量子鍵配送の安全性証明の量子プロセス計算を用いた形式的検証

久保田 貴大[1], 角谷 良彦[1], 加藤 豪[2],
河野 泰人[2], 櫻田 英樹[2]

[1]東京大学大学院情報理工学系研究科
[2]NTTコミュニケーション科学基礎研究所

背景

- 量子暗号安全性証明も,
  複雑かつ検証が難しくなることがある
  - MayersのBB84安全性証明に代表される,
    長大な証明 [M97]
  - 安全性が正しく証明されていない論文も多い
- 量子版の形式体系がいくつか提案されて
  いるが, QKDの安全性証明への適用例は
  あまりない [L04], [A07], [DF12],…
  - 量子テレポーテーションの仕様記述 [FDY11, D11]
  - コミットメントのモデリング [GN04]

研究の概要

- 量子プロセス計算qCCS[FDY11]を用いて, Shor-PreskillのBB84安全性証明を形式検証した
  - 二つのプロトコルBB84, EDPをqCCSプロセスとして形式化し, それらが双模倣であることを示した
  - 双模倣を示す際, 観測の記述法が注意点となるが, その一般的な方法を提案する

本発表の構成

- 量子プロセス計算qCCS
- BB84鍵配送の安全性
- qCCSを用いた形式検証
- まとめと今後の課題

qCCSの文法[FDY11]

量子通信

$$P ::= \mathbf{nil} \mid \tau.P \mid c?x.P \mid c!e.P \mid \mathbf{c}?q.P \mid \mathbf{c}!q.P$$
$$\mid \mathtt{if}\ b\ \mathtt{then}\ P \mid \mathcal{E}[\tilde{q}].P \mid M[\tilde{q};x].P \mid P||P \mid P\backslash L$$

量子演算　　観測

- ひとつのqubit型自由変数には, 2次元ヒルベルト空間が対応する
- 各qubitの状態をあらわす密度行列を ρ とする
  以後, 組 $\langle P, \rho \rangle$ のことをプロセスとよぶ

例)

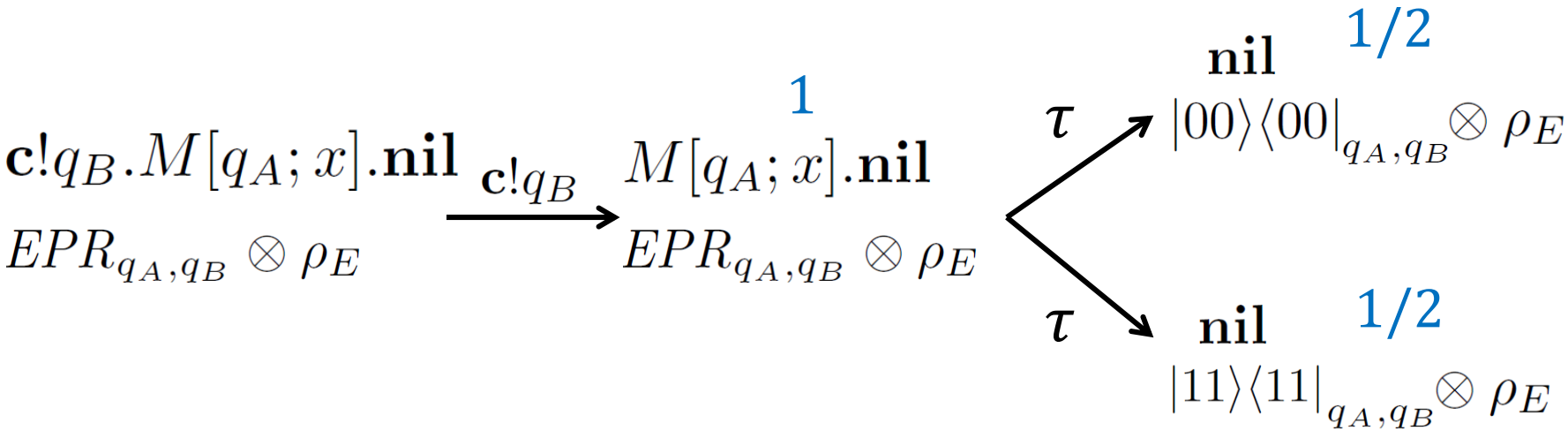
$$\langle \mathbf{c}!q_B.M[q_A;x].\mathbf{nil}, EPR_{q_A,q_B} \otimes \rho_E \rangle$$

ラベル付き状態遷移

- $\langle P, \rho \rangle \xrightarrow{\alpha} \mu$
- プロセス $\langle P, \rho \rangle$ は
  行動 α をおこなって,
  確率分布 μ に遷移する

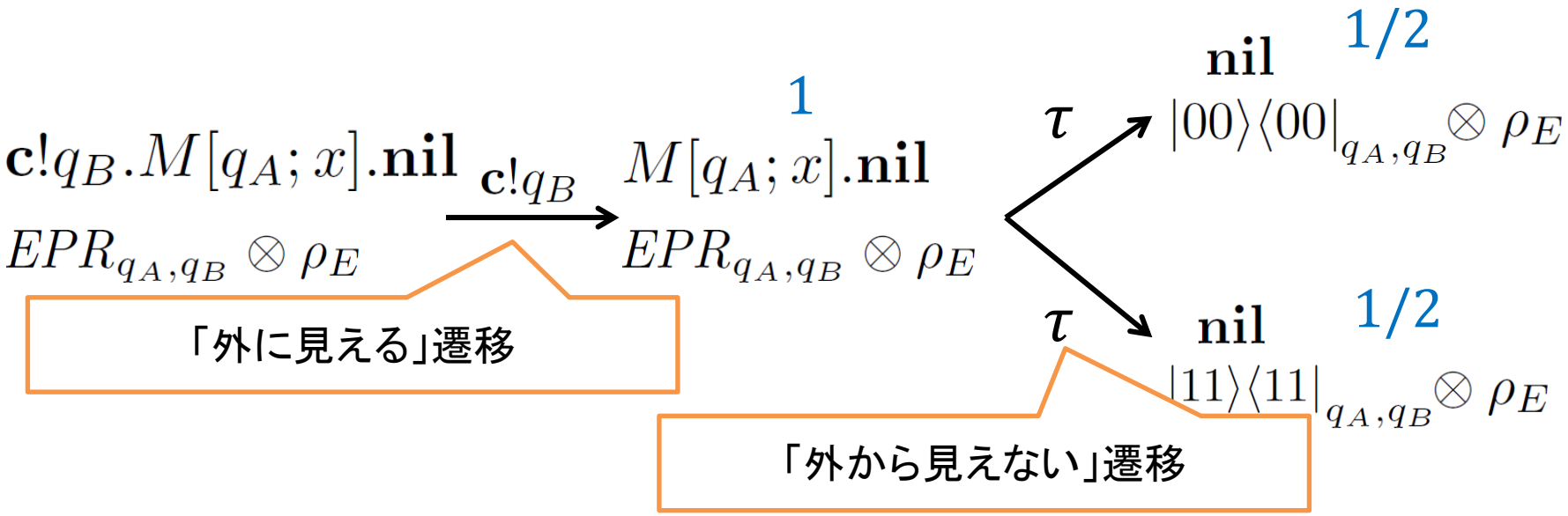
状態遷移の例

$$\langle \mathbf{c}!q_B.M[q_A;x].\mathbf{nil}, EPR_{q_A,q_B} \otimes \rho_E \rangle$$



状態遷移の例

$$\langle \mathbf{c}!q_B.M[q_A;x].\mathbf{nil}, EPR_{q_A,q_B} \otimes \rho_E \rangle$$



遷移規則 (抜粋)

$$\frac{}{\langle c?x.P, \rho\rangle \xrightarrow{c?v} \langle P\{v/x\}, \rho\rangle} \qquad \frac{}{\langle \mathcal{E}[\tilde{r}].P, \rho\rangle \xrightarrow{\tau} \langle P, \mathcal{E}_{\tilde{r}}(\rho)\rangle}$$

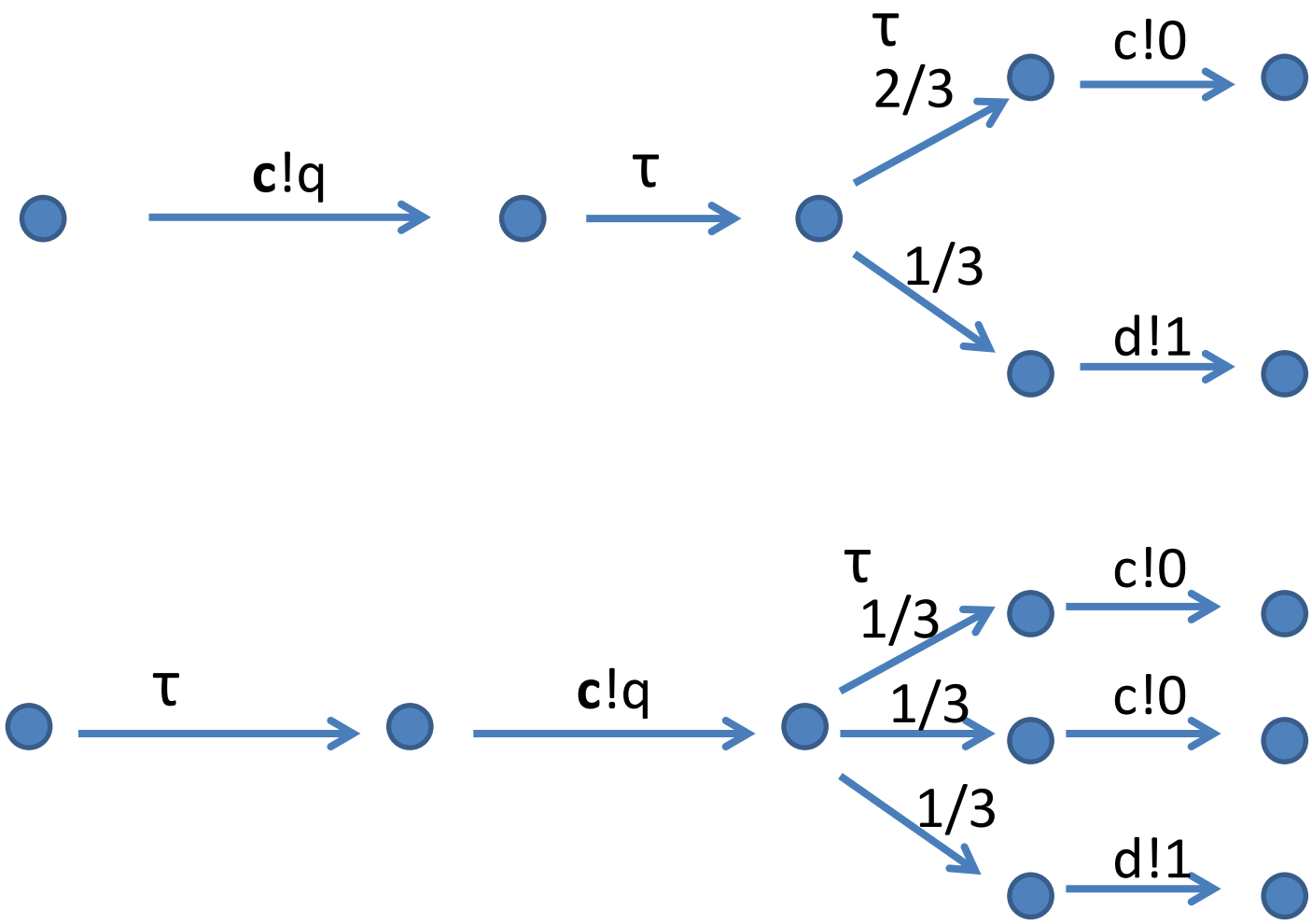
$$\frac{}{\langle M[\tilde{r}; x].P, \rho\rangle \xrightarrow{\tau} \sum_{i\in I} p_i \langle P\{\lambda_i/x\}, E^i_{\tilde{r}} \rho E^i_{\tilde{r}} / p_i\rangle}$$

$$\frac{\langle P, \rho\rangle \xrightarrow{\alpha} \mu, \quad [\![b]\!] = \mathtt{true}}{\langle \textbf{if } b \textbf{ then } P, \rho\rangle \xrightarrow{\alpha} \mu} \qquad \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i, \rho_i\rangle, \quad cn(\alpha) \notin L}{\langle P\backslash L, \rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i\backslash L, \rho_i\rangle}$$

双模倣関係

- ふたつのプロセス $\langle P, \rho \rangle, \langle Q, \sigma \rangle$が
  外から見て同じに振る舞うという関係
- 一方のプロセスが遷移可能なら, 他方でも
  τ 遷移を除いて同様の遷移が可能であり,
  かつ, 各ステップにおいて,
  外の人に見えている状態が同じ
- $\langle P, \rho \rangle \approx \langle Q, \sigma \rangle$ と書く

双模倣の例

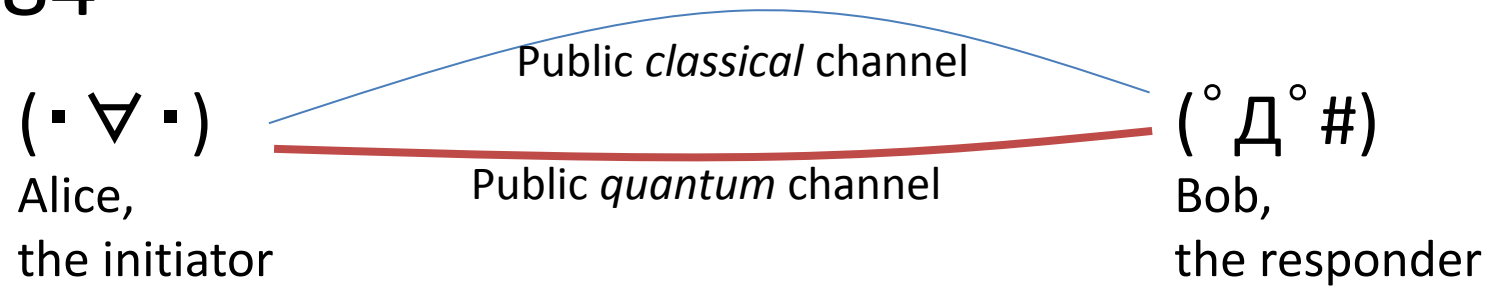


検証の対象 BB84鍵配送

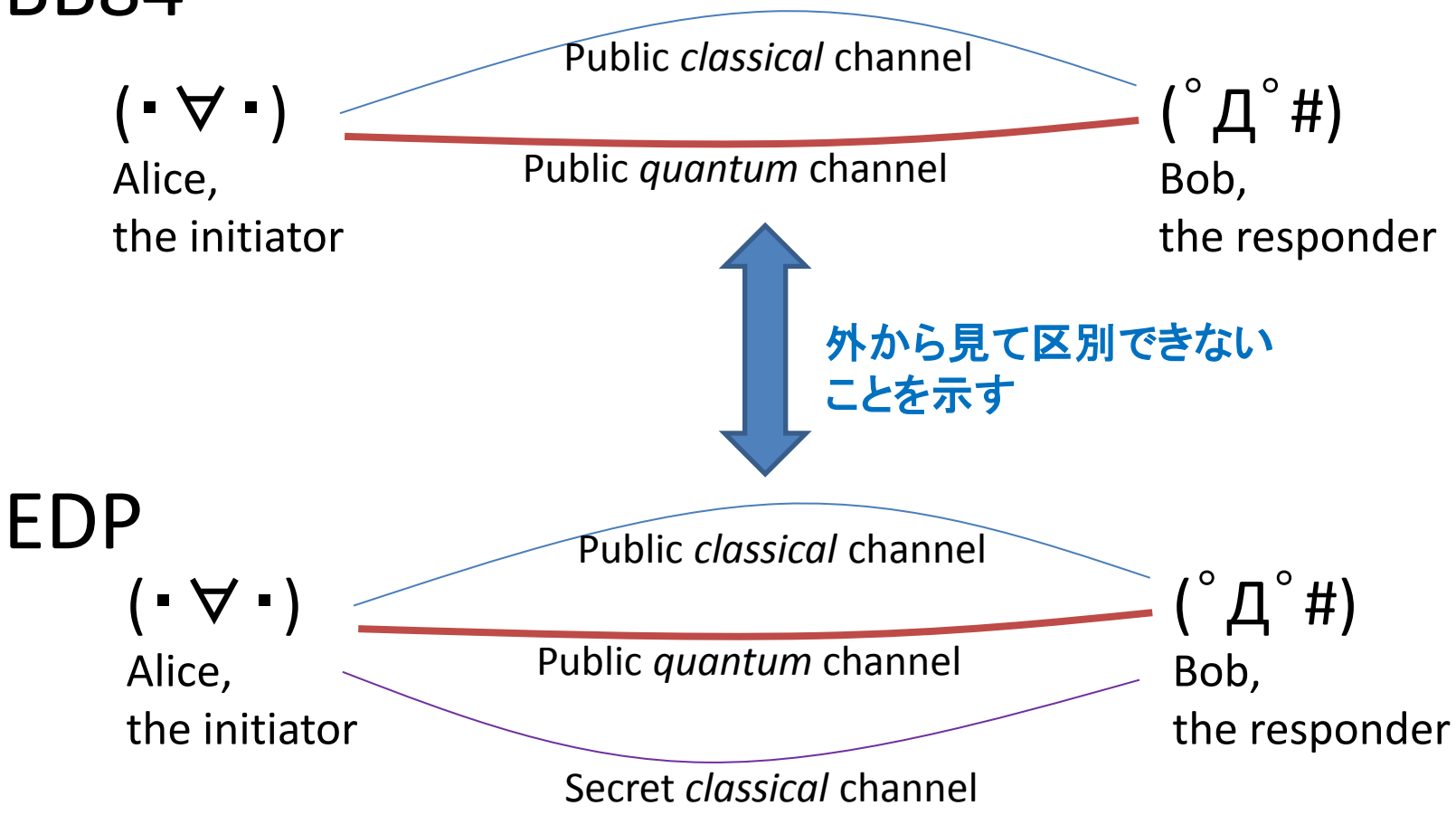
- 盗聴検知をおこなう
  - 攻撃者の観測が, AliceとBobが通信している量子ビットの量子状態を乱す
  - エラーレートから, 攻撃者に漏れている情報量を見積もることができる
  - 攻撃者に漏れている情報量が十分小さいと判断されるときのみ, プロトコルを続行
- 量子通信の後に,
  誤り訂正とプライバシ増幅を行う
  - 手段は何でもよいが, 本研究はCSS符号を用いるプロトコル[SP00]を対象とする

安全性証明の概要[SP00]

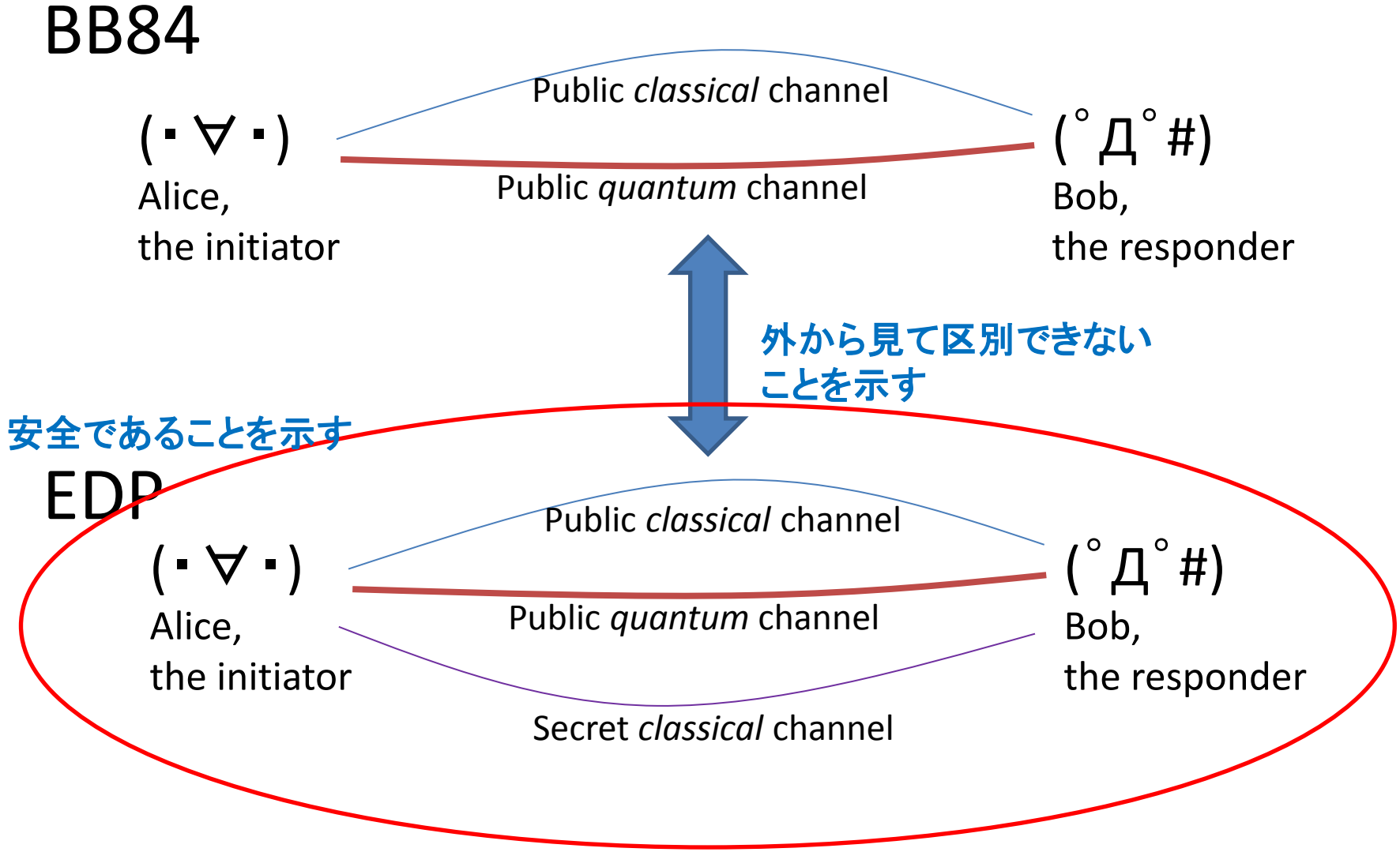
BB84



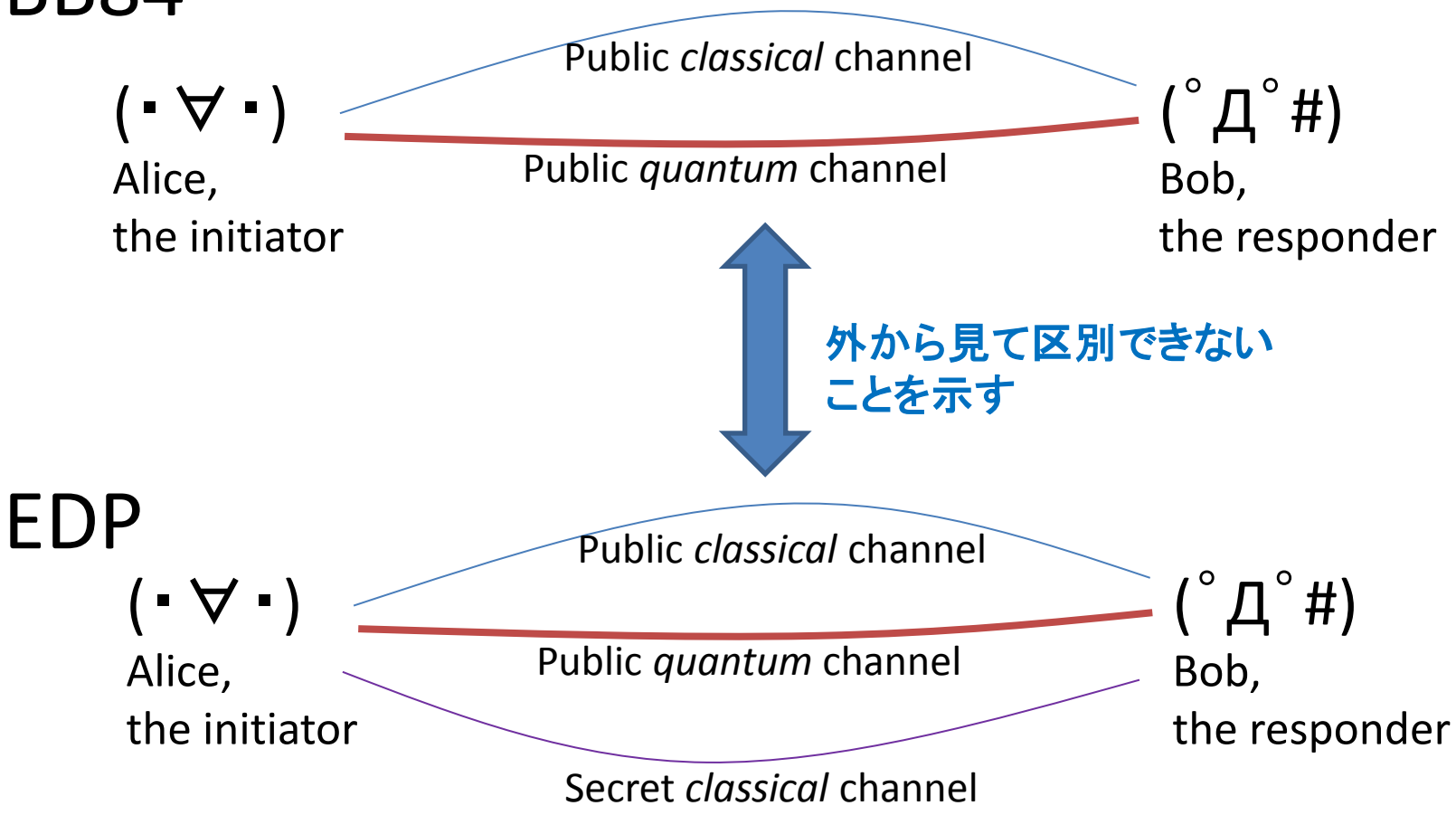
安全性証明の概要[SP00]



安全性証明の概要[SP00]



形式検証の概要


BB84
(・∀・)
Alice,
the initiator
Public *classical* channel
Public *quantum* channel
(゜Д゜#)
Bob,
the responder
外から見て区別できない
ことを示す
EDP
(・∀・)
Alice,
the initiator
Public *classical* channel
Public *quantum* channel
Secret *classical* channel
(゜Д゜#)
Bob,
the responder

形式検証の概要

BB84

qCCSプロセスとして
形式化

the initiato

Pu nnel

$\langle A||B\backslash\{c_1,c_2,c_3,c_4,c_5,c_6\},\ \rho_A\otimes\rho_B\otimes\rho_E\rangle$
$A \equiv \mathrm{hadamards}(q'_A, r^1_A).$
$\mathrm{shuffle}(q'_A, r^2_A).$
$c_1!q'_{A,1},...,q'_{A,2n}.c_1?x_A.$
$\mathrm{copy}(r^2_A, R^2_A).c_2!r^2_A.d_1!R^2_A.$
$\mathrm{copy}(r^1_A, R^1_A).c_3!r^1_A.d_2!R^1_A.$
$\mathrm{measure}(q_{A,1},...,q_{A,n}).$
$c_4?s_A.\mathrm{abort\_alice}(q_{A,1},...,q_{A,n},s_A,b_A)$
$M[b_A;y].c_2!y.d_1!y.\mathrm{if}\ y\ \mathrm{then}$
$\mathrm{css\_projection}(q_{A,n+1},...,q_{A,2n},u_A,v_A).$
$\mathrm{css\_decode}(q_{A,n+1},...,q_{A,2n},u_A,v_A)$
$\mathrm{copy}(u_A,U_A).c_5!u_A.d_3!U_A.$
$\mathrm{copy}(v_A,V_A).c_6!v_A.A_2$
$+\ \mathrm{if}\ \neg y\ \mathrm{then}\ \bot$
$\rho_A \equiv (|00\rangle\langle 00|+|00\rangle\langle 11|+|11\rangle\langle 00|+|11\rangle\langle 11|)^{\otimes 2n}_{q_A,q'_A}\otimes$
$(|0\rangle\langle 0|+|1\rangle\langle 1|)^{\otimes N}_{r^1_A}\otimes(|0\rangle\langle 0|+|1\rangle\langle 1|)^{\otimes N}_{r^2_A}\otimes$
$(|0\rangle\langle 0|)^{\otimes N}_{R^1_A}\otimes(|0\rangle\langle 0|)^{\otimes N}_{R^2_A}\otimes|0\rangle\langle 0|_{b_A}\otimes$
$(|0\rangle\langle 0|)^{\otimes n}_{u_A}\otimes(|0\rangle\langle 0|)^{\otimes n}_{v_A}\otimes(|0\rangle\langle 0|)^{\otimes n}_{U_A}\otimes(|0\rangle\langle 0|$

(゜Д゜#)
Bob,
the responder

双模倣の証明

≈

EDP

(・∀・)
Alice,
the initiator

Pul el

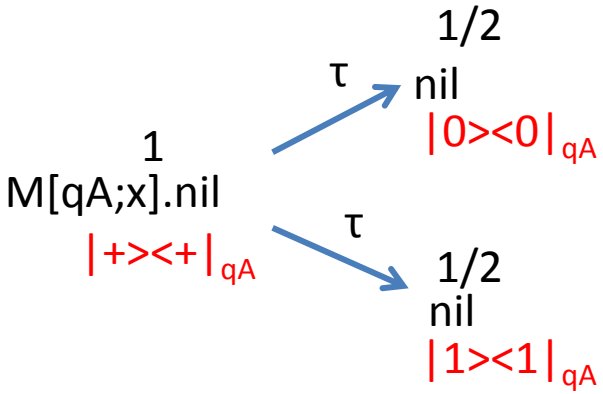
$\langle A||B\backslash\{c_1,c_2,c_3,c_4,c_5\}\ \rho_A\otimes\rho_B\otimes\rho_E\rangle$
$A \equiv \mathrm{hadamards}(q'_A, r^1_A).$
$\mathrm{shuffle}(q'_A, r^2_A).$
$c_1!q'_{A,1},...,q'_{A,2n}.c_1?x_A.$
$\mathrm{copy}(r^2_A, R^2_A).c_2!r^2_A.d_1!R^2_A.$
$\mathrm{copy}(r^1_A, R^1_A).c_3!r^1_A.d_2!R^1_A.$
$c_4?s_A.\mathrm{abort\_alice}(q_{A,1},...,q_{A,n},s_A,b_A).$
$M[b_A;y].c_2!y.d_1!y.\mathrm{if}\ y\ \mathrm{then}$
$\mathrm{if}\ b_A\ \mathrm{then}$
$\mathrm{cnot}(u_A,q_{A,n+1},...,q_{A,2n}).$
$\mathrm{copy}(u_A,q_{A,n+1},...,q_{A,2n}).$
$\mathrm{key}(q_{A,n+1},...,q_{A,2n}).$
$\mathrm{copy}(u_A,U_A).c_5!u_A.d_3!U_A.A_2$
$+\ \mathrm{if}\ \neg y\ \mathrm{then}\ \bot$
$\rho_A \equiv (|00\rangle\langle 00|+|11\rangle\langle 11|)^{\otimes 2n}_{q_A,q'_A}\otimes$
$(|0\rangle\langle 0|+|1\rangle\langle 1|)^{\otimes N}_{r^1_A}\otimes(|0\rangle\langle 0|+|1\rangle\langle 1|)^{\otimes N}_{r^2_A}\otimes$
$(|0\rangle\langle 0|)^{\otimes N}_{R^1_A}\otimes(|0\rangle\langle 0|)^{\otimes N}_{R^2_A}\otimes|0\rangle\langle 0|_{b_A}\otimes$
$(\sum_{u\in C_1}|u\rangle\langle u|)^{\otimes n}_{u_A}\otimes(|0\rangle\langle 0|)^{\otimes n}_{U_A}$

S el

(゜Д゜#)
Bob,
the responder

観測の記述について

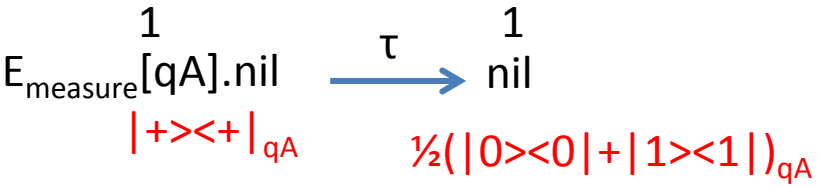
構文にある観測M[q~;x]で
書いた場合



・両者は
物理的に同じ？

観測をあらわす
量子演算で書いた場合

$$\mathcal{E}_{\mathtt{measure}}(\rho) = |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$$



$$P ::= \mathbf{nil} \mid \tau.P \mid c?x.P \mid c!e.P \mid \mathbf{c}?q.P \mid \mathbf{c}!q.P$$
$$\mid \mathtt{if}\ b\ \mathtt{then}\ P \mid \underline{\mathcal{E}[\tilde{q}].P} \mid \underline{M[\tilde{q};x].P} \mid P||P \mid P\backslash L$$

量子演算　　観測

安全性証明で最初にする推論

- AliceはEPRペアを準備し, 片方をBobに送り, そのあと自分が持つ片方を測定する

- AliceはEPRペアを準備し,自分が持つ片方を測定し, そのあともう片方をBobに送る

どちらも, 外からは区別できない

EPRペアの送信と観測

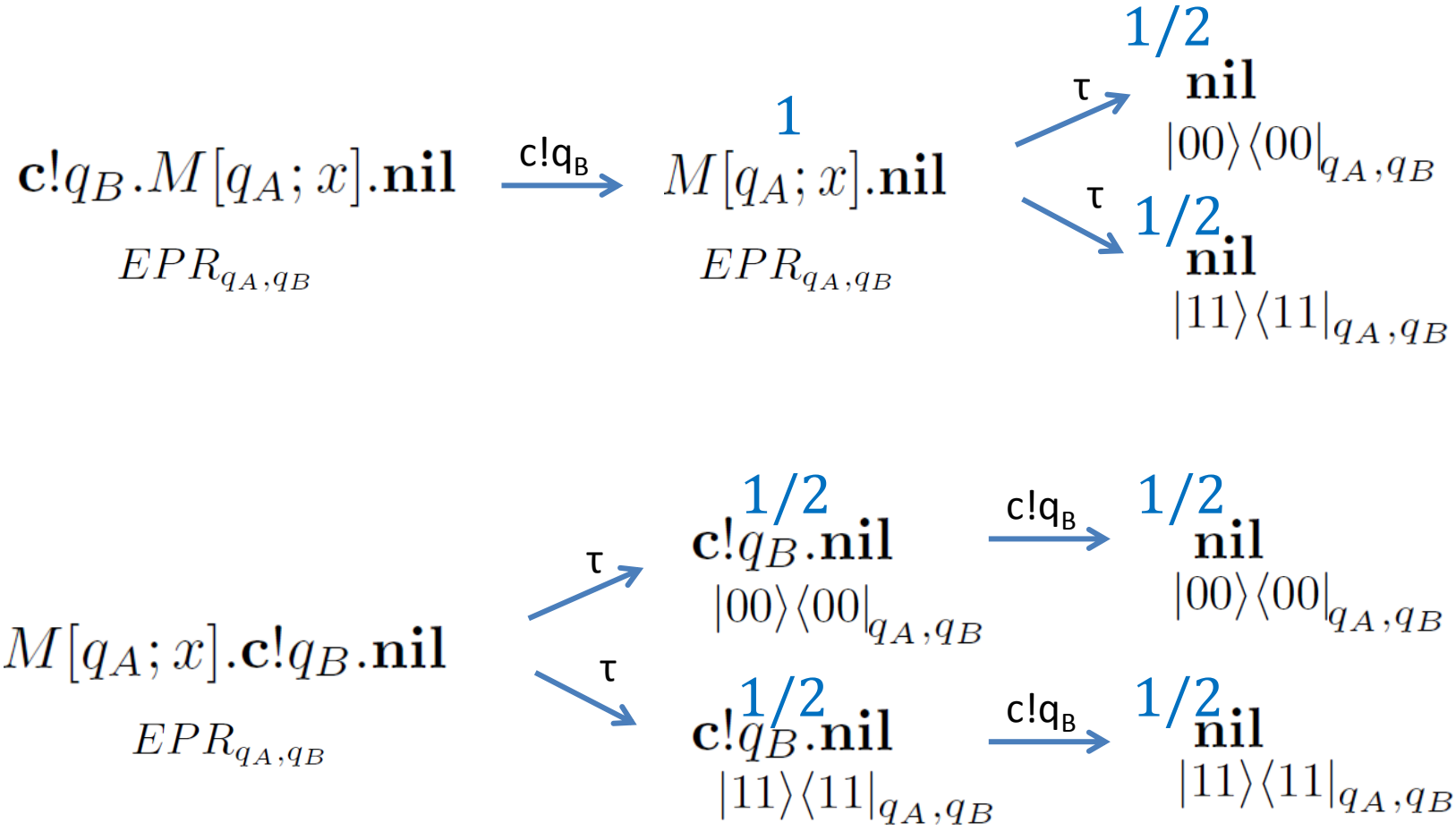
- $M[\tilde{q};x]$で書いた場合
  - 先に送信するプロセス

$$\langle \mathbf{c}!q_B.M[q_A;x].\mathbf{nil}, EPR_{q_A,q_B} \otimes \rho_E \rangle$$

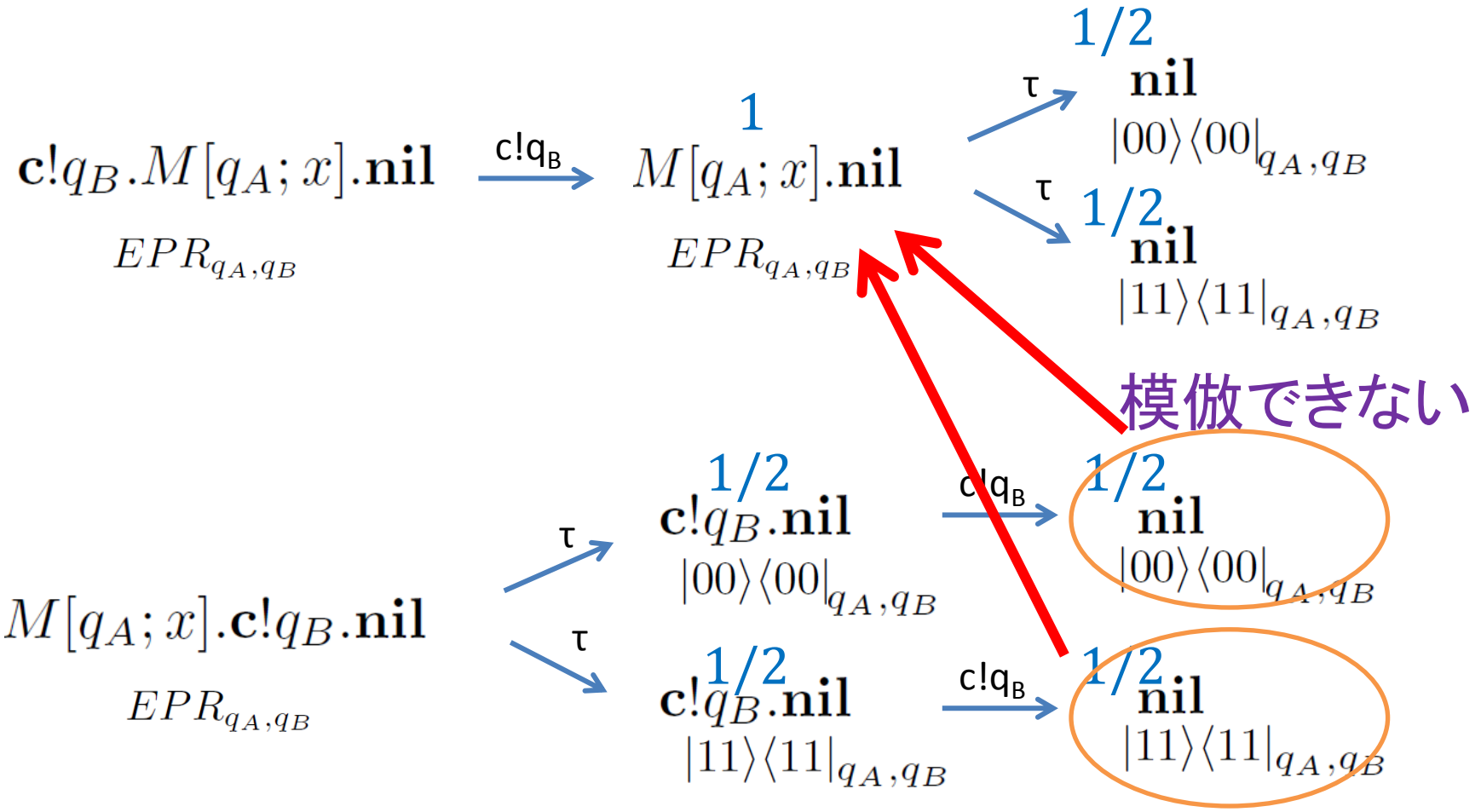
  - 後に送信するプロセス

$$\langle M[q_A;x].\mathbf{c}!q_B.\mathbf{nil}, EPR_{q_A,q_B} \otimes \rho_E \rangle$$

双模倣にならない


$\mathbf{c}!q_B.M[q_A;x].\mathbf{nil}$
EPR_{q_A,q_B}
c!q_B
1
$M[q_A;x].\mathbf{nil}$
EPR_{q_A,q_B}
τ
1/2
nil
$|00\rangle\langle 00|_{q_A,q_B}$
τ
1/2
nil
$|11\rangle\langle 11|_{q_A,q_B}$
$M[q_A;x].\mathbf{c}!q_B.\mathbf{nil}$
EPR_{q_A,q_B}
τ
1/2
$\mathbf{c}!q_B.\mathbf{nil}$
$|00\rangle\langle 00|_{q_A,q_B}$
c!q_B
1/2
nil
$|00\rangle\langle 00|_{q_A,q_B}$
τ
1/2
$\mathbf{c}!q_B.\mathbf{nil}$
$|11\rangle\langle 11|_{q_A,q_B}$
c!q_B
1/2
nil
$|11\rangle\langle 11|_{q_A,q_B}$

双模倣にならない


$\mathbf{c}!q_B.M[q_A;x].\mathbf{nil}$
EPR_{q_A,q_B}
c!q_B
1
$M[q_A;x].\mathbf{nil}$
EPR_{q_A,q_B}
τ
1/2
nil
$|00\rangle\langle 00|_{q_A,q_B}$
τ
1/2
nil
$|11\rangle\langle 11|_{q_A,q_B}$
模倣できない
$M[q_A;x].\mathbf{c}!q_B.\mathbf{nil}$
EPR_{q_A,q_B}
τ
τ
1/2
$\mathbf{c}!q_B.\mathbf{nil}$
$|00\rangle\langle 00|_{q_A,q_B}$
1/2
$\mathbf{c}!q_B.\mathbf{nil}$
$|11\rangle\langle 11|_{q_A,q_B}$
c!q_B
c!q_B
1/2
nil
$|00\rangle\langle 00|_{q_A,q_B}$
1/2
nil
$|11\rangle\langle 11|_{q_A,q_B}$

EPRペアの送信と観測

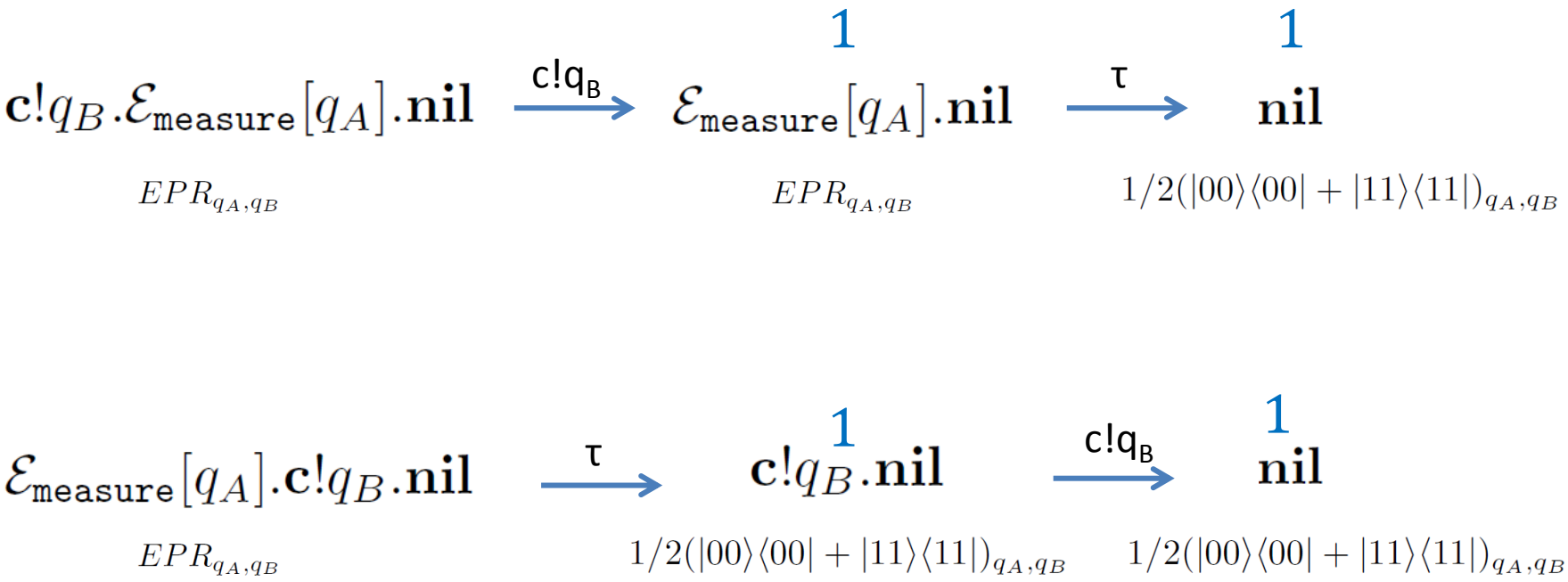
- 量子演算 $\mathcal{E}_{\mathtt{measure}}$ で書いた場合
  - 先に送信するプロセス

$$\langle \mathbf{c}!q_B.\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{nil}, EPR_{q_A,q_B} \otimes \rho_E \rangle$$

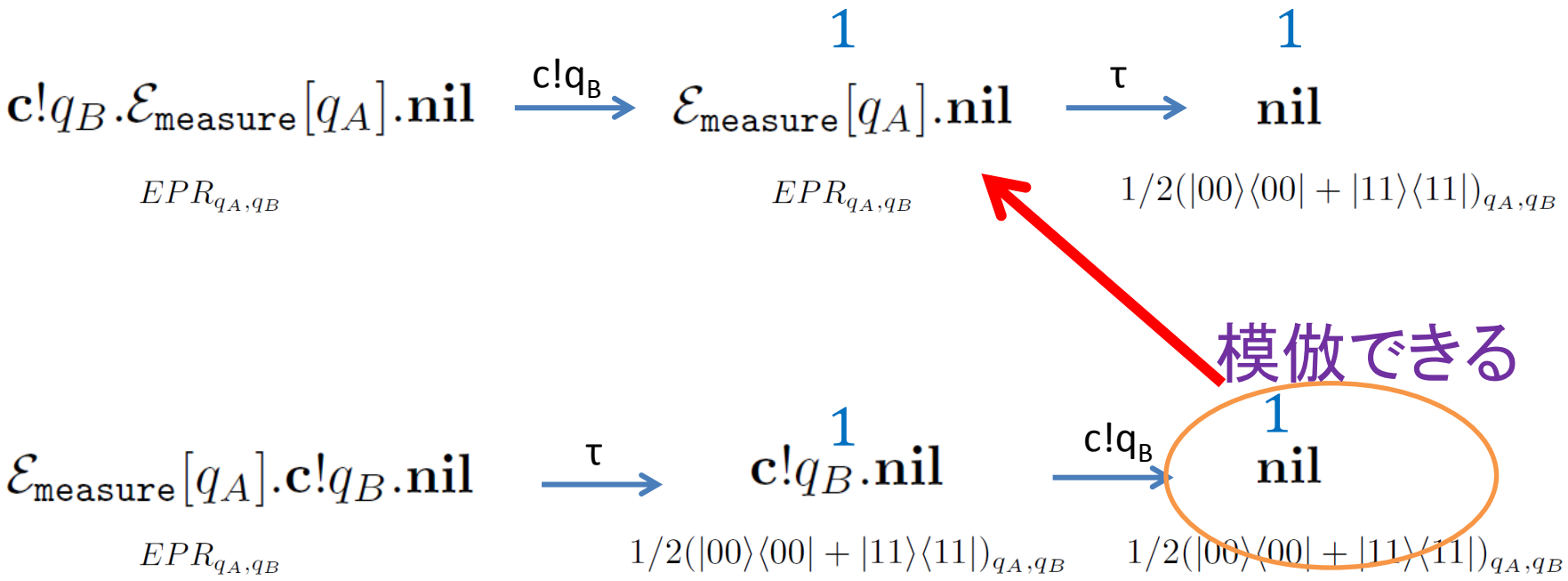
  - 後に送信するプロセス

$$\langle \mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{c}!q_B.\mathbf{nil}, EPR_{q_A,q_B} \otimes \rho_E \rangle$$

双模倣になる


$\mathbf{c}!q_B.\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{nil}$
c!q_B
1
$\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{nil}$
τ
1
$\mathbf{nil}$
EPR_{q_A,q_B}
EPR_{q_A,q_B}
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$
$\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{c}!q_B.\mathbf{nil}$
τ
1
$\mathbf{c}!q_B.\mathbf{nil}$
c!q_B
1
$\mathbf{nil}$
EPR_{q_A,q_B}
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$

双模倣になる


$\mathbf{c}!q_B.\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{nil}$
c!q_B
1
$\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{nil}$
τ
1
$\mathbf{nil}$
EPR_{q_A,q_B}
EPR_{q_A,q_B}
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$
模倣できる
$\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{c}!q_B.\mathbf{nil}$
τ
1
$\mathbf{c}!q_B.\mathbf{nil}$
c!q_B
1
$\mathbf{nil}$
EPR_{q_A,q_B}
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$

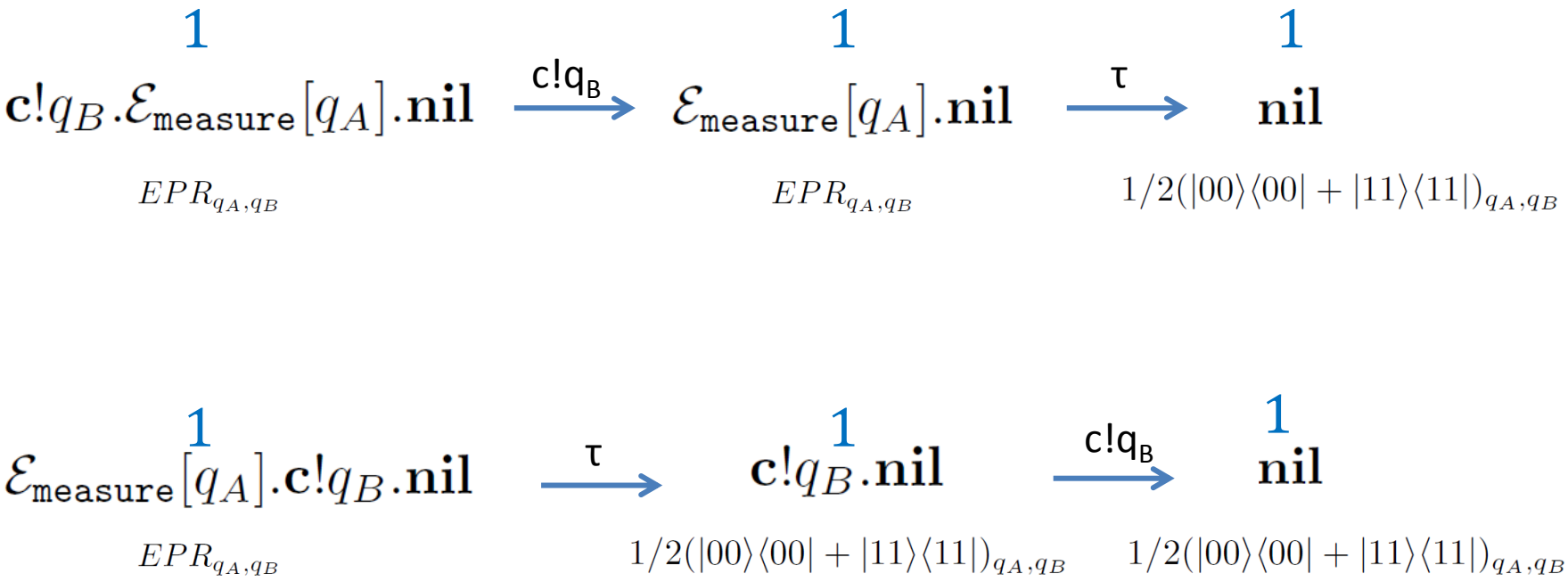
観測について

- 観測の形式化は二種類あり,
  使い分ける必要がある
- 攻撃者にとって分岐が見えるような観測
  だったら $M[\tilde{q}; x]$ で形式化する
  - 観測の結果によって違うラベルで遷移する場合など
- 見えないなら $\mathcal{E}_{\mathtt{measure}}$ で形式化する

$$P ::= \mathbf{nil} \mid \tau.P \mid c?x.P \mid c!e.P \mid \mathbf{c}?q.P \mid \mathbf{c}!q.P$$
$$\mid \mathtt{if}\ b\ \mathtt{then}\ P \mid \mathcal{E}[\tilde{q}].P \mid M[\tilde{q}; x].P \mid P||P \mid P\backslash L$$

量子演算　観測

正しい形式化


1
$\mathbf{c}!q_B.\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{nil}$
c!q_B
1
$\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{nil}$
τ
1
$\mathbf{nil}$
EPR_{q_A,q_B}
EPR_{q_A,q_B}
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$
1
$\mathcal{E}_{\mathtt{measure}}[q_A].\mathbf{c}!q_B.\mathbf{nil}$
τ
1
$\mathbf{c}!q_B.\mathbf{nil}$
c!q_B
1
$\mathbf{nil}$
EPR_{q_A,q_B}
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$
$1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)_{q_A,q_B}$

EDPの形式化

$\langle A||B\backslash\{c_1, c_2, \mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_5}, \mathbf{c_6}\},\ \rho_A \otimes \rho_B \otimes \rho_E\rangle$

$A \equiv$ hadamards(q'_A, r^1_A).
shuffle(q'_A, r^2_A).
$\mathbf{c_1}!q'_{A,1}, ..., q'_{A,2n}.c_1?x_A$.
copy$(r^2_A, R^2_A).\mathbf{c_2}!r^2_A.\mathbf{d_1}!R^2_A$.
copy$(r^1_A, R^1_A).\mathbf{c_3}!r^1_A.\mathbf{d_2}!R^1_A$.
measure$(q_{A,1}, ..., q_{A,n})$.
$\mathbf{c_4}?s_A$.abort_alice$(q_{A,1}, ..., q_{A,n}, s_A, b_A)$
$M[b_A; y].c_2!y.d_1!y.$if y then
css_projection$(q_{A,n+1}, ..., q_{A,2n}, u_A, v_A)$.
css_decode$(q_{A,n+1}, ..., q_{A,2n}, u_A, v_A)$
copy$(u_A, U_A).\mathbf{c_5}!u_A.\mathbf{d_3}!U_A$.
copy$(v_A, V_A).\mathbf{c_6}!v_A.A_2$

$B \equiv \mathbf{c_1}?q_{B,1}, ..., q_{B,2n}.c_1!0.d_2!0.$
$\mathbf{c_2}?r^2_B$.unshuffle(q_B, r^2_B).
$\mathbf{c_3}?r^1_B$.hadamards(q_B, r^1_B).
measure$(q_{B,1}, ..., q_{B,n})$.
copy$(q_{B,1}, ..., q_{B,n}, Q_{B,1}, ..., Q_{B,n})$
$\mathbf{c_4}!q_{B,1}, ..., q_{B,n}.\mathbf{d_5}!Q_{B,1}, ..., Q_{B,n}.$
$c_2?b_B$.if b_B then $\mathbf{c_5}?u_B.\mathbf{c_6}?v_B$.
css_syndrome$(q_{B,n+1}, ..., q_{B,2n}, u_B, v_B, sx_B, sz_B)$.
css_correct$(q_{B,n+1}, ..., q_{B,2n}, sx_B, sz_B)$
css_decode$(q_{B,n+1}, ..., q_{B,2n}, u_B, v_B).B_2$

$\rho_A \equiv (|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)^{\otimes 2n}_{q_A, q'_A} \otimes$
$(|0\rangle\langle 0| + |1\rangle\langle 1|)^{\otimes N}_{r^1_A} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)^{\otimes N}_{r^2_A} \otimes$
$(|0\rangle\langle 0|)^{\otimes N}_{R^1_A} \otimes (|0\rangle\langle 0|)^{\otimes N}_{R^2_A} \otimes |0\rangle\langle 0|_{b_A} \otimes$
$(|0\rangle\langle 0|)^{\otimes n}_{u_A} \otimes (|0\rangle\langle 0|)^{\otimes n}_{v_A} \otimes (|0\rangle\langle 0|)^{\otimes n}_{U_A} \otimes (|0\rangle\langle 0|)^{\otimes n}_{V_A}$

$\rho_B \equiv (|0\rangle\langle 0|)^{\otimes n}_{Q_B} \otimes (|0\rangle\langle 0|)^{\otimes n}_{sx_B} \otimes (|0\rangle\langle 0|)^{\otimes n}_{sz_B}$

EDPの形式化

秘匿チャネル

$\langle A||B\backslash\{c_1, c_2, \mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_5}, \mathbf{c_6}\},\ \rho_A \otimes \rho_B \otimes \rho_E\rangle$

$A \equiv \mathtt{hadamards}(q'_A, r^1_A).$
$\mathtt{shuffle}(q'_A, r^2_A).$
$\mathbf{c_1}!q'_{A,1}, ..., q'_{A,2n}.c_1?x_A.$
$\mathtt{copy}(r^2_A, R^2_A).\mathbf{c_2}!r^2_A.\mathbf{d_1}!R^2_A.$
$\mathtt{copy}(r^1_A, R^1_A).\mathbf{c_3}!r^1_A.\mathbf{d_2}!R^1_A.$
$\mathtt{measure}(q_{A,1}, ..., q_{A,n})$

改ざん不能公開チャネル

分岐のための観測

$,_1, ..., q_{A,n}, s_A, b_A)$
$M[b_A; y].c_2!y.d_1!y.\mathtt{if}\ y\ \mathtt{then}$
$\mathtt{css\_projection}(q_{A,n+1}, ..., q_{A,2n}, u_A, v_A).$
$\mathtt{css\_decode}(q_{A,n+1}, ..., q_{A,2n}, u_A, v_A)$
$\mathtt{copy}(u_A, U_A).\mathbf{c_5}!u_A.\mathbf{d_3}!U_A.$
$\mathtt{copy}(v_A, V_A).\mathbf{c_6}!v_A.A_2$

$B \equiv \mathbf{c_1}?q_{B,1}, ..., q_{B,2n}.c_1!0.d_2!0.$
$\mathbf{c_2}?r^2_B.\mathtt{unshuffle}(q_B, r^2_B).$
$\mathbf{c_3}?r^1_B.\mathtt{hadamards}(q_B, r^1_B).$
$\mathtt{measure}(q_{B,1}, ..., q_{B,n}).$
$\mathtt{copy}(q_{B,1}, ..., q_{B,n}, Q_{B,1}, ..., Q_{B,n})$
$\mathbf{c_4}!q_{B,1}, ..., q_{B,n}.\mathbf{d_5}!Q_{B,1}, ..., Q_{B,n}.$
$c_2?b_B.\mathtt{if}\ b_B\ \mathtt{then}\ \mathbf{c_5}?u_B.\mathbf{c_6}?v_B.$
$\mathtt{css\_syndrome}(q_{B,n+1}, ..., q_{B,2n}, u_B, v_B, sx_B, sz_B).$
$\mathtt{css\_correct}(q_{B,n+1}, ..., q_{B,2n}, sx_B, sz_B)$
$\mathtt{css\_decode}(q_{B,n+1}, ..., q_{B,2n}, u_B, v_B).B_2$

$\rho_A \equiv (|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)^{\otimes 2n}_{q_A, q'_A} \otimes$
$(|0\rangle\langle 0| + |1\rangle\langle 1|)^{\otimes N}_{r^1_A} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)^{\otimes N}_{r^2_A} \otimes$
$(|0\rangle\langle 0|)^{\otimes N}_{R^1_A} \otimes (|0\rangle\langle 0|)^{\otimes N}_{R^2_A} \otimes |0\rangle\langle 0|_{b_A} \otimes$
$(|0\rangle\langle 0|)^{\otimes n}_{u_A} \otimes (|0\rangle\langle 0|)^{\otimes n}_{v_A} \otimes (|0\rangle\langle 0|)^{\otimes n}_{U_A} \otimes (|0\rangle\langle 0|)^{\otimes n}_{V_A}$

$\rho_B \equiv (|0\rangle\langle 0|)^{\otimes n}_{Q_B} \otimes (|0\rangle\langle 0|)^{\otimes n}_{sx_B} \otimes (|0\rangle\langle 0|)^{\otimes n}_{sz_B}$

BB84の形式化

$\langle A||B\backslash\{c_1, c_2, \mathbf{c_2}, \mathbf{c_3}, \mathbf{c_4}, \mathbf{c_5}\},\ \rho_A \otimes \rho_B \otimes \rho_E\rangle$

$A \equiv \mathtt{hadamards}(q'_A, r^1_A).$
$\mathtt{shuffle}(q'_A, r^2_A).$
$\mathbf{c_1}!q'_{A,1}, ..., q'_{A,2n}.c_1?x_A.$
$\mathtt{copy}(r^2_A, R^2_A).\mathbf{c_2}!r^2_A.\mathbf{d_1}!R^2_A.$
$\mathtt{copy}(r^1_A, R^1_A).\mathbf{c_3}!r^1_A.\mathbf{d_2}!R^1_A.$
$\mathbf{c_4}?s_A.\mathtt{abort\_alice}(q_{A,1}, ..., q_{A,n}, s_A, b_A).$
$M[b_A; y].c_2!y.d_1!y.\mathtt{if}\ y\ \mathtt{then}$
$\mathtt{cnot}(u_A, q_{A,n+1}, ..., q_{A,2n}).$
$\mathtt{copy}(u_A, U_A).\mathbf{c_5}!u_A.\mathbf{d_3}!U_A.$
$\mathtt{cnot}(u_A, q_{A,n+1}, ..., q_{A,2n}).$
$\mathtt{copy}(u_A, q_{A,n+1}, ..., q_{A,2n}).$
$\mathtt{decode}(q_{A,n+1}, ..., q_{A,2n}).A_2$

$B \equiv \mathbf{c_1}?q_{B,1}, ..., q_{B,2n}.c_1!0.d_2!0.$
$\mathbf{c_2}?r^2_B.\mathtt{unshuffle}(q_B, r^2_B).$
$\mathbf{c_3}?r^1_B.\mathtt{hadamards}(q_B, r^1_B).$
$\mathtt{measure}(q_{B,1}, ..., q_{B,n}).$
$\mathtt{copy}(q_{B,1}, ..., q_{B,n}, Q_{B,1}, ..., Q_{B,n})$
$\mathbf{c_4}!q_{B,1}, ..., q_{B,n}.\mathbf{d_5}!Q_{B,1}, ..., Q_{B,n}.$
$c_2?b_B.\mathtt{if}\ b_B\ \mathtt{then}\ \mathbf{c_5}?u_B.$
$\mathtt{cnot}(u_B, q_{B,n+1}, ..., q_{B,2n}).$
$\mathtt{copy}(u_B, q_{B,n+1}, ..., q_{B,2n}).$
$\mathtt{syndrome}(q_{B,n+1}, ..., q_{B,2n}, sx_B).$
$\mathtt{correct}(q_{B,n+1}, ..., q_{B,2n}, sx_B).$
$\mathtt{decode}(q_{B,n+1}, ..., q_{B,2n}).B_2$

$\rho_A \equiv (|00\rangle\langle 00| + |11\rangle\langle 11|)^{\otimes 2n}_{q_A, q'_A} \otimes$
$(|0\rangle\langle 0| + |1\rangle\langle 1|)^{\otimes N}_{r^1_A} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)^{\otimes N}_{r^2_A} \otimes$
$(|0\rangle\langle 0|)^{\otimes N}_{R^1_A} \otimes (|0\rangle\langle 0|)^{\otimes N}_{R^2_A} \otimes |0\rangle\langle 0|_{b_A} \otimes$
$(\sum_{u \in C_1} |u\rangle\langle u|)_{u_A} \otimes (|0\rangle\langle 0|)^{\otimes n}_{U_A}$

$\rho_B \equiv (|0\rangle\langle 0|)^{\otimes n}_{Q_B} \otimes (|0\rangle\langle 0|)^{\otimes n}_{sx_B}$

EDPとBB84の双模倣関係

定理　十分大きな自然数 n, 任意のエラー閾値 e,
CSS符号の条件を満たす任意のC_1, C_2 に対して

$$EDPbased^{n,e}_{C_1,C_2} \approx BB84^{n,e}_{C_1,C_2}$$

系　複数セッションにしたプロセスも双模倣

結論

- BB84とEDPをプロセスとして形式化し，
  双模倣を示した
- 観測の種類によって形式化が異なる
  - 攻撃者に分岐が見える測定は $M[\tilde{q}; x]$ で形式化
  - 攻撃者に分岐が見えない測定は量子演算で形式化

関連研究

- An Algebra of Quantum Processes [YFDJ09]
  - プロセスの実行を分岐できない
- Barbed congruence [DF12]
  - qCCSの観測同値を定義し,
    双模倣と一致することを示した

今後の課題

- 観測のformalな分類
- 確率双模倣
- ケーススタディ
- 自動検証

双模倣関係

- 関係 $R \subseteq Con \times Con$ が模倣であるとは, 任意の $\langle P, \rho\rangle, \langle Q, \sigma\rangle$に対して, $\langle P, \rho\rangle R \langle Q, \sigma\rangle$ ならば, $\mathrm{qv}(P) = \mathrm{qv}(Q)$ かつ $\mathrm{tr}_{\mathrm{qv}(P)}(\rho) = \mathrm{tr}_{\mathrm{qv(Q)}}(\sigma)$であり,
  - $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ ならば, ある ν が存在して, $\langle Q, \sigma\rangle \Rightarrow \xrightarrow{\widehat{\alpha}} \Rightarrow \nu$ かつ $\mu R \nu$　ここで α は量子受信以外
  - $\langle P, \rho\rangle \xrightarrow{\mathbf{c}?q} \mu$ ならば, ある ν が存在して, $\langle Q, \sigma\rangle \Rightarrow \xrightarrow{\mathbf{c}?q} \nu$ かつ $\overline{\mathrm{qv}(P) \cup \{q\}}$に作用する任意の$E$に対して$E(\mu)RE(\nu)$が満たされることをいう
- 模倣Rの逆関係も模倣のとき, Rを双模倣という
- ある双模倣Rが存在してCRDのとき, $C \approx D$とかく

双模倣の性質

- 関係 $\approx$ は同値関係である
- $\langle P||Q,\rho\rangle \approx \langle Q||P,\rho\rangle$
- $\langle P,\rho\rangle \approx \langle Q,\sigma\rangle$ の必要十分条件は,
  $\mathrm{qv}(P) = \mathrm{qv}(Q)$ かつ $\mathrm{tr}_{\mathrm{qv}(P)}(\rho) = \mathrm{tr}_{\mathrm{qv(Q)}}(\sigma)$であり,
  - $\langle P,\rho\rangle \xrightarrow{\alpha} \mu$ ならば, ある ν が存在して,
    $\langle Q,\sigma\rangle \Rightarrow \xrightarrow{\hat{\alpha}} \Rightarrow \nu$ かつ $\mu \approx \nu$　ここで α は量子受信以外
  - $\langle P,\rho\rangle \xrightarrow{\mathbf{c}?q} \mu$ ならば, ある ν が存在して,
    $\langle Q,\sigma\rangle \Rightarrow \xrightarrow{\mathbf{c}?q} \nu$ かつ $\overline{\mathrm{qv}(P) \cup \{q\}}$に作用する
    任意のEに対して$E(\mu) \approx E(\nu)$が満たされることである