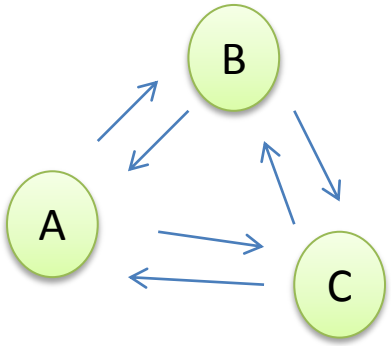
- 量子 Applied Pi-Calculus
- BB84プロトコルの形式的検証
- 関連研究
- 結論
- 今後の課題

Applied Pi-Calculus

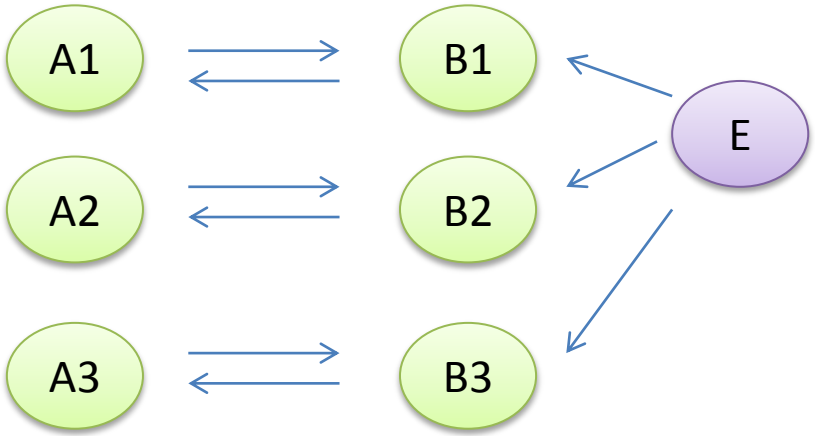
- 複数のエージェント
- メッセージのやりとり
- 非決定性
  [AF'01, GPT'07]

⇒ マルチパーティプロトコルを自然に記述

セッションの並列実行を統一的に記述



A | B | C



A1 | B1 | A2 | B2 | A3 | B3 | E

構文

$$\mathcal{P} \ni P ::= 0 \mid \nu v.P \mid (P_1|P_2) \mid \bar{n}\langle v\rangle.P \mid n(v).P$$
$$\mid \texttt{if } x \texttt{ then } P_1 \texttt{ else } P_0 \mid \{T/x\} \mid \{M/\chi_1, ..., \chi_n\}$$
$$T ::= B \mid \texttt{measure } \chi$$
$$B ::= x \mid 0 \mid 1 \mid B_1 \oplus B_2$$
$$M ::= \chi \mid |0\rangle \mid UM \mid M_1 \otimes M_2$$

- 拡張した部分は
  - 量子変数への代入 $\{M/\chi_1, ..., \chi_n\}$
  - 量子測定 $\texttt{measure } \chi$
  - 量子状態を表す項 M
- 量子変数は複製できない

構造同値関係

$$\equiv : \mathcal{P} \times \mathcal{P}$$

$$P \equiv P \mid 0,\ P_1 \mid P_2 \equiv P_2 \mid P_1,$$
$$(P_1 \mid P_2) \mid P_3 \equiv P_1 \mid (P_2 \mid P_3),\ \nu n.0 \equiv 0,$$
$$\nu n_1.\nu n_2.P \equiv \nu n_2.\nu n_1.P,$$
$$(\nu n.P) \mid Q \equiv \nu n.P \mid Q \text{ if } n \notin \mathtt{FV}(Q),$$
$$\nu v.\{V/v\} \equiv 0,$$
$$\{B/x\}|\{T'/x'\} \equiv \{B/x\}|\{T'\{B/x\}/x'\},$$
$$\{M/\chi_1, ..., \chi_i, ..., \chi_j, ..., \chi_n\} \equiv \{U_{i,j}M/\chi_1, ..., \chi_j, ..., \chi_i, ..., \chi_n\},$$
$$\{M/\chi_1, ..., \chi_n, \chi''_1, ..., \chi''_m\}|\{U'(|0\rangle \otimes ... \otimes |0\rangle \otimes \chi'''_1 \otimes ... \otimes \chi'''_l \otimes \chi_1 \otimes ... \otimes \chi_n)/\chi'_1, ..., \chi'_k\}$$
$$\equiv \{(U' \otimes 1)(|0\rangle \otimes ...|0\rangle \otimes \chi'''_1 \otimes ... \otimes \chi'''_l \otimes M)/\chi'_1, ..., \chi'_k, \chi''_1, ..., \chi''_m\},$$

反応関係 (状態遷移)

$$\rightarrow : \mathcal{P}/\equiv \times \Delta(\mathcal{P}/\equiv)$$

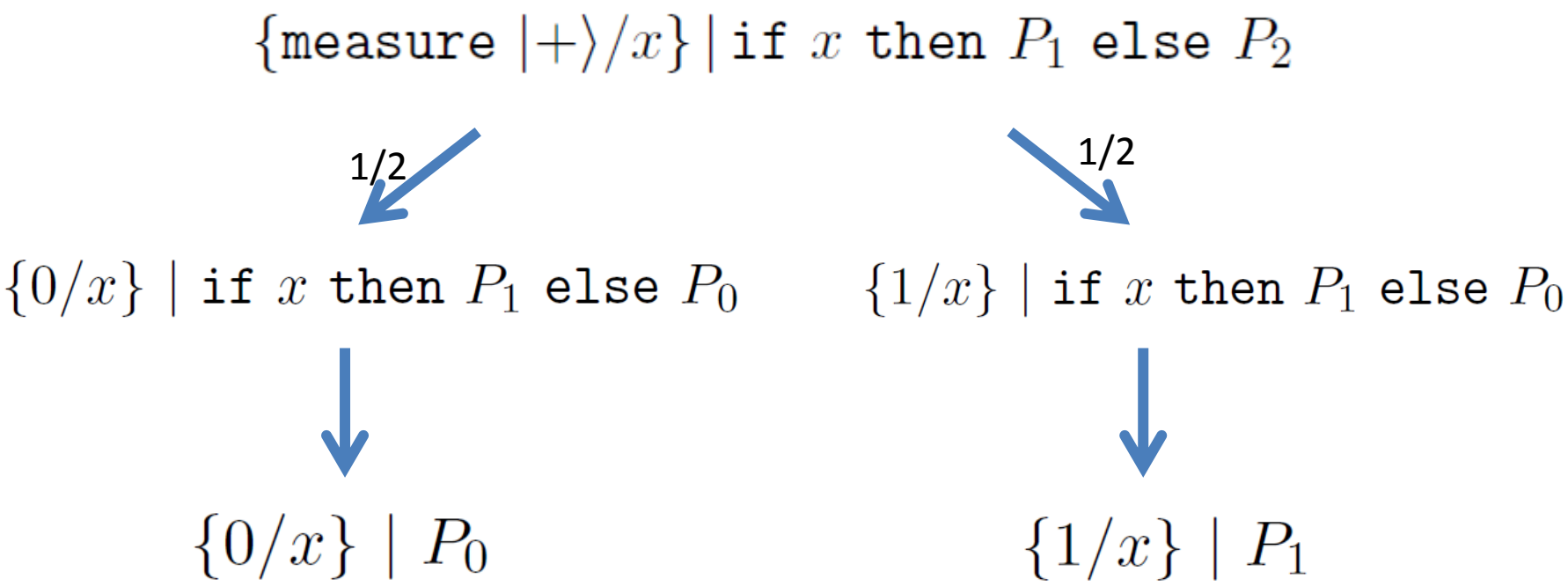
$$\bar{n}\langle v\rangle.P \,|\, n(u).Q \longrightarrow P \,|\, Q\{v/u\}$$
$$\{0/x\} \,|\, (\texttt{if } x \texttt{ then } P_1 \texttt{ else } P_0) \longrightarrow \{0/x\} \,|\, P_0$$
$$\{1/x\} \,|\, (\texttt{if } x \texttt{ then } P_1 \texttt{ else } P_0) \longrightarrow \{1/x\} \,|\, P_1$$

量子測定

$$\{\texttt{measure } \chi \ /x\} \,|\, \{M/\chi, \chi_1, ..., \chi_n\} \longrightarrow \sum_{i\in\{0,1\}} p_i(\{i/x\} \,|\, \{M_i/\chi_1, ..., \chi_n\})$$

ただし $M = \sqrt{p_0}(|0\rangle \otimes M_0) + \sqrt{p_1}(|1\rangle \otimes M_1)$

量子測定の例

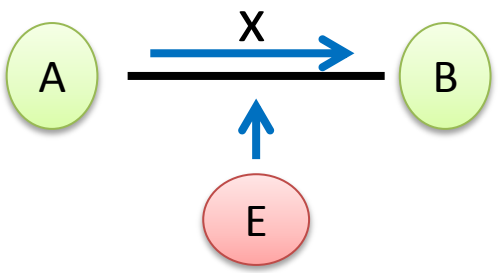

{measure |+⟩/x} | if x then P1 else P2
1/2
1/2
{0/x} | if x then P1 else P0
{1/x} | if x then P1 else P0
{0/x} | P0
{1/x} | P1

安全性の取り扱い方

- 攻撃者の表現
  - 攻撃者は, 任意の評価文脈として表現される

$$C[-] = - \mid (P|C[-]) \mid (C[-]|P) \mid \nu n.C[-]$$

$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E$$



安全性の取り扱い方

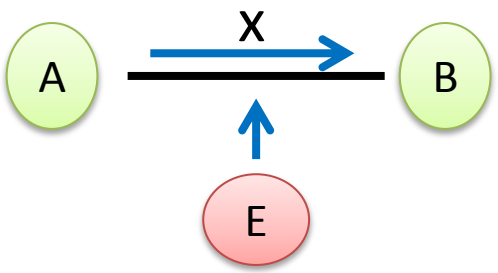
- 攻撃者の表現
  - 攻撃者は, 任意の評価文脈として表現される

$$C[-] = - \mid (P|C[-]) \mid (C[-]|P) \mid \nu n.C[-]$$

$$C[-] = - \mid a(x).E$$

とおくと、

$$C[\bar{a}\langle x\rangle.A \mid a(x).B]$$
$$= \bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E$$



スケジュール

- 通信は決定的でない
  - 攻撃者が任意に遷移を決められるモデル

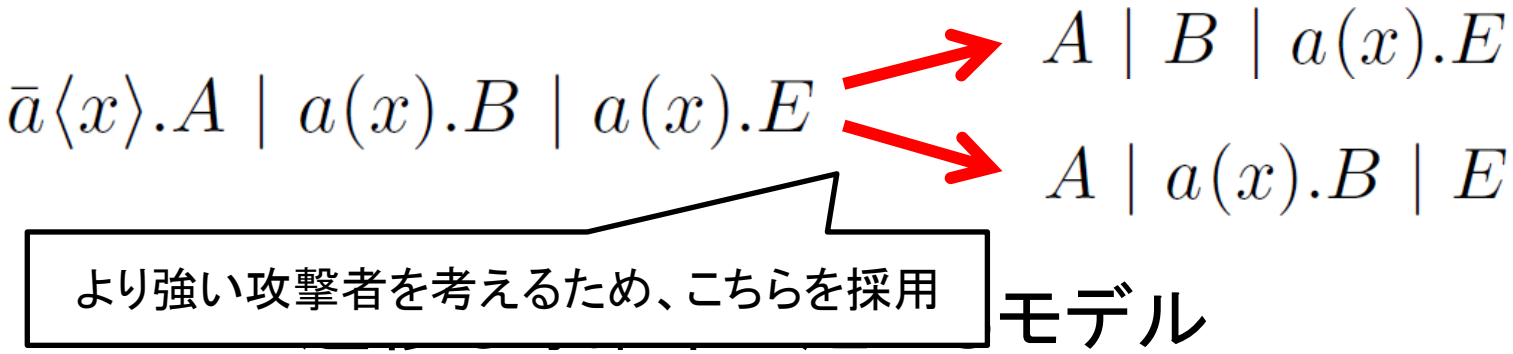
$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid B \mid a(x).E$$
$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid a(x).B \mid E$$

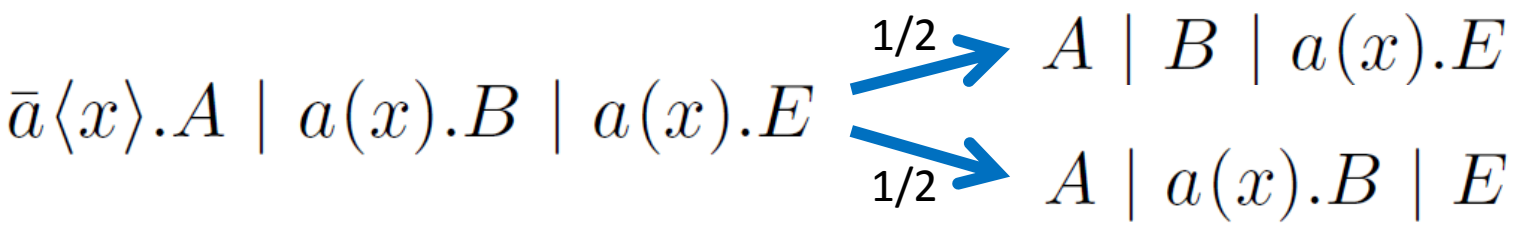
  - どの遷移も等確率で起こるモデル

$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \xrightarrow{1/2} A \mid B \mid a(x).E$$
$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \xrightarrow{1/2} A \mid a(x).B \mid E$$

スケジュール

- 通信は決定的でない
  - 攻撃者が任意に遷移を決められるモデル





スケジュール

- 通信の非決定性

$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid B \mid a(x).E$$
$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid a(x).B \mid E$$

- 観測による確率遷移

スケジュール

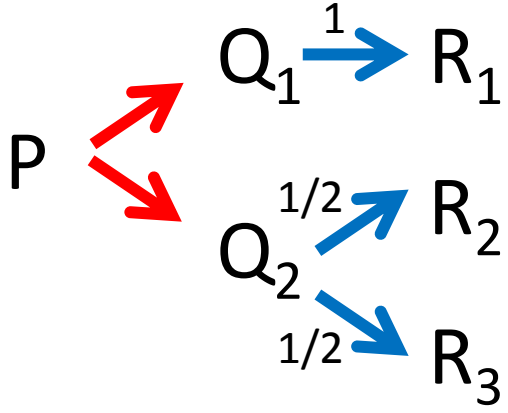
- 通信の非決定性 ← スケジュールを固定する

$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid B \mid a(x).E$$
$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid a(x).B \mid E$$

- 観測による確率遷移 → 固定したスケジュールのもとで確率分布を定める

非決定的な遷移 →

確率遷移 $\xrightarrow{p}$



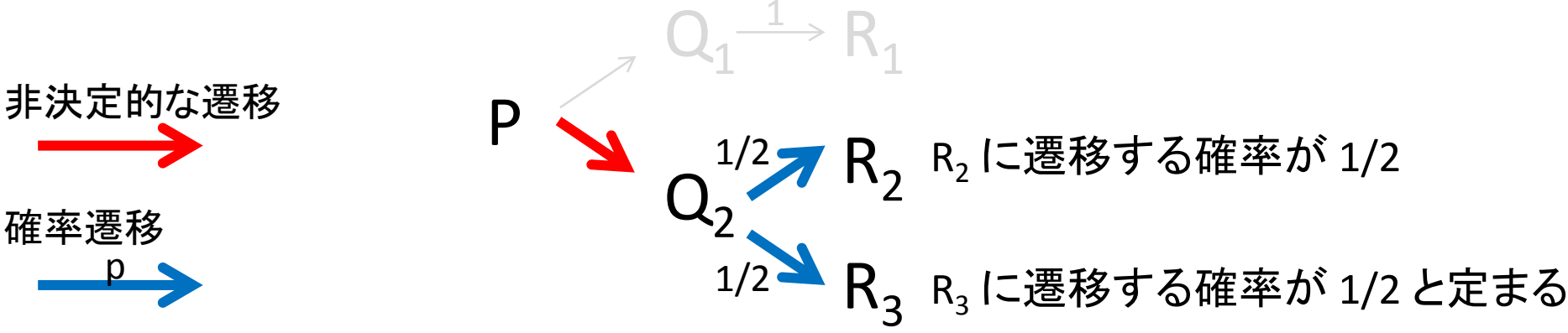
スケジュール

- 通信の非決定性 ← スケジュールを固定する

$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid B \mid a(x).E$$
$$\bar{a}\langle x\rangle.A \mid a(x).B \mid a(x).E \rightarrow A \mid a(x).B \mid E$$

- 観測による確率遷移 → 固定したスケジュールのもとで確率分布を定める

例えば, P は Q_2 と遷移するというスケジュールのもとでは



観測同値

- 確率 Applied Pi-Calculus の観測同値 [GPT'07]
  プロセス A, B が外から見て見分けがつかない
  - プロセス A, B が観測同値であるとは,
    任意の評価文脈 C と スケジュール F に対して,
    あるスケジュール F' が存在して,
    任意のチャネル a について
    C[A] が スケジュール F のもとで a にメッセージを送信する確率と
    C[B] が スケジュール F' のもとで a にメッセージを送信する確率が等しいことである.

観測同値

- 確率 Applied Pi-Calculus の観測同値 [GPT'07]
  プロセス A, B が外から見て見分けがつかない
  - プロセス A, B が観測同値であるとは,
    任意の評価文脈 C と スケジュール F に対して,
    あるスケジュール F' が存在して,
    任意のチャネル a について
    C[A] が スケジュール F のもとで a にメッセージを送信する確率と
    C[B] が スケジュール F' のもとで a にメッセージを送信する確率が等しいことである.

- しかし, 任意のスケジュールを許すと,
  量子力学に反する例ができてしまう

区別できない量子状態

- 量子の純粋状態の確率分布を混合状態という
- 混合状態は密度行列で表され,
  同じ密度行列で表現される混合状態は,
  区別することができない

区別できない量子状態

- σ と σ′ は純粋状態の確率分布で,
  $\sigma(|0\rangle) = \frac{1}{3}, \quad \sigma(|1\rangle) = \frac{2}{3}$ $\qquad$ $\sigma'(|\psi\rangle) = \frac{1}{2}, \quad \sigma'(|\phi\rangle) = \frac{1}{2}$
  であるとする
  ここで, $|\psi\rangle = \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle, \quad |\phi\rangle = \sqrt{\frac{1}{3}}|0\rangle - \sqrt{\frac{2}{3}}|1\rangle$ とする.

- どちらの分布も同じ密度行列で表現される.
  つまり, σ と σ′ は区別できない

量子力学に反する例

$\sigma(|0\rangle) = \frac{1}{3},\ \ \sigma(|1\rangle) = \frac{2}{3}$

P

1/3

2/3

$\{|0\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

$\{|1\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

区別できない
はず

$\sigma'(|\psi\rangle) = \frac{1}{2},\ \ \sigma'(|\phi\rangle) = \frac{1}{2}$

P’

1/2

1/2

$\{|\psi\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

$\{|\phi\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

P と P’ は観測同値であることが期待される

量子力学に反する例

$\sigma(|0\rangle) = \frac{1}{3},\quad \sigma(|1\rangle) = \frac{2}{3}$

P

1/3

2/3

$\{|0\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

$\{|1\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

異なるふるまいをさせる
スケジュールを選ぶ

区別できない
はず

$\{|0\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$

$\{|1\rangle/\chi_1\} \mid \nu a.(0 \mid a.\bar{b}.0 \mid \bar{c}.0)$

チャネル b に送信する確率が 1/3

チャネル c に送信する確率が 2/3

$\sigma'(|\psi\rangle) = \frac{1}{2},\quad \sigma'(|\phi\rangle) = \frac{1}{2}$

P’

1/2

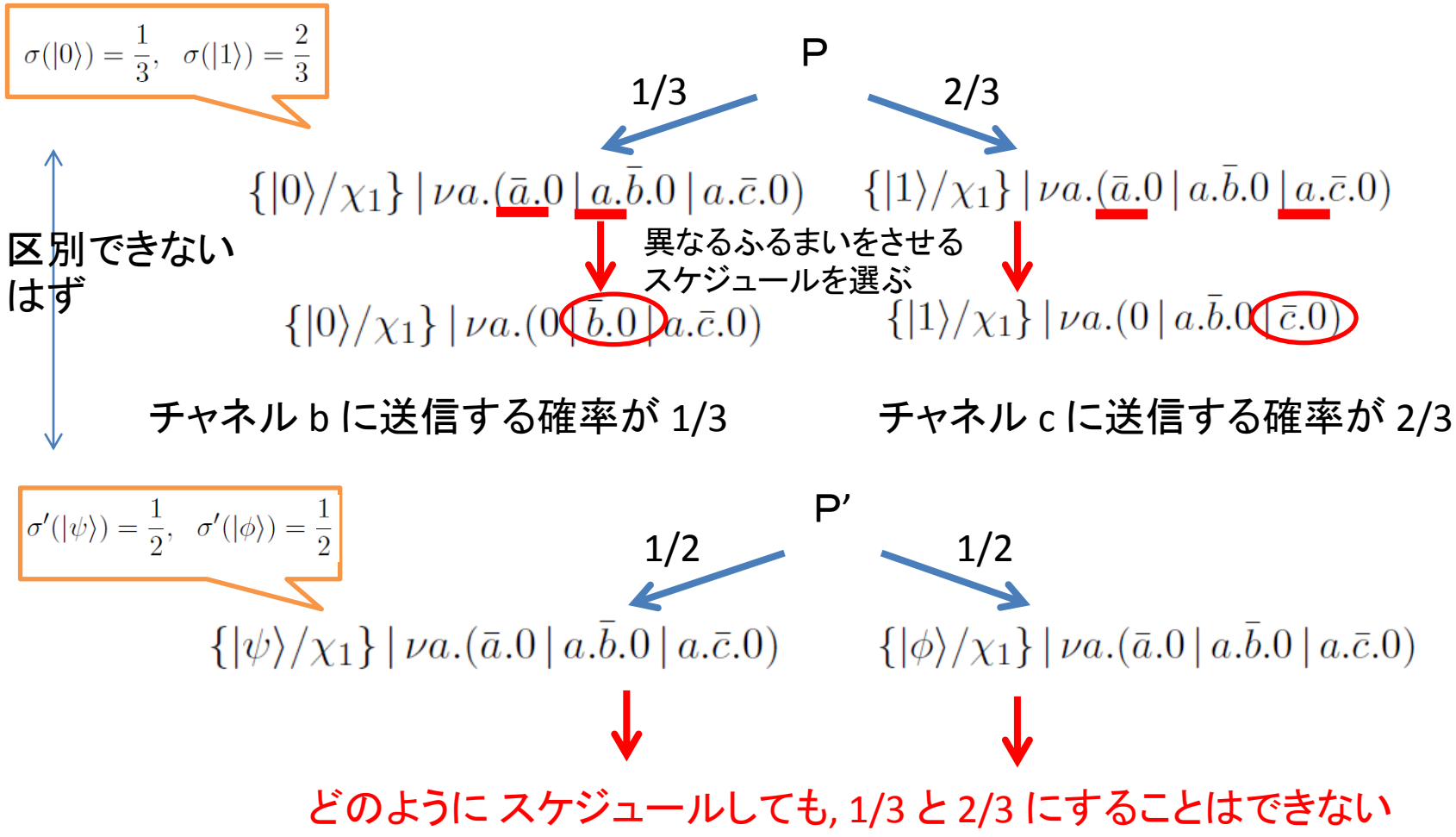
1/2

$\{|\psi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

$\{|\phi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

P と P’ は観測同値であることが期待される

量子力学に反する例


$\sigma(|0\rangle) = \frac{1}{3},\ \ \sigma(|1\rangle) = \frac{2}{3}$
P
1/3
2/3
$\{|0\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$
$\{|1\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$
区別できない
はず
異なるふるまいをさせる
スケジュールを選ぶ
$\{|0\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$
$\{|1\rangle/\chi_1\} \mid \nu a.(0 \mid a.\bar{b}.0 \mid \bar{c}.0)$
チャネル b に送信する確率が 1/3
チャネル c に送信する確率が 2/3
$\sigma'(|\psi\rangle) = \frac{1}{2},\ \ \sigma'(|\phi\rangle) = \frac{1}{2}$
P'
1/2
1/2
$\{|\psi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$
$\{|\phi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$
どのように スケジュールしても, 1/3 と 2/3 にすることはできない

戦略

- このような場合を回避するため,
  「代入を除いて同じプロセスは、次にする状態遷移を同じにする」という制限をつける
- スケジュールをそのように制限したものを戦略とよぶ

観測同値

- プロセス A, B が観測同値であるとは,
  任意の評価文脈 C と 戦略 F に対して,
  ある戦略 F’ が存在して,
  任意のチャネル a について
  C[A] が 戦略 F のもとで a にメッセージを送信する確率と
  C[B] が 戦略 F’ のもとで a にメッセージを送信する確率が
  等しいことである.

戦略を用いる場合

$\sigma(|0\rangle) = \frac{1}{3}, \quad \sigma(|1\rangle) = \frac{2}{3}$

P

1/3

2/3

$\{|0\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

$\{|1\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

$\sigma'(|\psi\rangle) = \frac{1}{2}, \quad \sigma'(|\phi\rangle) = \frac{1}{2}$

P’

1/2

1/2

$\{|\psi\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

$\{|\phi\rangle/\chi_1\} \,|\, \nu a.(\bar{a}.0 \,|\, a.\bar{b}.0 \,|\, a.\bar{c}.0)$

戦略を用いる場合

$\sigma(|0\rangle) = \frac{1}{3}, \quad \sigma(|1\rangle) = \frac{2}{3}$

P

1/3　　2/3

$\{|0\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$　　$\{|1\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

戦略では同じふるまい

$\{|0\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$　　$\{|1\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$

チャネル b に送信する確率が 1

$\sigma'(|\psi\rangle) = \frac{1}{2}, \quad \sigma'(|\phi\rangle) = \frac{1}{2}$

P’

1/2　　1/2

$\{|\psi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$　　$\{|\phi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

戦略を用いる場合

$\sigma(|0\rangle) = \frac{1}{3},\quad \sigma(|1\rangle) = \frac{2}{3}$

P

1/3　　2/3

$\{|0\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$　　$\{|1\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

戦略では同じふるまい

$\{|0\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$　　$\{|1\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$

チャネル b に送信する確率が 1

$\sigma'(|\psi\rangle) = \frac{1}{2},\quad \sigma'(|\phi\rangle) = \frac{1}{2}$

P'

1/2　　1/2

$\{|\psi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$　　$\{|\phi\rangle/\chi_1\} \mid \nu a.(\bar{a}.0 \mid a.\bar{b}.0 \mid a.\bar{c}.0)$

対応する戦略が存在

$\{|\psi\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$　　$\{|\phi\rangle/\chi_1\} \mid \nu a.(0 \mid \bar{b}.0 \mid a.\bar{c}.0)$

チャネル b に送信する確率が 1

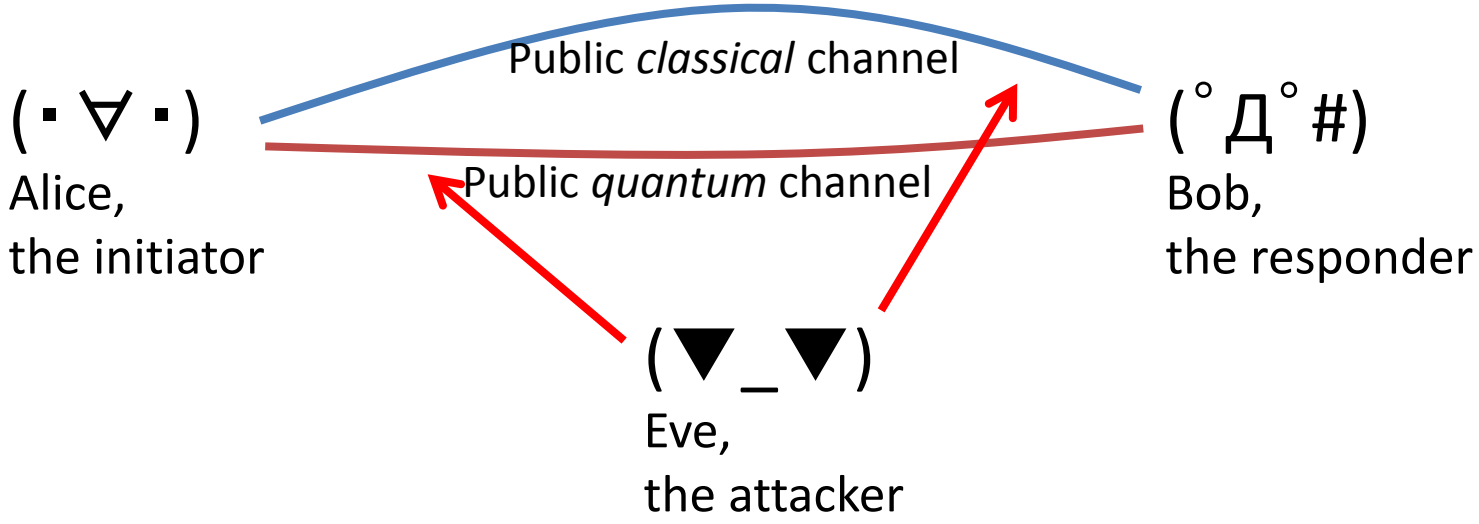
Outline

- 量子 Applied Pi-Calculus
- BB84プロトコルの形式的検証
- 関連研究
- 結論
- 今後の課題

量子鍵配送 (QKD) プロトコル

- 無条件安全性が得られる秘密鍵共有
  - 攻撃者は量子チャネルに任意の攻撃が可能
    - 攻撃者の盗聴を検知したら, アボートする
  - 攻撃者に漏れる情報量が無視できるほど小さい
    - 攻撃者の計算能力によらない
  - BB84, B92, DPS-QKD, COW-QKD…
- 安全性証明が複雑 [Mayers'97]
- 形式手法は利用できるか？

量子鍵配送プロトコル BB84



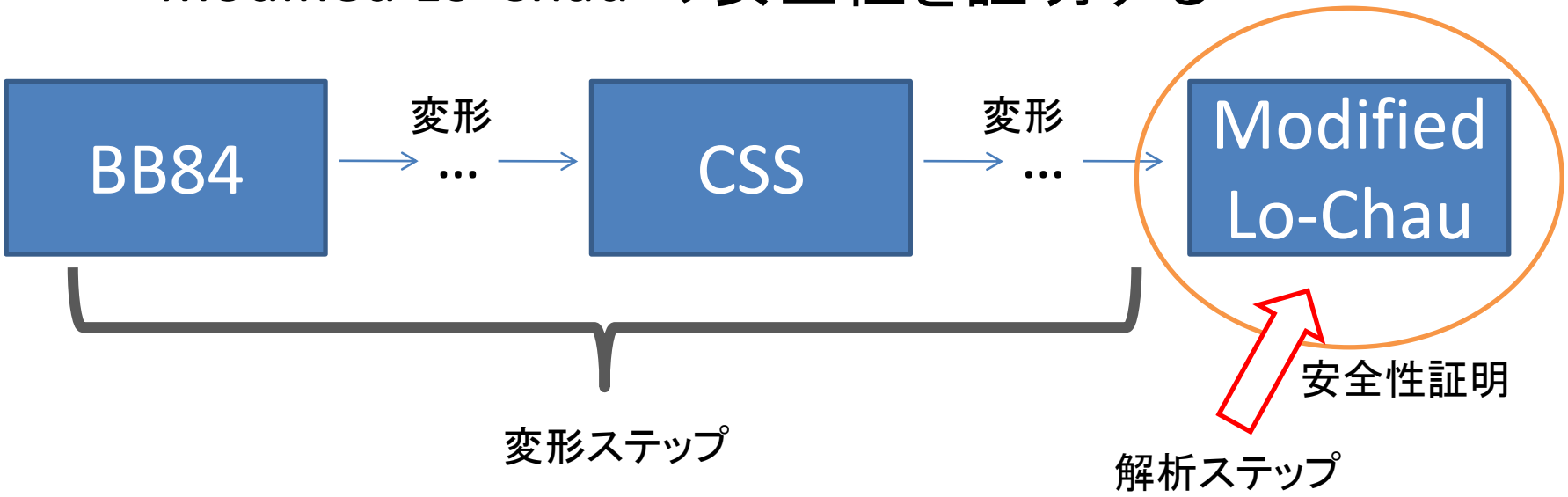
- 攻撃者の能力に関する仮定
  - 古典チャネルは盗聴可能、改ざん不可
  - 量子チャネルには任意の攻撃が可能
  - 無限の計算能力をもつ

安全性

- 無条件安全性
  - 任意の攻撃者(イブ)に対して, プロトコルが中断する確率が無視できるほど小さいならば,
    アリスの鍵とイブが推測した鍵との相互情報量が無視できるほど小さい.

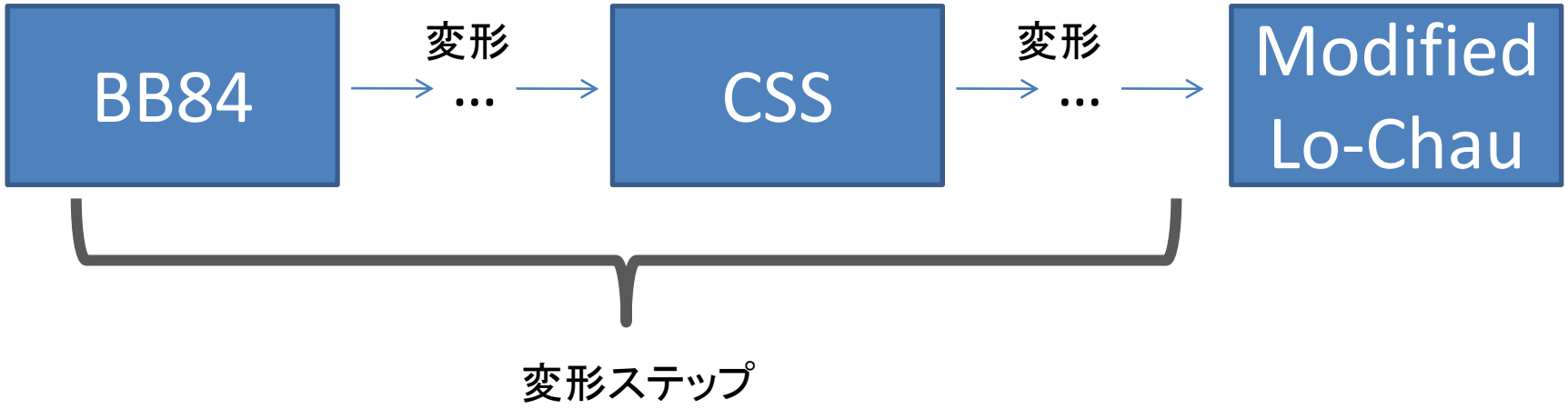
Shor-Preskill の証明法[SP'00]

- 変形ステップ
  - BB84 の安全性を modified Lo-Chauの安全性に帰着させる
- 解析ステップ
  - modified Lo-Chau の安全性を証明する



Shor-Preskill の証明の形式化を目指して

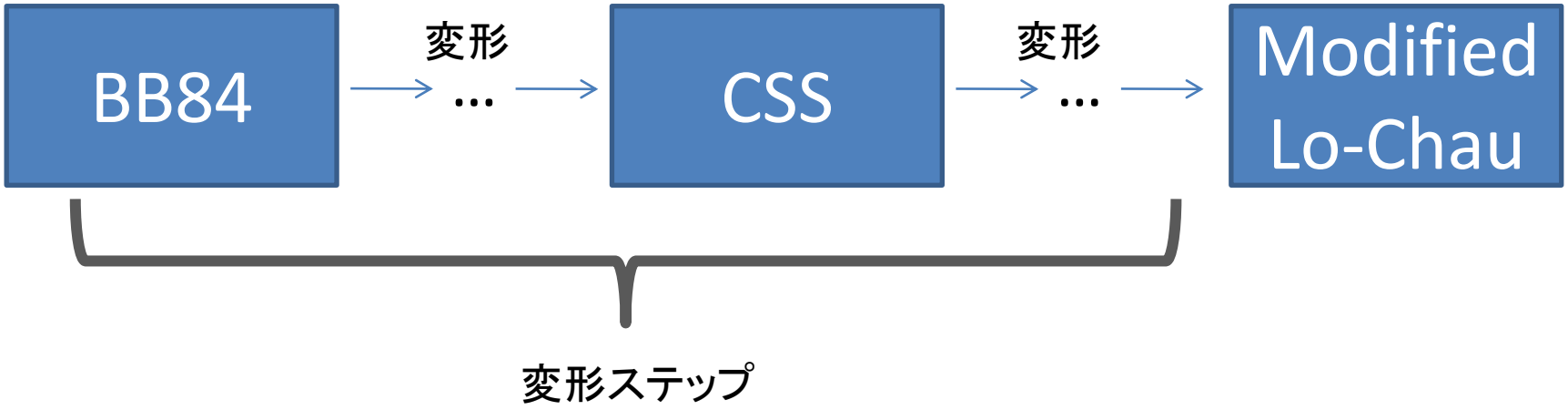
Shor-Preskill の方法



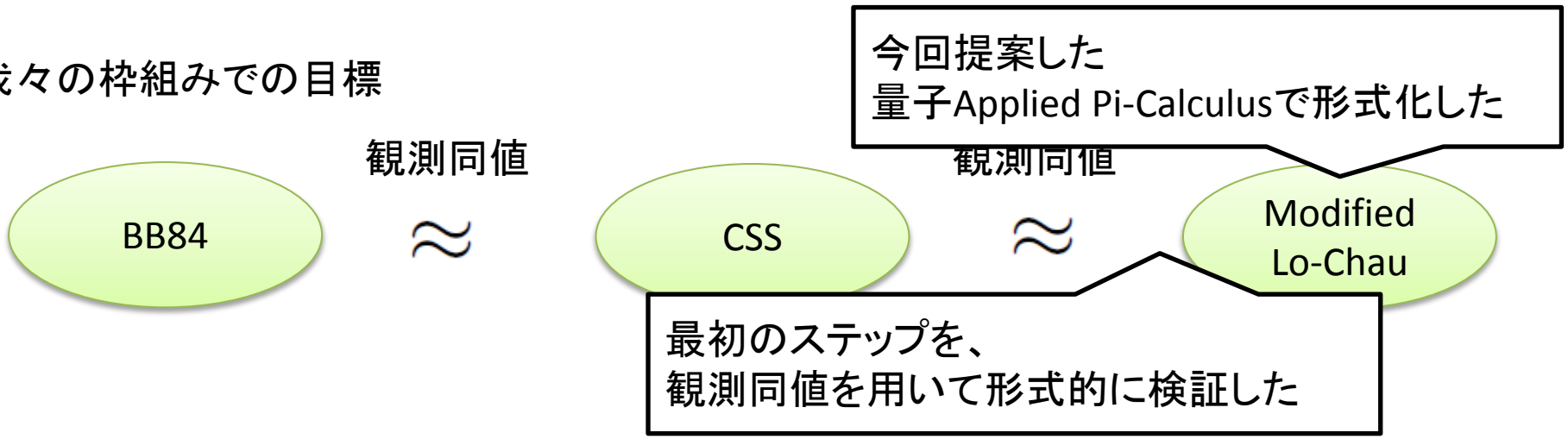
我々の枠組みでの目標

Shor-Preskill の証明の形式化を目指して

Shor-Preskill の方法



我々の枠組みでの目標



Outline

- 量子 Applied Pi-Calculus
- BB84プロトコルの形式的検証
- 関連研究
- 結論
- 今後の課題

関連研究

- Communicating Quantum Processes [GN'05]
  - モデル化中心
    - 量子テレポーテーション, コミットメントなど
  - 観測同値は定義されていない
- An Algebra of Quantum Processes [YFDJ'09]
  - If の分岐がない
    - 表現が直感的にわかりにくい
    - 今回提案した枠組みは, 表現力が上がっている

結論

- 量子 Applied Pi-Calculus の提案
  - 確率 Applied Pi-Calculus [GPT'07] を拡張した
    - 量子変数への代入
    - 量子測定の反応関係
    - 観測同値
  - BB84 の安全性証明の一部を,
    観測同値を利用して形式的に検証した

今後の課題

- 観測同値の定義の適切さについての議論
- 観測同値と完全に一致するような
  双模倣の定義 [AF'99, GPT'07]
- Shor-Preskill の安全性証明の
  π計算による形式的検証の完成
  - すべての変形ステップを形式化
- その他の量子プロトコルへの応用

ご清聴ありがとうございました